Chapter 1

The Principle of Inclusion and Exclusion

1.1 Introduction

For any set A, let $|A|$ denote the number of members in A. If A_1 and A_2 are disjoint sets (i.e., $A_1 \cap A_2 = \emptyset$), then

$$label : \mathbf{eq1-1} |A_1 \cup A_2| = |A_1| + |A_2| \tag{1.1}$$

and, in general, if $A_1, A_2, \cdots, A_n$ are pairwisely disjoint sets (i.e., $A_i \cap A_j = \emptyset$ for all i, j with $1 \le i < j \le n$), then

$$label : \mathbf{eq1-2} |A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|. \tag{1.2}$$

But, if $A_i \cap A_j \neq \emptyset$ for some pair i and j, then (1.2) does not hold.

Then a problem arises:

Problem 1.1.1 *How can we determine* $|A_1 \cup A_2 \cup \cdots \cup A_n|$ *if we just know the values of* $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$ *for all* $i_1, i_2, \cdots, i_k$ *with* $1 \le i_1 < i_2 < \cdots < i_k \le n$*?*

In this chapter we shall first develop a formula for $|A_1 \cup A_2 \cup \cdots \cup A_n|$ in terms of all $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$'s. This result is called the **Principle of Inclusion and Exclusion** (or simply **PIE**). We will then extend PIE to a more general result which is named **GPIE**.

In the remaining sections of this chapter, we shall apply GPIE to study some famous counting problems, such as

(i) to find a formula for the number of surjective mappings from N_n to N_m;

(ii) to find a formula for the number of permutations $a_1a_2\cdots a_n$ of $\{1,2,\cdots,n\}$ such that $a_i \neq i$; and

(iii) to find a formula for the number of numbers a in $\{1,2,\cdots,n\}$ such that a and n are coprime, i.e., $(a,n)=1$.

1.2 The Principle of Inclusion and Exclusion

Let $A_1, A_2, \cdots, A_n$ be finite sets. In this section, we shall find a formula to express $|A_1 \cup A_2 \cup \cdots \cup A_n|$ in terms of $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$ for all $i_1, i_2, \cdots, i_k$ with $1 \le i_1 < i_2 < \cdots < i_k \le n$.

Lemma 1.2.1 *label:* **le1-2-0** *For any two sets A_1 and A_2, if $A_1 \cap A_2 = \emptyset$, then*

$$label\ :\mathbf{eq1-2-0}|A_1 \cup A_2| = |A_1| + |A_2|. \tag{1.3}$$

Lemma 1.2.2 *label:* **le1-2-0-1** *For any two sets A_1 and A_2, if A_2 is a subset of A_1, then*

$$label\ :\mathbf{eq1-2-0-1}|A_1 - A_2| = |A_1| - |A_2|. \tag{1.4}$$

Can you prove Lemma 1.2.2 by applying Lemma 1.2.1?

Note that Lemma 1.2.2 is not true if A_2 is not a subset of A_1. For example, if $A_1 = \{1,2,3,4,5\}$ and $A_2 = \{3,4,5,6,7,8\}$, then

$$|A_1 - A_2| = |\{1,2\}| = 2$$

but

$$|A_1| - |A_2| = 5 - 6 = -1.$$

Is there an expression similar to Lemma 1.2.2 when A_2 is not a subset of A_1?

Now we apply Lemmas 1.2.1 and 1.2.2 to deduce the following well-known formula.

Lemma 1.2.3 *label:* **le1-2-1** *For any two sets A_1 and A_2, we have*

$$label\ :\mathbf{eq1-2-1}|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|. \tag{1.5}$$

Proof. Since

$$\textit{label}:\mathbf{eq1-2-2}A_1 \cup A_2 = A_1 \cup (A_2 - (A_1 \cap A_2)), \tag{1.6}$$

and

$$\textit{label}:\mathbf{eq1-2-3}A_1 \cap (A_2 - (A_1 \cap A_2)) = \emptyset, \tag{1.7}$$

by Lemmas 1.2.1, we have

$$\textit{label}:\mathbf{eq1-2-4}|A_1 \cup A_2| = |A_1| + |A_2 - (A_1 \cap A_2)|. \tag{1.8}$$

Since $A_1 \cap A_2$ is a subset of A_2, by Lemmas 1.2.1, we have

$$\textit{label}:\mathbf{eq1-2-5}|A_2 - (A_1 \cap A_2)| = |A_2| - |A_1 \cap A_2|. \tag{1.9}$$

Therefore, by (1.8) and (1.9), we have

$$\textit{label}:\mathbf{eq1-2-6}|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|. \tag{1.10}$$

□

Exercise 1.2.1 *Let $S = \{1, 2, 3, \cdots, 2000\}$. Find the number of integers in S which are of the form n^2 or n^3, where n is an integer.*

Exercise 1.2.2 *Let $S = \{1, 2, 3, \cdots, 2000\}$. Find the number of integers in S which are of the form n^2 but not of the form n^4, where n is an integer.*

Lemma 1.2.4 *label:* **le1-2-2** *For any three sets A_1, A_2 and A_3, we have*

$$\textit{label}:\mathbf{eq1-2-7}|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|. \tag{1.11}$$

Proof. We shall apply (1.5) to prove this result. Observe that

$$\begin{aligned}
& |A_1 \cup A_2 \cup A_3| \\
= & |(A_1 \cup A_2) \cup A_3| \\
= & |A_3| + |A_1 \cup A_2| - |A_3 \cap (A_1 \cup A_2)| \\
= & |A_3| + |A_1 \cup A_2| - |(A_3 \cap A_1) \cup (A_3 \cap A_2)| \\
= & |A_3| + |A_1| + |A_2| - |A_1 \cap A_2| - |A_3 \cap A_1| - |A_3 \cap A_2| + |(A_3 \cap A_1) \cap (A_3 \cap A_2)| \\
= & |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|.
\end{aligned}$$

□

Example 1.2.1 *label:* **ex1-2-1** *Determine the number of integers in* $B = \{1, 2, 3, \cdots, 200\}$ *which are multiples of* $2, 3$ *or* 5.

Solution. For any integer $k \geq 2$, let

$$Z_k = \{a \in B : a \text{ is divisible by } k\}.$$

We are required to determine $|Z_2 \cup Z_3 \cup Z_5|$.

