# 第一章　集合、映射与逻辑初步

## 1.7　拓展阅读：从星期到模 $m$ 剩余类环

### 1.7.1　集合的划分与等价关系

看 2010 年 3 月份的日历：

| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 31 | | | |

显然，“星期一”是由无穷多天组成的集合，“星期二”、……、“星期日”同理.

如何表示星期一这个集合呢？我们想到描述法，那么属于星期一的那些日子的特征是什么呢？为简化问题，我们将 2010 年 3 月 1 日对应到数 1，3 月 2 日对应到 2，$\cdots$，3 月 31 日对应到 31，……；把 2010 年 2 月 28 日对应到 0，2 月 27 日对应到 $-1$，2 月 26 日对应到 $-2$，$\cdots$. 这个对应法则是时间长河中的所有日子组成的集合到整数集 $\mathbb{Z}$ 的一个双射.

可以看出，星期日是由被 7 除后余数为 0 的整数组成的集合，星期一是由被 7 除后余数为 1 的整数组成的集合，$\cdots$，星期六是由被 7 除后余数为 6 的整数组成的集合，把这些子集依次记为 $H_0, H_1, H_2, \ldots, H_6$：

$$
\begin{aligned}
H_0 &= \{7k \mid k \in \mathbb{Z}\},\\
H_1 &= \{7k+1 \mid k \in \mathbb{Z}\},\\
H_2 &= \{7k+2 \mid k \in \mathbb{Z}\},\\
&\cdots \qquad\quad \cdots\cdots\\
H_6 &= \{7k+6 \mid k \in \mathbb{Z}\}.
\end{aligned}
$$

于是 $\mathbb{Z}$ 被分成了 7 个子集，且满足

$$\mathbb{Z} = H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5 \cup H_6 \cup H_0,\ \text{当} i \neq j \text{时},\ H_i \cap H_j = \varnothing$$

从这个例子抽象出下述概念：

**定义 1.7.1** (集合的划分)**.** 如果集合 $S$ 是它的一些非空子集的并集，其中每两个不相等的子集的交为空集（此时称它们不相交），那么把这些子集组成的集合称为 $S$ 的一个**划分**.

在上述例子中,$\{H_0, H_1, H_2, H_3, H_4, H_5, H_6\}$ 是整数集 $\mathbb{Z}$ 的一个划分.

我们自然要问, 如何给出任一集合 $S$ 的一个划分呢?

对于上述例子，两个整数 $a, b$ 属于同一个子集当且仅当它们模 7 同余。

任给两个整数 $a$ 与 $b$, 要么 $a$ 与 $b$ 模 7 同余, 要么 $a$ 与 $b$ 模 7 不同余, 二者必居其一且只居其一. 自然地，可以把模 7 同余称为整数集 $\mathbb{Z}$ 上的一个二元关系.

在数学上如何给出集合 $S$ 的二元关系的定义呢? 以 $\mathbf{Z}$ 上的模 7 同余关系为例, 既然要考察任意两个整数有没有这个关系, 自然要考虑所有有序整数对 $(a, b)$ 组成的集合 $\mathbb{Z} \times \mathbb{Z}$, 可知有下述结论:

$$a \equiv b (\mathrm{mod} 7) \iff (a, b) \in \bigcup_{i=0}^{6} H_i \times H_i,$$

$\bigcup_{i=0}^{6} H_i \times H_i$ 是 $\mathbb{Z} \times \mathbb{Z}$ 的一个子集,$(a, b)$ 属于这个子集就表明 $a$ 与 $b$ 有模 7 同余关系, 否则表明 $a$ 与 $b$ 没有模 7 同余关系. 我们干脆就把集合 $\bigcup_{i=0}^{6} H_i \times H_i$ 叫做 $\mathbb{Z}$ 上的模 7 同余关系. 由此抽象出下述概念:

**定义 1.7.2** (二元关系)**.** 设 $S$ 是一个非空集合, 把 $S \times S$ 的非空子集 $W$ 称为 $S$ 上的一个**二元关系**. 如果 $(a, b) \in W$, 那么称 $a$ 与 $b$ 有 $W$ 关系, 记做 $aWb$ 或 $a \sim b$, 否则称 $a$ 与 $b$ 没有 $W$ 关系.

$\mathbb{Z}$ 上的模 7 同余关系具有下述性质:

(1) $\forall a \in \mathbb{Z}, a \equiv a (\mathrm{mod} 7)$;

(2) 若 $a \equiv b (\mathrm{mod} 7)$, 则 $b \equiv a (\mathrm{mod} 7)$;

(3) 若 $a \equiv b (\mathrm{mod} 7)$ 且 $b \equiv c (\mathrm{mod} 7)$, 则 $a \equiv c (\mathrm{mod} 7)$.

由此引出下述概念:

**定义 1.7.3** (等价关系)**.** 集合 $S$ 上的一个二元关系 $\sim$ 如果具有下列性质:

1° : $a \sim a, \forall a \in S$ (**自反性/反身性**);

2° : 若 $a \sim b$, 则 $b \sim a$ (**对称性**);

3° : 若 $a \sim b$ 且 $b \sim c$, 则 $a \sim c$ (**传递性**),

那么称 $\sim$ 是 $S$ 上的一个**等价关系**.

$\mathbb{Z}$ 上的模 7 同余关系就是 $\mathbb{Z}$ 上的一个等价关系.

我们还能观察到: 星期一就是由与 1 模 7 同余的整数组成的子集,$\cdots$, 星期日是由与 0 模 7 同余的整数组成的子集. 由此受到启发, 引出下述概念:

**定义 1.7.4** (等价类)**.** 设 $\sim$ 是集合 $S$ 上的一个等价关系, 对于 $a \in S$, 集合 $\{x \in S \mid x \sim a\}$ 称为由 $a$ 确定的**等价类**, 记做 $\overline{a}$.

星期一、……、星期六、星期日就是 $\mathbb{Z}$ 在模 7 同余关系下的 7 个等价类:

$$\overline{0} = \{x \in \mathbb{Z} \mid x \equiv 0 (\mathrm{mod} 7)\} = \{7k \mid k \in \mathbb{Z}\}.$$

$$\overline{1} = \{x \in \mathbb{Z} \mid x \equiv 1(\mathrm{mod}7)\} = \{7k+1 \mid k \in \mathbb{Z}\},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\overline{6} = \{x \in \mathbb{Z} \mid x \equiv 6(\mathrm{mod}7)\} = \{7k+6 \mid k \in \mathbb{Z}\},$$

这 7 个等价类都叫做**模 7 剩余类**.

下面我们来探索等价类的性质. 设 $\sim$ 是集合 $S$ 上的一个等价关系.

**性质 1：** $a \in \overline{a}, \forall a \in S$.

由于性质 1, 可以把 $a$ 称为等价类 $\overline{a}$ 的一个**代表**.

**性质 2：** $x \in \overline{a} \iff x \sim a$.

**性质 3：** $\overline{x} = \overline{y} \iff x \sim y$.

由性质 2 和性质 3 得, 若 $x \in \overline{a}$, 则 $x \sim a$, 从而 $\overline{x} = \overline{a}$. 这表明 $\overline{a}$ 中任一元素 $x$ 都可以作为等价类 $\overline{a}$ 的代表.

**性质 4：**任给 $a, b \in S$, 则 $\overline{a}$ 与 $\overline{b}$ 或者相等, 或者不相交.

**问题 1.1** 尝试证明上述 4 个性质.

由性质 4 可以发现下述定理：

**定理 1** 设 $\sim$ 是集合 $S$ 上的一个等价关系, 则所有等价类组成的集合是 $S$ 的一个划分.

**问题 1.2** 尝试证明此定理

我们从星期一、……、星期六、星期日引出了等价类的概念. 通过探索等价类的性质, 发现并证明了定理 1. 这是数学思维方式的一个体现. 定理 1 给出了集合划分的一个统一的常用的方法, 即在集合 $S$ 上建立一个二元关系, 验证它是否为等价关系, 如果是等价关系, 那么所有等价类组成的集合是 $S$ 的一个划分. 反之, 如果给了集合 $S$ 的一个划分, 那么可以在 $S$ 上建立一个等价关系, 使得 $S$ 的这个划分就是由所有等价类组成的.

与模 7 同余关系类似, 给定 $m \in \mathbb{Z}, m > 1$, 可以在整数集 $\mathbb{Z}$ 上建立一个模 $m$ 同余关系：

$$a \equiv b(\mathrm{mod}m) \iff a - b \text{是} m \text{的整数倍}.$$

显然, 这是 $\mathbb{Z}$ 上的一个等价关系. 共有 $m$ 个等价类：

$$\overline{0} = \{x \in \mathbb{Z} \mid x \equiv 0(\mathrm{mod}m)\} = \{km \mid k \in \mathbb{Z}\},$$

$$\overline{1} = \{x \in \mathbb{Z} \mid x \equiv 1(\mathrm{mod}m)\} = \{km+1 \mid k \in \mathbb{Z}\},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\overline{m-1} = \{x \in \mathbb{Z} \mid x \equiv m-1(\mathrm{mod}m)\} = \{km+(m-1) \mid k \in \mathbb{Z}\},$$

它们都称为模 $m$ 剩余类. 集合

$$\{\overline{0},\overline{1},\ldots,\overline{m-1}\}$$

是 $\mathbb{Z}$ 的一个划分, 把这个集合记做 $\mathbb{Z}_m$.

观察：$23\equiv 2(\mathrm{mod}7), 10\equiv 3(\mathrm{mod}7)$,

$$23+10\equiv 2+3(\mathrm{mod}7),\quad 23\times 10\equiv 2\times 3(\mathrm{mod}7).$$

由此受到启发, 猜测模 $m$ 同余关系有下述性质：

**命题 1**　设 $m$ 是大于 1 的整数. 若 $a\equiv b(\mathrm{\ mod\ }m)$且$c\equiv d(\mathrm{\ mod\ }m)$, 那么 $a+c\equiv b+d(\mathrm{\ mod\ }m)$ 且 $ac\equiv bd(\mathrm{mod}m)$.

**问题 1.3**　请给出此命题的证明.

从命题 1 立即得到：若 $a\equiv b(\mathrm{mod}m)$, 则对任意整数 $c$ 有 $ca\equiv cb(\mathrm{mod}m)$.

**习题 1.1**

**1.** 在平面点集 $S$ 上定义一个二元关系：

$$P_1(x_1,y_1)\sim P_2(x_2,y_2)\iff x_1-x_2\in\mathbb{Z}\text{ 且}y_1-y_2\in\mathbb{Z}.$$

证明：$\sim$ 是 $S$ 上的一个等价关系.

**2.** 证明或反驳：若 $ca\equiv cb(\mathrm{mod}6)$, 则 $a\equiv b(\mathrm{mod}6)$.

### 1.7.2　模 $m$ 剩余类环 $\mathbb{Z}_m$, 环和域的概念

假设今天是星期五, 过了 181 天是星期几? 由于每过 7 天又是星期五,$181\equiv 6(\mathrm{mod}7)$,$5+6\equiv 4(\mathrm{mod}7)$, 因此过了 181 天是星期四.

星期五是 $\mathbb{Z}$ 的一个子集 $\overline{5}$；又有 $\overline{181}=\overline{6}$, 我们大胆地尝试如下计算：

$$\overline{5}+\overline{181}=\overline{5}+\overline{6}:=\overline{5+6}=\overline{4}$$

也得出, 过了 181 天是星期四.

由此受到启发, 我们规定模 $m$ 剩余类的加法：

$$\overline{a}+\overline{b}:=\overline{a+b}$$

这样的规定是否合理呢? 由于 $\overline{a},\overline{b}$ 的代表不唯一, 因此需要验证：若 $\overline{a}=\overline{c},\overline{b}=\overline{d}$, 是否有 $\overline{a+b}=\overline{c+d}$?

**问题 1.4**　请验证这种规定模 $m$ 剩余类的加法是合理的.

既然模 $m$ 剩余类可以做加法, 自然要问：它们能否做乘法呢? 运用类比的方法, 可以规定模 $m$ 剩余类的乘法：

$$\overline{a}\,\overline{b} = \overline{ab}$$

类似地可以证明：这个定义是合理的, 即与代表的选择无关.

这样, 我们在模 $m$ 剩余类组成的集合 $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ 中, 规定了加法和乘法两种运算. 模 $m$ 剩余类是 $\mathbb{Z}$ 的子集, 它们也能做加法和乘法, 这是数学上的一个创新点.

$\mathbb{Z}_m$ 中的加法和乘法满足哪些运算法则呢? 由于模 $m$ 剩余类的加法和乘法分别归结为它们的代表去做相加和相乘, 因此直觉判断 $\mathbb{Z}_m$ 的加法和乘法满足整数的加法和乘法的运算法则, 并且容易验证这一猜测是真的, 即 $\mathbb{Z}_m$ 的加法满足：交换律、结合律；$\overline{0}$ 具有下述性质：

$$\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}, \forall \overline{a} \in \mathbb{Z}_m$$

$\overline{0}$ 称为 $\mathbb{Z}_m$ 的零元；

对于 $\overline{a} \in \mathbb{Z}_m$, 有 $\overline{-a} \in \mathbb{Z}_m$, 使得

$$\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$$

$\overline{-a}$ 称为 $\overline{a}$ 的负元, 记做 $-\overline{a}$.

$\mathbb{Z}_m$ 的乘法满足交换律、结合律, 以及对加法的分配律, 并且

$$\overline{1}\,\overline{a} = \overline{a}\,\overline{1} = \overline{a}, \forall \overline{a} \in \mathbb{Z}_m,$$

$\overline{1}$ 称为 $\mathbb{Z}_m$ 的单位元.

$\mathbb{Z}_m$ 中还可以规定减法如下：

$$\overline{a} - \overline{b} := \overline{a} + (-\overline{b})$$

即减法通过加法来定义.

整数集 $\mathbb{Z}$, 模 $m$ 剩余类组成的集合 $\mathbb{Z}_m$, 它们都有加法和乘法两种运算, 并且满足上述运算法则.

所有偶数组成的集合记做 $2\mathbb{Z}$, 由于两个偶数的和、积仍是偶数, 因此 $2\mathbb{Z}$ 也有加法和乘法两种运算.$2\mathbb{Z}$ 中不存在一个偶数具有性质：与任一偶数的乘积等于那个偶数自身. 因此 $2\mathbb{Z}$ 中没有单位元. 上述其他运算法则在 $2\mathbb{Z}$ 中都成立.

整数集 $\mathbb{Z}$, 模 $m$ 剩余类集 $\mathbb{Z}_m$, 偶数集 $2\mathbb{Z}$ 有共同的特征：有加法和乘法两种运算, 并且满足加法的 4 条运算法则, 以及乘法的交换律、结合律, 乘法对加法的分配律. 我们由此抽象出现代数学的一个重要概念. 不过在此之前, 我们要先交代清楚：什么是集合上的运算?