Observe that for any $k \geq 2$,

$$|Z_k| = \left\lfloor \frac{200}{k} \right\rfloor.$$

Hence

$$|Z_2| = \left\lfloor \tfrac{200}{2} \right\rfloor = 100,$$

$$|Z_3| = \left\lfloor \tfrac{200}{3} \right\rfloor = 66,$$

$$|Z_5| = \left\lfloor \tfrac{200}{5} \right\rfloor = 40,$$

$$|Z_2 \cap Z_3| = |Z_6| = \left\lfloor \tfrac{200}{6} \right\rfloor = 33,$$

$$|Z_2 \cap Z_5| = |Z_{10}| = \left\lfloor \tfrac{200}{10} \right\rfloor = 20,$$

$$|Z_3 \cap Z_5| = |Z_{10}| = \left\lfloor \tfrac{200}{15} \right\rfloor = 13,$$

$$|Z_2 \cap Z_3 \cap Z_5| = |Z_{30}| = \left\lfloor \tfrac{200}{30} \right\rfloor = 6.$$

Therefore, by Lemma 1.2.4, we have

$$\begin{aligned} & |Z_2 \cup Z_3 \cup Z_5| \\ = \ & |Z_2| + |Z_3| + |Z_5| - (|Z_2 \cap Z_3| + |Z_2 \cap Z_5| + |Z_3 \cap Z_5|) + |Z_2 \cap Z_3 \cap Z_5| \\ = \ & 100 + 66 + 40 - (33 + 20 + 13) + 6 \\ = \ & 146. \end{aligned}$$

□

Exercise 1.2.3 *label:* **exer1-2-1-0** *Determine the number of integers in* $B = \{1, 2, 3, \cdots, 200\}$ *which are multiples of* $3, 4$ *or* 5.

In general, we have the following result, which is called the **Principle of Inclusion and Exclusion** (or simply **PIE**).

Theorem 1.2.1 (PIE) *label:* **th1-2-1** *For any n finite sets $A_1, A_2, \cdots, A_n$, where $n \geq 2$,*

$$label:\mathbf{eq1-2-9}|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|. \quad (1.12)$$

Proof. We shall this theorem by induction on n. If $n = 2$, then it holds by (1.5). Assume that it holds if $n < m$, where $m \geq 3$. Now let $n = m$. By (1.5), we have

$$\begin{aligned} label:\mathbf{eq1-2-10} \quad & |A_1 \cup A_2 \cup \cdots \cup A_n| \\ = & |(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n| \\ = & |A_1 \cup A_2 \cup \cdots \cup A_{n-1}| + |A_n| - |(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cap A_n| \\ = & |A_1 \cup A_2 \cup \cdots \cup A_{n-1}| + |A_n| \\ & -|(A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n)|. \quad (1.13) \end{aligned}$$

By the inductive assumption,

$$label:\mathbf{eq1-2-11}|A_1 \cup A_2 \cup \cdots \cup A_{n-1}| = \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|, \quad (1.14)$$

and

$$\begin{aligned} label:\mathbf{eq1-2-12} \quad & |(A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n)| \\ = & \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |(A_{i_1} \cap A_n) \cap (A_{i_2} \cap A_n) \cap \cdots \cap (A_{i_k} \cap A_n)| \\ = & \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k} \cap A_n|. \quad (1.15) \end{aligned}$$

Then, by (1.13), (1.14) and (1.15), we have

$$\begin{aligned} label:\mathbf{eq1-2-13} \quad & |A_1 \cup A_2 \cup \cdots \cup A_n| \\ = & \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \\ & +|A_n| - \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k} \cap A_n| \\ = & \sum_{k=1}^{n-1}(-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \end{aligned}$$

$$
\begin{aligned}
& +|A_n| + \sum_{k=1}^{n-1}(-1)^k \sum_{1\le i_1<i_2<\cdots<i_k\le n-1} |A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\cap A_n| \\
= & \sum_{k=1}^{n}(-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k<n} |A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}| \\
& +\sum_{k=1}^{n}(-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k=n} |A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}| \\
= & \sum_{k=1}^{n}(-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} |A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}|. \qquad (1.16)
\end{aligned}
$$

□

Exercise 1.2.4 *label:* **exer1-2-1** *Determine the number of integers in* $B = \{1, 2, 3, \cdots, 200\}$ *which are multiples of* $2, 3, 5$ *or* 7.

1.3 A generalization

Example 1.2.1 applies Lemma 1.2.4 (i.e., Theorem 1.2.1 for $n = 3$) to count the number of integers in $B = \{1, 2, \cdots, 200\}$ which are multiples of $2, 3$ or 5. Now we want to ask the following question:

Question 1.3.1 *label:* **qu1-3-1** *Can Theorem 1.2.1 be applied to determine directly the number of integers in* $B = \{1, 2, 3, \cdots, 200\}$ *which are divisible by*

(i) exactly one of $2, 3, 5$ *or*

(ii) exactly two of $2, 3, 5$*?*

The answer to Question 1.3.1 is **NO**.

In this section, we shall find a result which can be used to solve such questions, and this result is more general than Theorem 1.2.1.

Let S be a finite set. For $i = 1, 2, \cdots, k$, where $k \ge 1$, let P_i be a **property** for some elements of S. A property may be possessed by none, some or all elements of S.

For example, $S = \{1, 2, 3, \cdots, 1000\}$, $k = 3$ and

P_1 be the property that an integer is divisible by 3,

P_2 be the property that an integer is divisible by 5, and

P_3 be the property that an integer is divisible by 7.

Let $\omega(P_{i_1}P_{i_2}\cdots P_{i_s})$ be the number of elements in S which possess all the properties $P_{i_1}, P_{i_2}, \cdots, P_{i_s}$, where $1 \le i_1 < i_2 < \cdots < i_s \le k$.

For any s with $1 \le s \le k$, let

$$label\ :\mathbf{eq1-3-1}\omega(s) = \sum_{1\le i_1<i_2<\cdots<i_s\le k} \omega(P_{i_1}P_{i_2}\cdots P_{i_s}). \tag{1.17}$$

Note that

$$\begin{aligned}\omega(1) &= \omega(P_1) + \omega(P_2) + \cdots + \omega(P_k),\\ \omega(2) &= \omega(P_1P_2) + \omega(P_1P_3) + \cdots + \omega(P_1P_k) + \omega(P_2P_3) + \cdots + \omega(P_{k-1}P_k),\\ &\cdots.\end{aligned}$$

We also define $\omega(0)$ to be $|S|$.