$\mathbb{Z}$ 中的加法运算：$3 + 2 = 5$, 实质上是把有序整数对 $(3, 2)$ 对应到整数 5. 因此 $\mathbb{Z}$ 上的加法运算是 $\mathbb{Z} \times \mathbb{Z}$ 到 $\mathbb{Z}$ 的一个映射, 我们抓住这个主要特征, 抽象出运算的概念：

**定义 1.7.5** (运算)**.** 集合 $S$ 上的一个**二元代数运算**是指 $S\times S$ 到 $S$ 的一个映射.

**定义 1.7.6** (环)**.** 设 $R$ 是一个非空集合, 如果 $R$ 上定义了两个代数运算, 一个叫做加法, 另一个叫做乘法, 并且满足下列 6 条运算法则:

(1) $a+b=b+a,\forall a,b\in R$ **（加法交换律）**;

(2) $(a+b)+c=a+(b+c),\forall a,b,c\in R$ **（加法结合律）**;

(3) $R$ 中有一个元素 0, 且 $\forall a\in R, a+0=0+a=a$ （称 0 是 $R$ 的**零元**）;

(4) 任给 $a\in R$, 都有 $b\in R$ 使得 $a+b=b+a=0$, 把 $b$ 称为 $a$ 的**负元**, 记做 $-a$;

(5) $(ab)c=a(bc),\forall a,b,c\in R$ **（乘法结合律）**;

(6) $a(b+c)=ab+ac,(b+c)a=ba+ca,\forall a,b,c\in R$ **（乘法对加法的分配律）**.

那么称 $R$ 是一个**环（ring）**.

显然, $\mathbb{Z},\mathbb{Z}_m,2\mathbb{Z}$ 都是环. 称 $\mathbb{Z}$ 是整数环, 称 $\mathbb{Z}_m$ 是模 $m$ 剩余类环, 称 $2\mathbb{Z}$ 是偶数环.

环 $R$ 中可以定义减法运算如下:

$$a-b:=a+(-b)$$

如果环 $R$ 的乘法满足交换律, 那么称 $R$ 是**交换环**.$\mathbb{Z},\mathbb{Z}_m,2\mathbb{Z}$ 都是交换环.

如果环 $R$ 中有一个元素 $e$ 具有下述性质:

$$ea=ae=a,\quad \forall a\in R$$

那么称 $e$ 是 $R$ 的单位元, 此时 $R$ 是**有单位元的环**.

**问题 1.5**　证明: 在环 $R$ 中, 零元记为 0, 有 $0a=a0=0,\forall a\in R$

考虑模 4 剩余类环 $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$, 显然 $\overline{1}$ 是 $\mathbb{Z}_4$ 的单位元. 我们有

$$\overline{3}\cdot\overline{3}=\overline{9}=\overline{1}$$

由此受到启发, 引出下述概念:

**定义 1.7.7** (可逆元)**.** 设 $R$ 是有单位元 $e(\neq 0)$ 的环, 对于 $a\in R$, 如果存在 $b\in R$, 使得

$$ab=ba=e,\quad (16)$$

那么称 $a$ 是 $R$ 的一个**可逆元**, 把 $b$ 叫做 $a$ 的**逆元**, 记做 $a^{-1}$.

在 $\mathbb{Z}_4$ 中,$\overline{2}\cdot\overline{2}=\overline{4}=\overline{0}$. 由此受到启发, 引出下述概念.

**定义 1.7.8** (零因子)**.** 设 $R$ 是一个环, 对于 $a\in R$, 如果存在 $c\in R,\ c\neq 0$, 使得 $ac=0$ (或 $ca=0$), 那么称 $a$ 是 $R$ 的一个**左零因子（或右零因子）**. 左、右零因子统称为**零因子**.

可知 0 是零因子, 它被称为平凡零因子.

$\mathbb{Z}_4$ 中,$\overline{2}$ 是零因子, 由于

$$\overline{2}\cdot\overline{0}=\overline{0},\quad \overline{2}\cdot\overline{1}=\overline{2},\quad \overline{2}\cdot\overline{2}=\overline{0},\quad \overline{2}\cdot\overline{3}=\overline{6}=\overline{2}$$

因此 $\overline{2}$ 不是可逆元. 可猜测有下述命题：

**命题 1.7.9.** 设 $R$ 是有单位元 $e(\neq 0)$ 的环, 则 $R$ 的零因子不是可逆元.

**问题 1.6**　尝试证明此命题.

命题 2 的逆否命题同样成立：设 $R$ 是有单位元 $e(\neq 0)$ 的环, 则 $R$ 的可逆元不是零因子.

**问题 1.7**　请填写下表，求出 $\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_4,\mathbb{Z}_5,\mathbb{Z}_6,\mathbb{Z}_7$ 以及 $\mathbb{Z}$ 中的可逆元和零因子.

| 环 | 可逆元 | 不可逆元 | |
|---|---|---|---|
| | | 零因子 | 不是零因子 |
| $\mathbb{Z}_2$ | | | |
| $\mathbb{Z}_3$ | | | |
| $\mathbb{Z}_4$ | | | |
| $\mathbb{Z}_5$ | | | |
| $\mathbb{Z}_6$ | | | |
| $\mathbb{Z}_7$ | | | |
| $\mathbb{Z}$ | | | |

观察填表的结果, 我们猜想如下命题：

**命题 1.7.10.** 对于任意整数 $m>1$, 模 $m$ 剩余类环 $\mathbb{Z}_m$ 中每一个元素或者是可逆元, 或者是零因子, 二者必居其一, 且只居其一.[1]

从上面的表格看到：$\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_5,\mathbb{Z}_7$ 的非零元都是可逆元. 由此抽象出又一个重要的概念：

**定义 1.7.11** (域)**.** 设 $F$ 是一个有单位元 $e(\neq 0)$ 的交换环, 如果 $F$ 中每一个非零元都是可逆元, 那么称 $F$ 是一个**域（field）**.

例如,$\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_5,\mathbb{Z}_7$ 都是域；$\mathbb{Z}_4,\mathbb{Z}_6$ 不是域.

又如, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$, 复数集 $\mathbb{C}$ 都是域, 分别称它们为有理数域, 实数域, 复数域. 而整数环 $\mathbb{Z}$ 不是域.

如果域 $F$ 中的元素都属于复数集, 那么称 $F$ 是数域. 可以证明：最小的数域是有理数域. 显然, 最大的数域是复数域.

此外, 根据上述观察, 还可以猜测并证明下述命题：

**命题 1.7.12.** 若 $m$ 是合数, 则 $\mathbb{Z}_m$ 不是域.

[1]将在 1.7.4 中被证明其为真.

**问题 1.8** 给出该命题的证明.

从 $\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_5,\mathbb{Z}_7$ 都是域, 我们猜测有下述命题：

**命题 1.7.13.** 若 $p$ 是素数, 则 $\mathbb{Z}_p$ 是一个域, 称它为模 $p$ 剩余类域.

证明该命题需要搞清楚素数的特性, 于是我们考虑研究整数环的结构.

### 1.7.3 整数环的结构

整数集 $\mathbb{Z}$ 中没有除法运算, 但可以进行**带余除法**, 即小学讲的同时求解商与余数的除法.

**命题 1.7.14** (带余除法)**.** 任给 $a,b\in\mathbb{Z},\ b\neq 0$, 存在唯一的一对整数 $q,r$, 使得

$$a=qb+r,\quad 0\leqslant r<|b|.$$

式中的 $q$ 和 $r$ 分别称为 $a$ 被 $b$ 除所得的**商**和**余数**. 当 $r=0$ 时,$a$ 被 $b$ 除得尽, 由此引出整除的概念：

**定义 1.7.15** (整除)**.** 对于整数 $a,b$, 如果存在整数 $c$, 使得 $a=cb$, 那么称 $b$ **整除** $a$, 记做 $b\mid a$; 否则, 称 $b$ 不能整除 $a$, 记做 $b\nmid a$. 当 $b$ 整除 $a$ 时,$b$ 称为 $a$ 的一个**因数**,$a$ 称为 $b$ 的一个**倍数**.

**定义 1.7.16** (公因数)**.** 如果 $c\mid a$ 且 $c\mid b$, 那么称 $c$ 是 $a$ 与 $b$ 的一个公因数.

**定义 1.7.17** (最大公因数)**.** 对于整数 $a$ 与 $b$ 的一个公因数 $d$, 如果 $a$ 与 $b$ 的任一公因数都能整除 $d$, 那么称 $d$ 是 $a$ 与 $b$ 的一个**最大公因数**（Greatest Common Divisor）, 记为 $d=\gcd(a,b)$）.

当给出两个很大的正整数时, 难以直接找出它们的最大公因数, 因此需要探索一种统一规范的程式化方法. 我们不妨从带余除法入手, 探讨被除数与除数的最大公因数和除数与余数的最大公因数之间的关系.

**引理 1.7.18.** 如果在 $\mathbb{Z}$ 中有 $a=qb+r$, 那么 $d$ 是 $a$ 与 $b$ 的最大公因数当且仅当 $d$ 是 $b$ 与 $r$ 的最大公因数.

**证明.** 可知 $c\mid a$ 且$c\mid b$ 当且仅当 $c\mid b$ 且$c\mid r$, 设 $d$ 是 $a$ 与 $b$ 的一个最大公因数, 则 $d\mid b$ 且 $d\mid r$. 任取 $b$ 与 $r$ 的一个公因数 $c$, 则 $c\mid a$ 且 $c\mid b$. 于是 $c\mid d$. 因此 $d$ 也是 $b$ 与 $r$ 的一个最大公因数. 同理可证, 若 $d$ 是 $b$ 与 $r$ 的一个最大公因数, 则 $d$ 也是 $a$ 与 $b$ 的一个最大公因数. □

由上述引理结合带余除法即可得出求两个整数的最大公因数的方法：

**定理 1.7.19.** 任给两个整数 $a,b$, 都存在它们的一个最大公因数 $d$, 并且 $d$ 可以表示成 $a$ 与 $b$ 的倍数和, 即存在整数 $u,v$, 使得 $ua+vb=d$

**证明.** 如果 $b=0$, 那么 $a$ 是 $a$ 与 $0$ 的一个最大公因数. 下设 $b\neq 0$. 容易看出,$a$ 与 $b$ 的最大公因数是 $a$ 与 $-b$ 的最大公因数, 反之亦然. 于是不妨设 $b>0$. 据带余除法, 有整数 $q_1,r_1$, 使得 $a=q_1b+r_1,0\leqslant r_1<b$. 如果 $r_1\neq 0$, 那么用 $r_1$ 去除 $b$, 有整数 $q_2,r_2$, 使得 $b=q_2r_1+r_2,0\leqslant r_2<r_1$. 如果 $r_2\neq 0$, 再用 $r_2$ 去除 $r_1$. 如此辗转相除下去, 所得余数不断减

小, 因此在有限步以后, 必然有余数为 0. 设最后三步为：

$$r_{s-3}=q_{s-1}r_{s-2}+r_{s-1},\quad 0\leqslant r_{s-1}<r_{s-2},$$

$$r_{s-2}=q_sr_{s-1}+r_s,\quad 0\leqslant r_s<r_{s-1},$$

$$r_{s-1}=q_{s+1}r_s+0.$$

由于 $r_s$ 是 $r_s$ 与 0 的一个最大公因数, 因此从最后一个等式得出,$r_s$ 是 $r_{s-1}$ 与 $r_s$ 的一个最大公因数. 再从倒数第二个等式得出,$r_s$ 是 $r_{s-2}$ 与 $r_{s-1}$ 的一个最大公因数. 依次往上看, 最后得出,$r_s$ 是 $a$ 与 $b$ 的一个最大公因数.

从倒数第二个等式得出

$$r_s=r_{s-2}-q_sr_{s-1}.\quad (*)$$

用倒数第三个等式消去 (*) 式中的 $r_{s-1}$. 依次利用上面的等式可逐步消去 $r_{s-2},\dots,r_2,r_1$, 最后得出

$$r_s=ua+vb,$$

其中 $u,v$ 都是整数. □

定理 2 的证明给出了求两个整数的最大公因数的统一方法, 称为**辗转相除法**. 它是一种非常重要的算法, 有着广泛的应用.

**定义 1.7.20** (互素)**.** 设 $a,b\in\mathbb{Z}$, 如果 $(a,b)=1$, 那么称 $a$ 与 $b$ **互素**

**定义 1.7.21** (贝祖定理,Bézout's theorem)**.** 整数 $a$ 与 $b$ 互素当且仅当存在整数 $u,v$, 使得 $ua+vb=1$

**证明.** 必要性可从定理 2 立即得出. 下证明充分性。设 $ua+vb=1$ 成立, 任取 $a$ 与 $b$ 的一个公因数 $c$. 由于 $c\mid a$ 且 $c\mid b$, 因此 $c\mid ua+vb$, 即 $c\mid 1$. 从而 $c=\pm1$, 所以 $a$ 与 $b$ 互素　□

用贝祖定理来刻画两个整数互素的特征是非常有用的.

下面我们尝试推导互素整数的一些重要性质.

性质 1：在 $\mathbb{Z}$ 中, 如果 $a\mid bc$, 且 $(a,b)=1$, 那么 $a\mid c$.

性质 2：在 $\mathbb{Z}$ 中, 如果 $a\mid c,b\mid c$, 且 $(a,b)=1$, 那么 $ab\mid c$.

性质 3：在 $\mathbb{Z}$ 中, 如果 $(a,c)=1$, 且 $(b,c)=1$, 那么 $(ab,c)=1$.

运用数学归纳法可以把性质 3 推广为：在 $\mathbb{Z}$ 中, 如果 $(a_i,c)=1,i=1,2,\cdots,s$, 那么 $(a_1a_2\cdots a_s,c)=1$. 运用数学归纳法并且利用性质 3 的推广, 可以把性质 2 推广为：在 $\mathbb{Z}$ 中, 如果 $a_i\mid c,i=1,2,\cdots,s$ 且 $a_1,a_2,\cdots,a_s$ 两两互素, 那么 $a_1a_2\cdots a_s\mid c$.

素数在整数环的结构中起基本建筑块的作用. 下面分别从几个不同的角度来刻画素数的特征:

**定理 1.7.22.** 设 $p$ 是大于 1 的整数, 则下列命题等价：

(1) $p$ 是素数;

（2）对任意整数 $a$, 都有 $p \mid a$ 或 $(p,a)=1$;

（3）对于整数 $a,b$, 从 $p \mid ab$ 可以推出 $p \mid a$ 或 $p \mid b$;

（4）$p$ 不能分解成两个比 $p$ 小的正整数的乘积.

**证明.** 采用轮回证法：

(1) $\Longrightarrow$ (2)：**（补充此证明）**

(2) $\Longrightarrow$ (3)：

设 $p \mid ab$. 如果 $p \mid a$, 则命题得证. 否则,**（补充这一部分的证明）**, $p \mid b$

(3) $\Longrightarrow$ (4)：

假如 $p=p_1p_2, 0<p_1<p, 0<p_2<p$, 由整除的反身性得, $p \mid p_1p_2$

由 (3) 得：$p \mid p_1$ 或 $p \mid p_2$, 矛盾.

因此 $p$ 不能分解成两个比 $p$ 小的正整数的乘积.