Example 1.3.1 *label:* **ex1-3-1** *Let* $S = \{1, 2, 3, \cdots, 1000\}$. *Let*

P_1 *be the property that an integer is divisible by* 3,

P_2 *be the property that an integer is divisible by* 5, *and*

P_3 *be the property that an integer is divisible by* 7.

Find

(i) $\omega(P_1)$, $\omega(P_2)$, $\omega(P_3)$, $\omega(P_1P_2)$, $\omega(P_1P_3)$, $\omega(P_2P_3)$ *and* $\omega(P_1P_2P_3)$;

(ii) $\omega(0)$, $\omega(1)$, $\omega(2)$ *and* $\omega(3)$.

Solution. (i) We have

$$\omega(P_1) = \left\lfloor \tfrac{1000}{3} \right\rfloor = 333;$$

$$\omega(P_2) = \left\lfloor \tfrac{1000}{5} \right\rfloor = 200;$$

$$\omega(P_3) = \left\lfloor \tfrac{1000}{7} \right\rfloor = 142;$$

$$\omega(P_1P_2) = \left\lfloor \tfrac{1000}{15} \right\rfloor = 66;$$

$$\omega(P_1P_3) = \left\lfloor \tfrac{1000}{21} \right\rfloor = 47;$$

$$\omega(P_2P_3) = \left\lfloor \tfrac{1000}{35} \right\rfloor = 28;$$

$$\omega(P_1P_2P_3) = \left\lfloor \tfrac{1000}{105} \right\rfloor = 9.$$

(ii) $\omega(0) = |S| = 1000$. By (i), we have

$$\omega(1) = \omega(P_1) + \omega(P_2) + \omega(P_3) = 333 + 200 + 142 = 675;$$

$$\omega(2) = \omega(P_1P_2) + \omega(P_1P_3) + \omega(P_2P_3) = 66 + 47 + 28 = 141;$$

$$\omega(3) = \omega(P_1P_2P_3) = 9.$$

□

For any integer m with $0 \le m \le k$, let $E(m)$ denote the number of elements in S which possess *exactly* m of the k properties $P_1, P_2, \cdots, P_k$.

For example, Let $S = \{1, 2, 3, \cdots, 1000\}$. Let P_1 be the property that a number in S is divisible by 2, P_2 be the property that a number in S is divisible by 3, and P_3 be the property that a number in S is divisible by 5. Then

- $E(1)$ is the number of integers in S which are divisible exactly one of $2, 3, 5$,
- $E(2)$ is the number of integers in S which are divisible exactly two of $2, 3, 5$
- $E(3)$ is the number of integers in S which are divisible exactly three of $2, 3, 5$ (i.e., divisible by each of $2, 3, 5$).

Theorem 1.3.1 (GPIE) *label:* **th1-3-1** *Let S be a finite set and $P_1, P_2, \cdots, P_k$ be k properties for elements in S. Then, for each $m = 0, 1, 2, \cdots, k$,*

$$label\ :\mathbf{eq1-3-2} E(m) = \sum_{s=m}^{k} (-1)^{s-m} \binom{s}{m} \omega(s). \tag{1.18}$$

Proof. We just need to show that every member of S has equal contribution to both sides.

Let x be any member in S. Assume that x has exactly t properties of $P_1, P_2, \cdots, P_k$, where $t \le k$. Without loss of generality, assume that x possesses properties $P_1, P_2, \cdots, P_t$, but x does not possess properties $P_{t+1}, P_{t+2}, \cdots, P_k$.

Case 1: $t < m$.

The contribution of x to $E(m)$ is 0 and to $\omega(s)$ is also 0 for all $s \ge m$. Hence x contributes 0 to both sides of (1.18).

Case 2: $t = m$.

The contribution of x to $E(m)$ is 1, to $\omega(m)$ is also 1, but to $\omega(s)$ is 0 for all $s > m$. Hence x contributes 1 to both sides of (1.18).

Case 3: $t > m$.

The contribution of x to $E(m)$ is 0. The contribution of x

$$\begin{array}{llll} \text{to} & \omega(m) & \text{is} & \binom{t}{m}, \\ \text{to} & \omega(m+1) & \text{is} & \binom{t}{m+1}, \\ & \vdots & & \\ \text{to} & \omega(t) & \text{is} & \binom{t}{t}, \quad \text{and} \\ \text{to} & \omega(s) & \text{is} & 0 \quad \text{for} \quad s > t. \end{array}$$

Hence the contribution of x to the left-hand side is 0 and to the right-hand side is

$$label\ \text{:}\mathbf{eq1-3-3} \sum_{s=m}^{t} (-1)^{s-m} \binom{s}{m} \binom{t}{s}. \tag{1.19}$$

Observe that

$$\begin{aligned} label\ \text{:}\mathbf{eq1-3-4} \sum_{s=m}^{t} (-1)^{s-m} \binom{s}{m} \binom{t}{s} &= \sum_{s=m}^{t} (-1)^{s-m} \binom{t-m}{s-m} \binom{t}{m} \\ &= \binom{t}{m} \sum_{s=m}^{t} (-1)^{s-m} \binom{t-m}{s-m} \\ &= \binom{t}{m} \sum_{i=0}^{t-m} (-1)^{i} \binom{t-m}{i} \\ &= \binom{t}{m} (1-1)^{t-m} \\ &= 0. \end{aligned} \tag{1.20}$$

Hence x contributes 0 to both sides of (1.18).

Since x contributes equally to both sides of (1.18) for all numbers $x \in S$, the theorem holds. □

If $k = 3$, then by Theorem 1.3.1, we have

$$E(0) = \sum_{s=0}^{3} (-1)^{s-0} \binom{s}{0} \omega(s) = \sum_{s=0}^{3} (-1)^{s} \omega(s) = \omega(0) - \omega(1) + \omega(2) - \omega(3);$$

$$E(1) = \sum_{s=1}^{3}(-1)^{s-1}\binom{s}{1}\omega(s) = \sum_{s=1}^{3}(-1)^{s-1}s\omega(s) = \omega(1) - 2\omega(2) + 3\omega(3);$$

$$E(2) = \sum_{s=2}^{3}(-1)^{s-2}\binom{s}{2}\omega(s) = \sum_{s=2}^{3}(-1)^{s-2}\binom{s}{2}\omega(s) = \omega(2) - 3\omega(3);$$

$$E(3) = \sum_{s=3}^{3}(-1)^{s-3}\binom{s}{3}\omega(s) = \omega(3).$$

Exercise 1.3.1 *label:* **exer1-3-2** *Let* $S = \{1, 2, 3, \cdots, 1000\}$*. Determine the number of integers in* S *which are divisible by*

(i) exactly one of $2, 3, 5$*;*

(ii) exactly two of $2, 3, 5$.

By considering some special cases in Theorem 1.3.1, we obtain some corollaries.

Corollary 1.3.1 *label:* **cor1-3-1** *Let* S *be a finite set and* $P_1, P_2, \cdots, P_k$ *be* k *properties for elements in* S*. Then*

$$label :\mathbf{eq1-3-5} E(0) = \sum_{s=0}^{k}(-1)^s\omega(s) = \omega(0) - \omega(1) + \omega(2) - \cdots + (-1)^k\omega(k). \quad (1.21)$$

□

Corollary 1.3.2 *label:* **cor1-3-2** *Let* S *be a finite set and* $P_1, P_2, \cdots, P_k$ *be* k *properties for elements in* S*. Then*

$$label :\mathbf{eq1-3-6} E(1) = \sum_{s=1}^{k}(-1)^{s-1}s\omega(s) = \omega(1) - 2\omega(2) + 3\omega(3) - \cdots + (-1)^{k-1}k\omega(k); \quad (1.22)$$

$$label :\mathbf{eq1-3-6-1} E(2) = \sum_{s=2}^{k}(-1)^{s-2}\binom{s}{2}\omega(s) = \omega(2) - 3\omega(3) + 6\omega(4) - \cdots + (-1)^k\binom{k}{2}\omega(k). \quad (1.23)$$

□

Corollary 1.3.3 *label:* **cor1-3-3** *Let* $A_1, A_2, \cdots, A_k$ *be* k *subsets of a finite set* S*. Then*

$$label :\mathbf{eq1-3-7} |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_k| = |S| + \sum_{s=1}^{k}(-1)^s \sum_{1 \le i_1 < i_2 < \cdots < i_s \le k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_s}|, \quad (1.24)$$

where $\bar{A}_i$ denotes the complement of A_i in S (i.e., $\bar{A}_i = S - A_i$).

Proof. For any integer i with $1 \le i \le k$, assume that P_i is the property in S defined below:

for every $a \in S$, a has the property P_i if and only if $a \in A_i$.

Then

$$E(0) = |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_k|$$

and for any $i_1, i_2, \cdots, i_s$ with $1 \le i_1 < i_2 < \cdots < i_s \le k$,

$$\omega(P_{i_1} P_{i_2} \cdots P_{i_s}) = |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_s}|.$$

Thus $\omega(0) = |S|$ and for any s with $1 \le s \le k$,

$$\omega(s) = \sum_{1 \le i_1 < i_2 < \cdots < i_s \le k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_s}|.$$

By Corollary 1.3.1,

$$E(0) = \sum_{s=0}^{k} (-1)^s \omega(s).$$

Hence

$$\begin{aligned} |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_k| &= \omega(0) + \sum_{s=1}^{k} (-1)^s \omega(s) \\ &= |S| + \sum_{s=1}^{k} (-1)^s \sum_{1 \le i_1 < i_2 < \cdots < i_s \le k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_s}|. \end{aligned}$$

This completes the proof. □

Exercise 1.3.2 *label:* **exer1-3-3** *Let $S = \{1, 2, \cdots, 10000\}$.*

(i) *Find the number of those integers in S which are not divisible by any one of $2, 3, 5$.*

(ii) *Find the number of those integers in S which are divisible by exactly one of $2, 3, 5$;*

(iii) *Find the number of those integers in S which are divisible by exactly two of $2, 3, 5$.*

1.4 Surjective mappings

A mapping $f : A \longmapsto B$ is called a **surjective mapping** if $f(A) = B$, i.e., for every $b \in B$, there exists $a \in A$ such that $f(a) = b$.

Note that if A and B are finite sets and there is a surjective mapping from A to B, then $|A| \geq |B|$. Thus there are no surjective mapping from A to B if A and B are finite sets and $|A| < |B|$.

For any positive integer k, let

$$label :\mathbf{eq1-4-1} N_k = \{1, 2, \cdots, k\}. \tag{1.25}$$

For any two positive integers n and m, let $F(n, m)$ be the *number of surjective mappings* from N_n to N_m.

$F(n, m)$ can also be regarded as *the number of ways of distributing n distinct apples into m distinct boxes such that no box is empty.*

In this section, we shall apply **GPIE** to establish a general formula for $F(n, m)$. We first consider some special cases.

Lemma 1.4.1 *label:* **le1-4-1** *Let n, m be positive integer.*

(i) $F(n, m) = 0$ if $n < m$;

(ii) $F(n, n) = n!$;

(iii) $F(n, n-1) = \binom{n}{2}(n-1)!$; and

(vi) $F(n, 1) = 1$.

Proof. (i) holds obviously, since there are no surjective mappings from N_n to N_m if $n < m$.

(ii) A mapping f from N_n to N_n is surjective if and only if $f(1), f(2), \cdots, f(n)$ is a permutation of $1, 2, \cdots, n$. Since N_n has $n!$ permutations, we have $F(n, n) = n!$.

(iii) A mapping f from N_n to N_{n-1} is surjective if and only if $f(i) = f(j)$ for some pair i, j with $1 \leq i < j \leq n$ and $f(1), f(2), \cdots, f(j-1), f(j+1), \cdots, f(n)$ is a permutation of $1, 2, \cdots, n-1$. There are $\binom{n}{2}$ ways to select a pair i, j from N_n and there are $(n-1)!$ permutations of $1, 2, \cdots, n-1$. Thus (iii) holds.

(iv) Since $m = 1$, there is only one mapping from N_n to N_1. This only one mapping is clearly surjective. Hence $F(n, 1) = 1$. □

Now we are going to apply **GPIE** to find an expression for $F(n, m)$.