(4) $\Longrightarrow$ (1)：

任取 $p$ 的一个正因数 $a$, 则存在正整数 $b$, 使得 $p=ba$.

由 (4) 得 $b=p, a=1$ 或 $a=p, b=1$.

因此 $p$ 的正因数只有 1 和 $p$, 从而 $p$ 是素数. □

从素数的等价条件 (4) 得知, 大于 1 的整数 $a$ 是合数当且仅当 $a$ 能分解成两个比 $a$ 小的正整数的乘积，如果这两个正整数中仍存在合数，则对之再次作分解，直到不能再分解为止，于是猜想对于任一大于 1 的整数 $a$, 它都可以被分解成有限多个素数的乘积。

**定理 1.7.23** (算术基本定理)**.** 任一大于 1 的整数 $a$ 都能唯一地分解成有限多个素数的乘积. 所谓唯一性指的是, 如果 $a$ 有两个分解式: $a=p_1p_2\cdots p_s=q_1q_2\cdots q_t$, 那么一定有 $s=t$, 并且适当排列因数的次序后, 有 $p_i=q_i(i=1,2,\cdots,s)$.

**证明.** 先证明可分解性。对大于 1 的整数 $n$ 用第二数学归纳法. 当 $n=2$ 时, 2 是素数, 命题为真. 假设对任意大于 1 且小于 $n$ 的整数, 命题为真, 现考虑整数 $n$, 如果 $n$ 是素数, 则命题为真. 如果 $n$ 是合数, 那么存在正整数 $n_1,n_2, 1<n_1<n_2<n$, 使得 $n=n_1n_2$ ，由归纳假设，$n_1$ 和 $n_2$ 分别能分解成有限多个素数的乘积. 从而 $n$ 能分解成有限多个素数的乘积。

再证明唯一性。假设 $a$ 有两个分解式 $a=p_1p_2\cdots p_s=q_1q_2\cdots q_t(*)$, 其中 $p_i$ 和 $q_j(i=1,2,\cdots,s, j=1,2,\cdots,t)$ 都是素数. 对 $a$ 的第一个分解式中素数的个数 $s$ 作数学归纳法.

当 $s=1$ 时, $a=p_1$. 于是 $p_1=q_1q_2\cdots q_t$. 从而 $q_1 \mid p_1$. 由于 $p_1$ 是素数, 因此 $q_1=p_1$, 从而 $a=p_1=q_1$. 命题为真. 假设 $s-1$ 时命题为真, 看 $s$ 的情形. 可知 $p_1 \mid q_1q_2\cdots q_t$. 由于 $p_1$ 是素数, 因此对某个 $j\in\{1,2,\cdots,t\}$ $p_1 \mid q_j$, 不妨设 $p_1 \mid q_1$. 由于 $q_1$ 是素数, 因此 $p_1=q_1$. 于是 $(*)$ 式两边可消去 $p_1$, 得

$$p_2\cdots p_s=q_2\cdots q_t$$

由归纳假设，$s-1=t-1$, 且适当排列因数的次序后, 有 $p_i=q_i, i=2,\cdots,s$. 因此 $s=t$, 且 $p_i=q_i, i=1,2,\cdots,s$, 唯一性得证.

□

算术基本定理刻画了整数环的结构:，它指出，任一大于 1 的整数 $a$ 能唯一地写成

$$a = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

其中 $p_1, p_2, \cdots, p_m$ 是两两不等的素数, $r_i$ 是正整数, $i = 1, 2, \cdots, m$. 这称为 $a$ 的标准分解式.

## 习　题

**1.** 证明：对一切正整数 $n$, 都有 $8 \mid 9^n - 1$

**2.** 证明：对一切正整数 $n$, 都有 $3 \mid n(n+1)(n+2)$.

**3.** 分别求下列各组中两个整数的正的最大公因数, 并且把它表示成这两个整数的倍数和:

（1）126 与 99；（2）183 与 567；（3）1023 与 31；（4）127 与 2047.

**4.** 证明：如果 $a$ 与 $b$ 是不全为 0 的整数, 那么 $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$.

**5.** 证明: 在 $\mathbb{Z}$ 中, 若 $(a,b) = 1$, 则 $(a, a+b) = 1$, 且 $(ab, a+b) = 1$.

**6.** 写出下列整数的标准分解式: $234, 678, 2345$.

### 1.7.4　$\mathbb{Z}_m$ 的可逆元判定, 模 $p$ 剩余类域, 域的特征, 费马小定理

**问题 1.9**　观察**问题 1.29** 的填表结果, 猜测在模 $m$ 剩余类环 $\mathbb{Z}_m$ 中, 当 $a$ 与 $m$ 有什么关系时, $\overline{a}$ 是 $\mathbb{Z}_m$ 的可逆元? 当 $a$ 与 $m$ 有什么关系时, $\overline{a}$ 是 $\mathbb{Z}_m$ 的零因子?

从上述问题受到启发, 我们可以提出并证明下述定理：

**定理 1.7.24.** 在模 $m$ 剩余类环 $\mathbb{Z}_m$ 中, $\overline{a}$ 是可逆元当且仅当 $a$ 与 $m$ 互素.

**证明.** 先证充分性。设 $a$ 与 $m$ 互素, 则存在整数 $u, v$ 使得 $ua + vm = 1$，即 $\overline{u} \cdot \overline{a} + \overline{v} \cdot \overline{m} = \overline{1}$, 而 $\overline{v} \cdot \overline{m} = \overline{0}$, 从而 $\overline{u} \cdot \overline{a} = \overline{1}$, 于是 $\overline{u}$ 是 $\overline{a}$ 的逆元.$\overline{a}$ 是可逆元。

再证必要性。设 $\overline{a}$ 是 $\mathbb{Z}_m$ 的可逆元, 其中 $0 < a < m$。用反证法，假设 $a$ 与 $m$ 不互素, 设它们的一个公因数为 $d > 1$，则存在整数 $n_1, n_2$ 使得 $n_1 d = a, n_2 d = m$，于是 $n_1 n_2 d = n_2 a = n_1 m$，即 $\overline{n_2} \cdots \overline{n_1} = \overline{n_1} \cdot \overline{m} = \overline{0}$，所以 $\overline{a}$ 是零因子，这与 $\overline{a}$ 是可逆元矛盾. 因此 $a$ 与 $m$ 互素. □

从定理 1 的充分性的证明看到：若 $a$ 与 $m$ 互素, 则 $\overline{a}$ 是可逆元. 从定理 1 的必要性的证明看到：设 $0 < a < m$, 若 $a$ 与 $m$ 不互素, 则 $\overline{a}$ 是零因子, 于是立即得到：

**定理 1.7.25.** $\mathbb{Z}_m$ 的每一个元素或者是可逆元, 或者是零因子.

设 $p$ 是素数, 则对于 $0 < k < p$, 有 $p \nmid k$, 从而 $k$ 与 $p$ 互素. 于是在 $\mathbb{Z}_p$ 中, 每个非零元 $\overline{k}$ 都可逆, 因此我们证明了下述定理

**定理 1.7.26.** 若 $p$ 是素数, 则 $\mathbb{Z}_p$ 是域

定理 1 充分性的证明给出了当 $a$ 与 $m$ 互素时, 求 $\overline{a}$ 的逆元的方法：对 $a$ 和 $m$ 用辗转相除法求出它们的正最大公因数 1, 然后把 1 表示成 $a$ 与 $m$ 的倍数和, 据此得到 $\overline{a}$ 的逆元.

在环 $R$ 中有加法运算, 据此可定义元素 $a$ 的正整数倍.