Theorem 1.4.1 *label:* **th1-4-1** *For any two positive integers n and m,*

$$label\ :\mathbf{eq1-4-2} F(n,m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n. \tag{1.26}$$

Proof. Let S be the set of mappings from N_n to N_m. Define m properties $P_1, P_2, \cdots, P_m$ for members of S as follows: for $i = 1, 2, \cdots, m$,

$$\text{a mapping } f \in S \text{ is said to possess } P_i \iff i \notin f(N_n).$$

Then a mapping $f : N_n \to N_m$ is surjective if and only if f possesses none of the properties $P_1, P_2, \cdots, P_m$. Thus $F(n,m) = E(0)$, and we can apply Corollary 1.3.1 to determine $F(n,m)$.

Observe that

$$\omega(0) = |S| = m^n;$$

$$\omega(1) = \sum_{i=1}^{m} \omega(P_i) = \tbinom{m}{1}(m-1)^n;$$

and for each k with $2 \le k \le m$, we have

$$\omega(k) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le m} \omega(P_{i_1} P_{i_2} \cdots P_{i_k}) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le m} (m-k)^n = \binom{m}{k}(m-k)^n.$$

Thus, By Corollary 1.3.1, we have

$$\begin{aligned} F(n,m) &= E(0) \\ &= \sum_{k=0}^{m} (-1)^k \omega(k) \\ &= \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n, \end{aligned}$$

as desired. □

By Lemma 1.4.1 (i) to (iii) and Theorem 1.4.1, we have

Corollary 1.4.1 *For any positive integers n and m, we have*

(i) $\sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n = 0$ *if* $n < m$;

(ii) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n = n!$;

(iii) $\sum_{k=0}^{n-1} (-1)^k \binom{n-1}{k} (n-1-k)^n = (n-1)! \binom{n}{2}$. □

Example 1.4.1 *label:* **exa1-4-1** *Find the expression for $F(n, 2)$.*

Solution. By Theorem 1.4.1, we have

$$\begin{aligned} F(n,2) &= \sum_{k=0}^{2}(-1)^k\binom{2}{k}(2-k)^n \\ &= \binom{2}{0}(2-0)^n - \binom{2}{1}(2-1)^n + \binom{2}{2}(2-2)^n \\ &= 2^n - 2. \end{aligned}$$

□

Exercise 1.4.1 *label:* **exer1-4-1** *Find the expression for $F(n, 3)$.*

In the end of this section, we study the **Stirling number of the second kind**, denoted by $S(n, m)$, defined below.

Definition 1.4.1 *label:* **def1-4-1** *For any positive integers n and m, let $S(n, m)$ denote the number of ways of distributing n distinct objects into m identical boxes such that no box is empty.*

By the definitions of $F(n, m)$ and $S(n, m)$, we have

$$label\ :\mathbf{eq1-4-3}F(n,m) = m!S(n,m). \tag{1.27}$$

Thus (1.27) and Theorem 1.4.1 give a formula for $S(n, m)$.

Theorem 1.4.2 *label:* **th1-4-2** *For any positive integers n and m,*

$$label\ :\mathbf{eq1-4-4}S(n,m) = \frac{1}{m!}\sum_{k=0}^{m}(-1)^k\binom{m}{k}(m-k)^n. \tag{1.28}$$

□

In the following, we introduce some properties of $S(n,m)$. First, by Definition 1.4.1, we observe that

$$label:\mathbf{eq1-4-5} \begin{cases} S(n,m)=0 & \text{if } n<m; \\ S(n,n)=1; \\ S(n,1)=1. \end{cases} \tag{1.29}$$

In general, there is a recursive expression for $S(n,m)$.

Theorem 1.4.3 *label:* **th1-4-3** *For any positive integers n and m with $n \geq m$,*

$$label:\mathbf{eq1-4-6} S(n,m) = S(n-1,m-1) + mS(n-1,m). \tag{1.30}$$

Proof. Let $a_1, a_2, \cdots, a_n$ be n distinct objects. There are two different types of ways of distributing these n objects into m identical boxes such that no box is empty:

Type 1: a_1 is the only object in a box;

Type 2: a_1 is mixed with some other objects in a box.

In type 1, the other $n-1$ objects $a_2, a_3, \cdots, a_n$ are distributed to other $m-1$ identical boxes such that no box is empty, and so the number of ways to do so is

$$S(n-1,m-1).$$

In type 2, the other $n-1$ objects $a_2, a_3, \cdots, a_n$ must be distributed to the m identical boxes such that no box is empty. So, in type 2, each way consists of two steps:

Step 1: $a_2, a_3, \cdots, a_n$ are first distributed to the m identical boxes such that no box is empty, and the number of ways to do so is

$$S(n-1,m).$$

Step 2: a_1 is then distributed into any one of the m boxes, and the number of ways to do so is m.

Hence, in type 2, there are $mS(n-1,m)$ ways. Therefore,

$$S(n,m) = S(n-1,m-1) + mS(n-1,m),$$

as desired. □

It is clear that $S(n,m)$ is completely determined by (1.29) and (1.30).

Corollary 1.4.2 *label:* **cor1-4-2** *The Stirling number $S(n, m)$ of the second kind is determined by the recursive expression: for $2 \le m < n$,*

$$S(n, m) = S(n-1, m-1) + mS(n-1, m),$$

together with the boundary conditions:

$$\begin{cases} S(n, m) = 0, & \textit{if } n < m; \\ S(n, n) = 1; \\ S(n, 1) = 1. \end{cases}$$

□

Example 1.4.2 *By Corollary 1.4.2, we can obtain values of $S(n, m)$ for $1 \le n \le 4$ and $1 \le m \le 7$, as shown in the table below.*

Values of $S(n, m)$, for $1 \le n \le 7$ and $1 \le m \le 7$

$n \setminus m$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0
3	1	3	1	0	0	0	0
4	1	7	6	1	0	0	0
5							
6							
7							

Exercise 1.4.2 *Complete the above table for $5 \le n \le 7$ and $1 \le m \le 7$.*

We end this section with a result on the expression of x^n in terms of $(x)_0, (x)_1, \cdots, (x)_n$, where $(x)_k$ is given in the following definition.

Definition 1.4.2 *label:* **def1-4-2** *Let x be a variable which can be any complex number. Let $(x)_0 = 1$ and for any positive integer m,*

$$label\ :\mathbf{eq1-4-7} (x)_m = x(x-1)\cdots(x-m+1). \tag{1.31}$$

The function $(x)_m$ is usually called a partial factorial.

The polynomial x^n can be expressed in terms of $(x)_m$'s. For example,

$$label\ :\mathbf{eq1-4-8} \begin{cases} x^1 = (x)_1; \\ x^2 = x + x(x-1) = (x)_1 + (x)_2; \\ x^3 = x + 3x(x-1) + x(x-1)(x-2) = (x)_1 + 3(x)_2 + (x)_3. \end{cases} \tag{1.32}$$

Theorem 1.4.4 *label:* **th1-4-4** *Prove that for any integer n,*

$$label\ :\mathbf{eq1-4-9} x^n = \sum_{m=1}^{n} S(n,m)(x)_m. \tag{1.33}$$

Proof. Assume that

$$label\ :\mathbf{eq1-4-10} x^n = \sum_{m=1}^{n} T(n,m)(x)_m, \tag{1.34}$$

and we also assume that $T(n,m) = 0$ for all m with $m > n$. So we are required to prove that $T(n,m) = S(n,m)$ for all positive integers n and m with $1 \leq m \leq n$. We shall prove it by induction on n.

We first show that $T(n,1) = 1 = S(n,1)$ and $T(n,n) = 1 = S(n,n)$ for all $n \geq 1$.

Since $(1)_m = 0$ if $m \geq 2$, by (1.34), we have

$$1 = T(n,1).$$

In (1.34), the left-hand side expression is a polynomial of degree n, the right-hand side expression is also a polynomial of degree n. This implies that $T(n,n) = 1$.

Hence $T(n,1) = 1 = S(n,1)$ and $T(n,n) = 1 = S(n,n)$. This also implies that $T(n,m) = S(n,m)$ if $1 \leq n \leq 2$. Now assume that $n \geq 3$. We just need to show that $T(n,m) = S(n,m)$ if $2 \leq m \leq n-1$.

By inductive assumption, $T(n-1,m) = S(n-1,m)$ for all m with $1 \leq m \leq n-1$, and so

$$label\ :\mathbf{eq1-4-11} x^{n-1} = \sum_{m=1}^{n-1} S(n-1,m)(x)_m. \tag{1.35}$$

By (1.35), we have

$$\begin{aligned}
x^n &= x \times x^{n-1} \\
&= x \sum_{m=1}^{n-1} S(n-1,m)(x)_m \\
&= \sum_{m=1}^{n-1} S(n-1,m)((x-m)+m)(x)_m \\
&= \sum_{m=1}^{n-1} S(n-1,m)(x-m)(x)_m + \sum_{m=1}^{n-1} S(n-1,m)m(x)_m \\
&= \sum_{m=1}^{n-1} S(n-1,m)(x)_{m+1} + \sum_{m=1}^{n-1} mS(n-1,m)(x)_m \\
&= \sum_{m=2}^{n} S(n-1,m-1)(x)_m + \sum_{m=1}^{n-1} mS(n-1,m)(x)_m.
\end{aligned}$$

Hence for any m with $2 \le m < n$, we have

$$T(n,m) = S(n-1,m-1) + mS(n-1,m).$$

Then, by Theorem 1.4.3, we have $T(n,m) = S(t,m)$. $\square$

Example 1.4.3 *Express $x^2 - 3x + 6$ in terms of $(x)_0, (x)_1$ and $(x)_2$.*

Solution. By Theorem 1.4.4,

$$x^2 = \sum_{m=1}^{2} S(2,m)(x)_m = (x)_1 + (x)_2$$

and

$$x = (x)_1.$$

Thus

$$x^2 - 3x + 6 = (x)_1 + (x)_2 - 3(x)_1 + 6(x)_0 = (x)_2 - 2(x)_1 + 6(x)_0.$$

$\square$

Exercise 1.4.3 *Express $x^2 + 2x + 3$ in terms of $(x)_0, (x)_1$ and $(x)_2$.*

Exercise 1.4.4 *Express $x^3 + 2x^2 + 3x + 3$ in terms of $(x)_0, (x)_1, (x)_2$ and $(x)_3$.*

1.5 Derangements

Suppose two decks, A and B, of cards are given. The cards of A are first laid out in a row, and those of B are then placed at random, one at the top on each card of A such that 52 pairs of cards are formed. What is the probability that no 2 cards are the same in each pair? This problem, known as "le problème des rencontres" was posed by the Frenchman Pierre Rémond de Montmort (1678-1719) in 1708, and he solved it in 1713.

To solve this problem, the pattern of cards of A laid on a row is regarded to be fixed. The total number of ways to place cards of B is 52!. If there are T ways to place cards of B such that no two cards in each pair are the same, then the answer for the above problem is

$$\frac{T}{52!}.$$

Hence the essential part of the above problem is to determine T.

Let n be any positive integer. A permutation $a_1a_2\cdots a_n$ of $N_n = \{1, 2, \cdots, n\}$ is called a **derangement** (nothing is at its right place) of N_n if $a_i \neq i$ for each $i = 1, 2, \cdots, n$. For example, the following permutations are derangement of $\{1, 2, 3\}$:

$$231, 312.$$

Exercise 1.5.1 *Can you find all derangement of* $\{1, 2, 3, 4\}$ *starting with* 2*?*

Let $D_0 = 1$ and for any positive integer n, let D_n denote the number of derangements of N_n. By this definition, we have

$$D_0 = 1, D_1 = 0, D_2 = 1, D_3 = 2.$$

What is D_n for $n \geq 4$?

Is there any general formula for D_n? This problem was solved by N.Bernoulli and P.R. Montmort in 1713.

Theorem 1.5.1 *label:* **th1-5-1** *For any integer* $n \geq 0$,

$$label:\mathbf{eq1-5-1} D_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right). \tag{1.36}$$

Proof. The result is obvious when $n = 0$.

Let S be the set of permutations of N_n. We define n properties $P_1, P_2, \cdots, P_n$ for members of S as follows: for any $i : 1 \leq i \leq n$,

a permutation $a_1a_2\cdots a_n$ is said to possess the property $P_i \iff a_i = i$.