**定义 1.7.27.** 对于任一正整数 $n$, 规定 $a$ 的 $n$ 倍为：$na := \underbrace{a+a+\cdots+a}_{n\text{个}}$

设 $a \in R, n, m \in \mathbb{N}^*$, 由上述定义可推导出：

$$(n+m)a = na + ma, (nm)a = n(ma)$$

$$n(a+b) = na + nb, n(ab) = (na)b = a(nb)$$

对于自然数 0, 可以定义 $a$ 的 0 倍为：$0a = 0$, 其中等号右边的 0 是环 $R$ 中的零元.

下面来讨论模 $p$ 剩余类域 $\mathbb{Z}_p$ 与数域的不同点.
在 $\mathbb{Z}_2$ 中, $2\overline{1} = \overline{1} + \overline{1} = \overline{2} = \overline{0}$
在 $\mathbb{Z}_3$ 中, $3\overline{1} = \overline{1} + \overline{1} + \overline{1} = \overline{3} = \overline{0}$; $2\overline{1} = \overline{2} \neq \overline{0}$
设 $p$ 是素数, 则在 $\mathbb{Z}_p$ 中, 有 $p\overline{1} = \overline{p} = \overline{0}$, 当 $0 < l < p$ 时,$l\overline{1} = \overline{l} \neq \overline{0}$
在数域 $K$ 中, 对于任意正整数 $n$, 都有 $n1 = n \neq 0$, 只有 1 的 0 倍等于 0.
我们可以探索：任一域 $F$, 它的单位元 $e$ 的正整数倍是否等于零元？有什么规律?

**情形 1：**对任意正整数 $n$, 都有 $ne \neq 0$.
**情形 2：**存在正整数 $n$, 使得 $ne = 0$, 并设 $n$ 是使 $ne = 0$ 成立的最小正整数.
假如 $n$ 不是素数, 则 $n = n_1 n_2, 1 < n_1 < n, 1 < n_2 < n$, 于是有

$$\begin{aligned}(n_1e)(n_2e) &= n_1[e(n_2e)] = n_1[n_2(ee)] = n_1(n_2e) = (n_1n_2)e \\ &= ne = 0.\end{aligned}$$

而 $n_1e \neq 0$ 且 $n_2e \neq 0$, 于是 $n_1e$ 是零因子, 从而 $n_1e$ 不是可逆元, 这与 $F$ 是域矛盾, 因此 $n$ 是素数.

于是证明了下述定理：

**定理 1.7.28.** 设域 $F$ 的单位元为 $e$, 则或者对任意正整数 $n$, 都有 $ne \neq 0$；或者存在一个素数 $p$, 使得 $pe = 0$, 而对于 $0 < l < p$, 有 $le \neq 0$

从该定理受到启发, 引出下述重要概念

**定义 1.7.29** (域的特征)**.** 设域 $F$ 的单位元为 $e$, 如果对任意正整数 $n$, 都有 $ne \neq 0$, 那么称域 $F$ 的**特征**为 0；如果存在一个素数 $p$, 使得 $pe = 0$, 而对于 $0 < l < p$, 有 $le \neq 0$, 那么称域 $F$ 的**特征**为 $p$, 域 $F$ 的特征记做 $\mathrm{char}F$.

据定理 4, 任一域 $F$ 的特征或者为 0, 或者为一个素数, 例如模素数 $p$ 剩余类域 $\mathbb{Z}_p$ 的特征为 $p$, 任一数域的特征为 0, 这就是 $\mathbb{Z}_p$ 与数域的本质区别.

在特征为素数 $p$ 的域 $F$ 中, 单位元 $e$ 的 $p$ 倍等于零元, 我们自然要问: 任一元素 $a$ 的 $p$ 倍是否也等于零元?

**命题 1.7.30.** 设域 $F$ 的特征为素数 $p$, 则对 $F$ 中任一元素 $a$, 都有 $pa = 0$.

**证明.** 设 $F$ 的单位元为 $e$, 则 $pa = p(ea) = (pe)a = 0a = 0$ □

在特征为素数 $p$ 的域 $F$ 中, 由于任一元素的 $p$ 倍都等于 0, 因此可以简化计算.

**问题 1.10** 证明: 在 $\mathbb{Z}_3$ 中, 元素 $\overline{a}, \overline{b}$ 满足

$$(\overline{a} + \overline{b})^3 = \overline{a}^3 + \overline{b}^3$$

由此受到启发, 提出下述命题:

**命题 1.7.31.** 设域 $F$ 的特征为素数 $p$, 则对于任意 $a, b \in F$, 有

$$(a + b)^p = a^p + b^p$$

**证明.** 由于域 $F$ 具有与实数域同样的运算规则, 因此在域 $F$ 中也有二项式定理:

$$(a + b)^p = a^p + \mathrm{C}_p^1 a^{p-1} b + \cdots + \mathrm{C}_p^k a^{p-k} b^k + \cdots + \mathrm{C}_p^{p-1} a b^{p-1} + b^p$$

其中 $\mathrm{C}_p^k = \dfrac{p(p-1)\cdots(p-k+1)}{k!}, 1 \leqslant k < p$. 当 $1 \leqslant k < p$ 时, 有 $(k!, p) = 1$, 由于 $\mathrm{C}_p^k \in \mathbb{Z}$, 则 $k! \mid p(p-1)\cdots(p-k+1)$, 因此

$$k! \mid (p-1)\cdots(p-k+1), 1 \leqslant k < p$$

可得

$$p \mid C_p^k \quad 1 \leqslant k < p$$

即

$$(a + b)^p = a^p + b^p$$

□

**例 2** $2^{97}$ 模 97 同余于几? $90^{97}$ 模 97 同余于几?

**解:** 97 是素数, 于是域 $\mathbb{Z}_{97}$ 的特征为 97. 在 $\mathbb{Z}_{97}$ 中有

$$\overline{2^{97}} = \overline{2}^{97} = (\overline{1} + \overline{1})^{97} = \overline{1}^{97} + \overline{1}^{97} = \overline{1} + \overline{1} = \overline{2}$$

$$\overline{90^{\overline{97}}}=\overline{90}^{97}=(\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{90\text{ 个}})^{97}=\underbrace{\overline{1}^{97}+\overline{1}^{97}+\cdots+\overline{1}^{97}}_{90\text{ 个}}=\overline{90}$$

可得

$$2^{97}\equiv 2 \pmod{97}, 90^{97}\equiv 90 \pmod{97}$$

从例 2 受到启发, 可以猜测并证明下述定理：

**定理 1.7.32** (费马小定理（Fermat's Little Theorem）)**.** 设 $p$ 是素数, 则对于任意整数 $a$, 都有

$$a^p\equiv a \pmod{p}$$

**证明.** 若 $p\mid a$, 则 $a\equiv 0 \pmod{p}$ 且 $a^p\equiv 0 \pmod{p}$, 从而 $a^p\equiv a \pmod{p}$

下面设 $p\nmid a$, 作带余除法，$a=hp+r, 0<r<p$，在 $\mathbb{Z}_p$ 中, 有 $\overline{a}=\overline{hp+r}=\overline{r}$，由于 $\mathbb{Z}_p$ 的特征为 $p$, 因此

$$\begin{aligned}\overline{a}^p=\overline{r}^p&=(\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{r\text{ 个}})^p=\underbrace{\overline{1}^p+\overline{1}^p+\cdots+\overline{1}^p}_{r\text{ 个}}\\&=\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{r\text{ 个}}=\overline{r}=\overline{a}\end{aligned}$$

即 $a^p\equiv a \pmod{p}$ □

**1.** 分别写出 $\mathbb{Z}_{18},\mathbb{Z}_{36}$ 的所有可逆元和所有零因子.

**2.** 在 $\mathbb{Z}_{86}$ 中,$\overline{3},\overline{35}$ 是不是可逆元？如果是, 分别求它们的逆元.

**3.** 在 $\mathbb{Z}_{89}$ 中, 求 $\overline{2},\overline{86}$ 的逆元；在 $\mathbb{Z}_{113}$ 中, 求 $\overline{36},\overline{48}$ 的逆元.

**4.** 设 $F$ 是特征为 2 的域, 任给 $a,b\in F$, 计算：$(a+b)^2,(a+b)^4,(a+b)^8$, 由此你能猜测 $(a+b)^{2^n}$ 等于多少吗？你能证明这个猜测是真的吗?

**5.** 求 $2010^{79} \bmod 79, 2010^{127} \bmod 127$.

**6.** 设域 $F$ 的特征为素数 $p$, 证明：对任意 $a_1,a_2,\cdots,a_s\in F$, 有

$$(a_1+a_2+\cdots+a_s)^p=a_1^p+a_2^p+\cdots+a_s^p$$

（提示：使用数学归纳法）

### 1.7.5　中国剩余定理

设这个连有 $x$ 名战士, 按照上述已知条件, 得 $\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 4 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$ (1)

这样的方程组叫做一次同余方程组. 如何解这种一次同余方程组呢? 它有多少解呢?

一般地, 设 $m_1, m_2, \cdots, m_s$ 是两两互素的大于 1 的整数,$b_1, b_2, \cdots, b_s$ 是任意给定的整数, 考虑一次同余方程组: $\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots \\ x \equiv b_s \pmod{m_s}. \end{cases}$ (2)

我们来探索如何求同余方程组 (2) 的解? 它有多少解?

由于 $m_1, m_2, \cdots, m_s$ 两两互素, 因此对于 $i \in \{1, 2, \cdots, s\}$, 有

$$\left(m_i, \prod_{j \neq i} m_j\right) = 1,$$

从而存在 $u_i, v_i \in \mathbb{Z}$, 使得

$$u_i m_i + v_i \prod_{j \neq i} m_j = 1.$$

由上式得到

$$v_i \prod_{j \neq i} m_j = 1 - u_i m_i$$

从而有

$$\begin{cases} v_i \prod\limits_{j \neq i} m_j \equiv 1 \pmod{m_i}, \\ v_i \prod\limits_{j \neq i} m_j \equiv 0 \pmod{m_k}, \quad k \neq i. \end{cases}$$

由于同余方程组 (2) 的解应当满足模 $m_i$ 同余于 $b_i (i = 1, 2, \cdots, s)$, 因此, 令

$$c = b_1 v_1 \prod_{j \neq 1} m_j + \cdots + b_i v_i \prod_{j \neq i} m_j + \cdots + b_s v_s \prod_{j \neq s} m_j$$

则

$$c \equiv b_1 \cdot 0 + \cdots + b_i \cdot 1 + \cdots + b_s \cdot 0 \equiv b_i \pmod{m_i}$$

其中 $i = 1, 2, \cdots, s$. 因此, 由 (7) 式定义的 $c$ 是同余方程组 (2) 的一个解.

若 $d$ 也是同余方程组 (2) 的一个解, 则

$$c \equiv d \pmod{m_i}, \quad i = 1, 2, \cdots, s$$

从而

$$m_i \mid c - d, \quad i = 1, 2, \cdots, s$$

由于 $m_1, m_2, \cdots, m_s$ 两两互素, 因此

$$m_1 m_2 \cdots m_s \mid c - d,$$

由此得出

$$c \equiv d \pmod{m_1 m_2 \cdots m_s}$$

上述的探索过程发现并且证明了下述定理:

**定理 1.7.33** (中国剩余定理)**.** 设 $m_1, m_2, \cdots, m_s$ 是两两互素的大于 1 的整数, 则对于任意给定的整数 $b_1, b_2, \cdots, b_s$, 一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots \\ x \equiv b_s \pmod{m_s}. \end{cases}$$

在 $\mathbb{Z}$ 中有解, 它的全部解是

$$c + k m_1 m_2 \cdots m_s, \quad k \in \mathbb{Z}$$

其中

$$c = b_1 v_1 \prod_{j \neq 1} m_j + b_2 v_2 \prod_{j \neq 2} m_j + \cdots + b_s v_s \prod_{j \neq s} m_j$$

$v_i$ 满足 $u_i m_i + v_i \prod\limits_{j \neq i} m_j = 1, i = 1, 2, \cdots, s.$

从定理 1 看出, 为了求一次同余方程组 (12) 的全部解, 需要先求出 $v_i (i = 1, 2, \cdots, s)$, 而这只要对 $m_i$ 和 $\prod\limits_{j \neq i} m_j$ 作辗转相除法, 并且把它们的最大公因数 1 表示成它们的倍数和, 此时 $\prod\limits_{j \neq i} m_j$ 的倍数就是 $v_i$.

我国南宋数学家秦九韶在他的著作《数书九章》卷一“大衍总数术”中, 系统地叙述了求解一次同余方程组的一般方法, 其关键部分就是求 (14) 式中的 $v_i(i=1,2,\cdots,s)$. 秦九韶把他自己发现的求 $v_i$ 的方法称为“大衍求一术”, 实际上就是做辗转相除法.

秦九韶的算法是正确的, 但他本人没有给出证明. 而欧拉和高斯分别在 1743 年、1801 年对一次同余方程组进行了详细研究, 重新独立地获得与秦九韶“大衍求一术”相同的定理, 并对模数两两互素的情形作出了严格证明. 1876 年德国人马蒂生首先指出秦九韶的方法与高斯算法是一致的, 因此, 关于一次同余方程组求解的剩余定理通常被称为“中国剩余定理”.

### 习题 1.5

**1.** 设 $m_1$ 和 $m_2$ 是互素的大于 1 的整数,$b$ 是任意给定的一个整数. 证明：整数 $a$ 满足 $\begin{cases} a\equiv b \pmod{m_1}, \\ a\equiv b \pmod{m_2} \end{cases}$ 的充分必要条件是 $a\equiv b \pmod{m_1m_2}$.

### 1.7.6　$\mathbb{Z}_m$ 的可逆元的个数, 欧拉函数

我们之前证明了：在模 $m$ 剩余类环 $\mathbb{Z}_m$ 中,$\overline{a}$ 是可逆元当且仅当 $a$ 与 $m$ 互素. 把 $\mathbb{Z}_m$ 中所有可逆元组成的集合记做 $\mathbb{Z}_m^*$, 我们首先要问：$\mathbb{Z}_m^*$ 有多少个元素?

**定义 1.7.34** (欧拉函数)**.** 设 $m$ 是大于 1 的整数, 把 $\mathbb{Z}_m$ 中可逆元的个数记做 $\varphi(m)$, 称 $\varphi(m)$ 为**欧拉函数**.

可知, $\varphi(m)$ 等于集合 $\Omega_m=\{1,2,3,\cdots,m\}$ 中与 $m$ 互素的整数的个数.

**问题 1.11**　填写下表.

| $m$ | $1\sim m$ 中与 $m$ 互素的整数 | $\varphi(m)$ |
|---|---|---|
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 12 | | |
| 15 | | |
| 24 | | |

观察填写后的表, 当 $m$ 为素数 $2,3,5,7$ 时,$\varphi(m)$ 的值有何规律?