Thus

$$D_n = E(0).$$

Observe that $\omega(0) = |S| = n!$ and for any $k \geq 1$, we have

$$label:\mathbf{eq1-5-2}\omega(k) = \sum_{1\leq i_1<i_2<\cdots<i_k\leq n}\omega(P_{i_1}P_{i_2}\cdots P_{i_k}) = \sum_{1\leq i_1<i_2<\cdots<i_k\leq n}(n-k)! = \binom{n}{k}(n-k)! = \frac{n!}{k!}. \tag{1.37}$$

By Corollary 1.3.1, we have

$$label\ :\mathbf{eq1-5-3} D_n = E(0) = \sum_{k=0}^{n}(-1)^k\omega(k) = \sum_{k=0}^{n}(-1)^k\frac{n!}{k!} = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}, \tag{1.38}$$

as desired. □

Exercise 1.5.2 *Find the values of D_n for $n = 3, 4, 5, 6$.*

Corollary 1.5.1 *label:* **cor1-5-1**

$$label\ :\mathbf{eq1-5-4} \lim_{n\to\infty}\frac{D_n}{n!} = e^{-1} \approx 0.367. \tag{1.39}$$

Why?

We end this section with some recursive expressions for D_n.

Theorem 1.5.2 *For any integer $n \geq 3$,*

$$label\ :\mathbf{eq1-5-5-1} D_n = (n-1)(D_{n-1} + D_{n-2}). \tag{1.40}$$

Proof. Let $n \geq 3$ and $\mathcal{D}_n$ be the set of all derangements $a_1a_2\cdots a_n$ of $\{1, 2, \cdots, n\}$.

For each member $a_1a_2\cdots a_n$ of $\mathcal{D}_n$, we have $1 \leq a_n \leq n-1$. Then, it suffices to show that for each integer k with $1 \leq k \leq n-1$, the number of those members $a_1a_2\cdots a_n$ of $\mathcal{D}_n$ with $a_n = k$ is equal to $D_{n-1} + D_{n-2}$. As an example, without loss of generality, we will show that the number of those members $a_1a_2\cdots a_n$ of $\mathcal{D}_n$ with $a_n = 1$ is equal to $D_{n-1} + D_{n-2}$.

Let $\mathcal{D}'$ be the set those members $a_1a_2\cdots a_n$ of $\mathcal{D}_n$ with $a_n = 1$. There are two types of members in $\mathcal{D}'$:

Type 1: $a_1 = n$;

Type 2: $a_1 \neq n$.

It is quite obvious that the number of members of $\mathcal{D}'$ in type 1 is equal to D_{n-2}. It is also obvious that the number of members of $\mathcal{D}'$ in type 2 is equal to D_{n-1} by treating n as 1.

Thus $|\mathcal{D}'| = D_{n-2} + D_{n-1}$. The proof is then completed. □

Applying Theorem 1.5.1 or (1.40), we can deduce the following results.

Exercise 1.5.3 *Prove that for* $n \geq 2$,

$$label: \mathbf{eq1-5-5-2} D_n = nD_{n-1} + (-1)^n. \tag{1.41}$$

Exercise 1.5.4 *Find the values of* D_n *for all* $n = 2, 3, \cdots, 10$ *by (1.41).*

1.6 Euler φ-function

For any two positive integers a and b, let (a, b) denote the HCF of a and b, where HCF is the *highest common factor* of a and b. If $(a, b) = 1$, we say a and b are **coprime**.

Example 1.6.1 *label:* **exa1-6-1** *Determine all integers* k *in* $\{1, 2, 3, \cdots, 20\}$ *such that* $(k, 20) = 1$.

Solution. There are eight integers k in $\{1, 2, 3, \cdots, 20\}$ such that $(k, 20) = 1$, as shown below:

$$1, 3, 7, 9, 11, 13, 17, 19.$$

□

For any positive integer n, let $\varphi(n)$ denote the number of integers k in $\{1, 2, 3, \cdots, n\}$ such that $(k, n) = 1$, i.e., k and n are coprime. Thus $\varphi(20) = 8$.

The function $\varphi(n)$, called the *Euler φ-function*, was introduced by Swiss mathematician Leonard Euler (1707-1783).

Exercise 1.6.1 *label:* **exa1-6-2** *Determine* $\varphi(n)$ *for* $n = 5, 6, \cdots, 10$.

In this section, we shall find a formula for $\varphi(n)$.

Exercise 1.6.2 *label:* **exa1-6-3** *If* n *is prime, what is the value of* $\varphi(n)$*?*

Exercise 1.6.3 *label:* **exa1-6-4** *If* n *is prime, what is the value of* $\varphi(n^2)$*?*

Exercise 1.6.4 *label:* **exa1-6-5** *If* n *is prime and* k *is a positive integer, what is the value of* $\varphi(n^k)$*?*

Exercise 1.6.5 *label:* **exa1-6-6** *If* $n = p_1 p_2$*, where* p_1 *and* p_2 *are different prime numbers, what is the value of* $\varphi(n)$*?*

Exercise 1.6.6 *label:* **exa1-6-7** *If p_1 and p_2 are different prime numbers, is it true that $\varphi(p_1p_2) = \varphi(p_1)\varphi(p_2)$?*

Now we deduce a general formula for $\varphi(n)$. Let

$$label\ :\mathbf{eq1-6-1}n = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k} \tag{1.42}$$

be the unique decomposition of n as a product of prime powers, where $p_1, p_2, \cdots, p_m$ are prime numbers and $m_1, m_2, \cdots, m_k$ are positive integers.

Theorem 1.6.1 *label:* **th1-6-1** *For any positive integer n,*

$$label\ :\mathbf{eq1-6-2}\varphi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right), \tag{1.43}$$

where $p_1, p_2, \cdots, p_k$ are prime numbers determined in (1.42).

Proof. Let $S = \{1, 2, \cdots, n\}$. Define k properties $P_1, P_2, \cdots, P_k$: for any $i : 1 \le i \le k$,

$$x \in S \text{ is said to possess } P_i \iff p_i|x,$$

where $p_i|x$ means that x is divisible by p_i.

It is clear that x is coprime to n if and only if $p_i \not| x$ for all $i = 1, 2, \cdots, k$, i.e., x possesses none of properties $P_1, P_2, \cdots, P_k$. Therefore

$$\varphi(n) = E(0).$$

Observe that $\omega(0) = |S| = n$, and for $1 \le t \le k$,

$$\begin{aligned} label\ :\mathbf{eq1-6-3}\omega(t) &= \sum_{1\le i_1<i_2<\cdots<i_t\le k} \omega(P_{i_1}P_{i_2}\cdots P_{i_t}) \\ &= \sum_{1\le i_1<i_2<\cdots<i_t\le k} \left\lfloor \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_t}} \right\rfloor \\ &= \sum_{1\le i_1<i_2<\cdots<i_t\le k} \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_t}}. \end{aligned} \tag{1.44}$$

Hence, by Corollary 1.3.1,

$$label\ :\mathbf{eq1-6-4}\varphi(n) \;=\; E(0)$$

$$
\begin{aligned}
&= n + \sum_{t=1}^{k} (-1)^t \omega(t) \\
&= n + \sum_{t=1}^{k} (-1)^t \sum_{1 \le i_1 < i_2 < \cdots < i_t \le k} \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_t}} \\
&= n \left(1 + \sum_{t=1}^{k} (-1)^t \sum_{1 \le i_1 < i_2 < \cdots < i_t \le k} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_t}} \right) \\
&= n \left(1 + \sum_{t=1}^{k} \sum_{1 \le i_1 < i_2 < \cdots < i_t \le k} \left(\frac{-1}{p_{i_1}} \right) \left(\frac{-1}{p_{i_2}} \right) \cdots \left(\frac{-1}{p_{i_t}} \right) \right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i} \right), \qquad (1.45)
\end{aligned}
$$

as desired. □

Exercise 1.6.7 label: **exa1-6-8** *If $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \cdots, p_k$ are pairwisely different prime numbers, what is the value of $\varphi(n)$?*

Exercise 1.6.8 label: **exa1-6-9** *If $p_1, p_2, \cdots, p_k$ are pairwisely different prime numbers, is it true that*

$$
\varphi(p_1 p_2 \cdots p_k) = \varphi(p_1)\varphi(p_2) \cdots \varphi(p_k)?
$$

Problems of Chapter 1[1]

1. Determine the number of integers in $\{1, 2, 3, \cdots, 500\}$ which are multiples of $3, 5$ or 7.

2. Determine the number of integers in $\{1, 2, 3, \cdots, 1000\}$ which are multiples of $4, 6$ or 9.

3. Let p, q, r be three distinct prime numbers, and k be any positive integer. Determine the number of integers in $\{1, 2, 3, \cdots, kpqr\}$ which are multiples of p, q or r.

4. Let $S = \{1, 2, 3, \cdots, 400\}$. Let

   P_1 be the property that an integer is divisible by 2,

   P_2 be the property that an integer is divisible by 3, and

   P_3 be the property that an integer is divisible by 5.

   Find $\omega(0)$, $\omega(1)$, $\omega(2)$ and $\omega(3)$.

5. Let $S = \{1, 2, 3, \cdots, 400\}$. Determine the number of integers in S which are divisible by

   (a) none of $4, 6, 9$;

   (b) exactly one of $4, 6, 9$;

   (c) exactly two of $4, 6, 9$;

   (d) all of $4, 6, 9$.

6. (a) Let A, B and C be finite sets. Show that

   (i) $|\bar{A} \cap B| = |B| - |A \cap B|$;

   (ii) $|\bar{A} \cap \bar{B} \cap C| = |C| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

   (b) Find the number of integers in the set $\{1, 2, 3, 4, \cdots, 1000\}$ which are not divisible by 5 nor by 7 but are divisible by 3.

7. Find the number of integers in the set $\{100, 101, 102, \cdots, 1000\}$ which are divisible by exactly 'm' of the integers $2, 3, 5, 7$, where $m = 0, 1, 2, 3, 4$.

[1]Optional.

8. How many positive integers n are there such that n is a divisor of at least one of the numbers $10^{60}, 20^{50}$ and 30^{40}?

9. Find the number of integers in the set $\{1, 2, 3, 4, \cdots, 10000\}$ which are not of the form n^2 or n^3.

10. (a) How many arrangements of $a, a, a, b, b, b, c, c, c$ are there such that no three consecutive letters are the same?

    (b) How many arrangements of three 1's, three 2's, $\cdots$, and three k's are there such that no three consecutive numbers are the same?

11. Find the number of ways of arranging n couples $\{H_i, W_i\}$, $i = 1, 2, \cdots, n$, in a row such that H_i is not adjacent to W_i for each $i = 1, 2, \cdots, n$.

12. Let r and n be positive integers with $r \geq n$.

    (a) Find the number of ways of distributing r identical objects into n distinct boxes such that no box is empty.

    (b) Show that

$$\sum_{i=0}^{n-1} (-1)^i \binom{n}{i} \binom{r+n-i-1}{r} = \binom{r-1}{n-1}.$$

13. Let m, n and r be positive integers with $m \leq r \leq n$.

    (a) Let $A = \{1, 2, 3, \cdots, n\}$ and $B = \{1, 2, 3, \cdots, m\}$. Find the number of r-element sets C such that $B \subseteq C \subseteq A$.

    (b) Show that

$$\binom{n-m}{n-r} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{n-i}{r}.$$

14. (a) For any positive integer n, find the number of $0-1$ binary sequences of length n which do not contain '01' as a block.

    (b) Show that

$$n+1 = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \binom{n-i}{i} 2^{n-2i}.$$

15. n persons are to be allocated to q distinct rooms. Find the number of ways that this can be done if only m of the q rooms have exactly k persons each, where $1 \leq m \leq q$ and $mk \leq n$.

16. For any positive integer n, let C_n be the number of permutations of the set $\{1, 2, 3, \cdots, n\}$ in which k is never followed immediately by $k+1$ for each $k = 1, 2, \cdots, n-1$.

    (a) Find C_n;

    (b) Show that $C_n = D_n + D_{n-1}$.

17. Let m, n be positive integers with $m < n$. Find, in terms of D_k's, the number of derangements $a_1 a_2 \cdots a_n$ of $\{1, 2, \cdots, n\}$ such that

$$\{a_1, a_2, \cdots, a_m\} = \{1, 2, \cdots, m\}.$$

18. label: **try1** Let m and n be positive integers. Without using (1.43), show that if $m|n$, then

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

19. label: **try2** (a) Let p be a prime and $(p, n) = 1$. Show that $\varphi(pn) = (p-1)\varphi(n)$.

    (b) Let $p_1, p_2, \cdots, p_k$ be distinct prime numbers. Prove that

$$\varphi(p_1 p_2 \cdots p_k) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

20. By the results of Problems 18 and 19, show that for all positive integers m, n with $(m, n) = 1$,

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

21. Show that for any positive integer n,

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

22. Show that for any integer $n \geq 3$, $\varphi(n)$ is always even.