由此受到启发, 猜测且容易证明下述命题：

**命题 2**　若 $p$ 是素数, 则 $\varphi(p)=p-1$.

**问题 1.12**　观察上表中 $\varphi(4)=\varphi(2^2),\varphi(8)=\varphi(2^3),\varphi(9)=\varphi(3^2)$ 的值, 你能作出什么猜测?

**定理 1.7.35.** 设 $p$ 是素数, 对任意正整数 $r$, 有

$$\varphi(p^r)=p^{r-1}(p-1)$$

**问题 1.13**　完成该定理的证明.（提示：考虑 $1,2,\cdots,p^r$ 中与 $p^r$ 不互素的数的个数。）

**问题 1.14**　回答下述问题：

（1）$\varphi(6)$ 与 $\varphi(2)\varphi(3)$ 相等吗?

（2）$\varphi(15)$ 与 $\varphi(3)\varphi(5)$ 相等吗?

（3）$\varphi(12)$ 与 $\varphi(2)\varphi(6)$ 相等吗? $\varphi(3)\varphi(4)$ 呢?

（4）$\varphi(24)$ 与 $\varphi(4)\varphi(6)$ 相等吗? $\varphi(3)\varphi(8)$ 呢?

（5）设 $m=m_1m_2,m_1,m_2$ 是大于 1 的整数, 如果 $\varphi(m)=\varphi(m_1)\varphi(m_2)$, 猜测 $m_1,m_2$ 应该满足什么关系?

猜测有下述结论：

设 $m=m_1m_2$, 且 $m_1$ 与 $m_2$ 是互素的大于 1 的整数, 则 $\varphi(m)=\varphi(m_1)\varphi(m_2)$

这个猜测是真是假? 我们来探索.

$\varphi(m_1)$ 是 $\mathbb{Z}_{m_1}$ 中可逆元的个数,$\varphi(m_2)$ 是 $\mathbb{Z}_{m_2}$ 中可逆元的个数.$\varphi(m_1)\varphi(m_2)$ 是什么呢?

一个创新的想法是考虑集合 $\mathbb{Z}_{m_1}$ 与 $\mathbb{Z}_{m_2}$ 的笛卡儿积：

$$\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}=\{(\widetilde{a}_1,\widetilde{\widetilde{a}}_2)\mid\widetilde{a}_1\in\mathbb{Z}_{m_1},\widetilde{\widetilde{a}}_2\in\mathbb{Z}_{m_2}\}$$

并规定它的加法和乘法运算如下：

$$(\widetilde{a}_1,\widetilde{\widetilde{a}}_2)+(\widetilde{b}_1,\widetilde{\widetilde{b}}_2):=(\widetilde{a}_1+\widetilde{b}_1,\widetilde{\widetilde{a}}_2+\widetilde{\widetilde{b}}_2)$$

$$(\widetilde{a}_1,\widetilde{\widetilde{a}}_2)(\widetilde{b}_1,\widetilde{\widetilde{b}}_2):=(\widetilde{a}_1\widetilde{b}_1,\widetilde{\widetilde{a}}_2\widetilde{\widetilde{b}}_2)$$

容易验证 $\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}$ 称为一个有单位元 $(\widetilde{1},\widetilde{\widetilde{1}})$ 的交换环, 把这个环叫做环 $\mathbb{Z}_{m_1}$ 与 $\mathbb{Z}_{m_2}$ 的直和, 记做 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$.

**问题 1.15**　解答下述问题：

（1）证明：$(\widetilde{a}_1,\widetilde{\widetilde{a}}_2)$ 是 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元当且仅当 $\widetilde{a}_1,\widetilde{\widetilde{a}}_2$ 分别是 $\mathbb{Z}_{m_1},\mathbb{Z}_{m_2}$ 的可逆元.

（2）据第（1）问, 证明：$\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元的个数等于 $\varphi(m_1)\varphi(m_2)$

上述结论给出了 $\varphi(m_1)\varphi(m_2)$ 一个结构性解释, 这是一个创新点.

既然待证等式的右端是 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元的个数, 左端是 $\mathbb{Z}_m$ 的可逆元的个数, 我们自然要研究环 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 与环 $\mathbb{Z}_m$ 的关系.

首先建立 $\mathbb{Z}_m$ 的元素与 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的元素之间的对应关系.

容易想到, 令

$$\begin{aligned}\sigma : \mathbb{Z}_m &\longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \\ \overline{x} &\longmapsto (\widetilde{x}, \widetilde{\widetilde{x}})\end{aligned}$$

**问题 1.16** 解答下述问题：

（1）验证 $\sigma$ 是 $\mathbb{Z}_m$ 到 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的一个映射.

（2）证明：$\sigma$ 是双射；

（3）证明：$\forall x, y \in \mathbb{Z}_m$, 有

$$\sigma(\overline{x} + \overline{y}) = \sigma(\overline{x}) + \sigma(\overline{y}), \sigma(\overline{xy}) = \sigma(\overline{x})\sigma(\overline{y})$$

这称为 $\sigma$ 保持加法和乘法运算.

**定义 2 （环同构）** 如果环 $R$ 到环 $R'$ 有一个双射 $\sigma$, 且 $\sigma$ 保持加法和乘法运算, 那么称 $\sigma$ 是环 $R$ 到 $R'$ 的一个**同构映射**, 此时称环 $R$ 与环 $R'$ 是**同构**的, 记做 $R \cong R'$.

从上面的讨论得出：

**定理 3** 设 $m = m_1 m_2$, 且 $m_1$ 与 $m_2$ 是互素的大于 1 的整数, 则 $\sigma : \overline{x} \longmapsto (\overline{x}, \tilde{\tilde{x}})$ 是环 $\mathbb{Z}_m$ 到 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的一个同构映射, 从而环 $\mathbb{Z}_m$ 与 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 同构.

利用环 $\mathbb{Z}_m$ 到 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的同构映射 $\sigma$ 可以探讨 $\mathbb{Z}_m$ 的可逆元与 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的可逆元之间的关系.

$$\begin{aligned}&\overline{x} \text{ 是} \mathbb{Z}_m \text{ 的可逆元} \\ \Longleftrightarrow\ &\text{存在} \overline{b} \in \mathbb{Z}_m, \text{ 使得} \overline{x}\overline{b} = \overline{1} \\ \Longleftrightarrow\ &\text{存在} \overline{b} \in \mathbb{Z}_m, \text{ 使得} \sigma(\overline{1}) = \sigma(\overline{x}\overline{b}) = \sigma(\overline{x})\sigma(\overline{b}) \\ \Longleftrightarrow\ &\sigma(\overline{x}) \text{ 是} \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \text{ 的可逆元.}\end{aligned}$$

上述表明：$\sigma$ 诱导了 $\mathbb{Z}_m^*$ 到 $(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2})^*$ 的一个双射. 于是 $|\mathbb{Z}_m^*| = |(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2})^*|$. 因此,$\varphi(m) = \varphi(m_1)\varphi(m_2)$. 这样我们证明了前面作出的猜测是真的, 即

**定理 4** 设 $m = m_1 m_2$, 且 $m_1$ 与 $m_2$ 是互素的大于 1 的整数, 则 $\varphi(m) = \varphi(m_1)\varphi(m_2)$.

我们证明定理 4 的方法是运用现代数学研究结构和态射（即保持运算的映射）的观点, 第一步证明 $\varphi(m_1)\varphi(m_2)$ 是环 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的可逆元的个数；第二步建立环 $\mathbb{Z}_m$ 到 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的一个映射 $\sigma : \overline{x} \longmapsto (\overline{x}, \tilde{\tilde{x}})$, 证明 $\sigma$ 是满射, 从而 $\sigma$ 是单射, 于是 $\sigma$ 是双射；且证明 $\sigma$ 保持加法和乘法运算, 因此 $\sigma$ 是环 $\mathbb{Z}_m$ 到 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的一个同构映射. 由此得出,$\overline{a}$ 是 $\mathbb{Z}_m$ 的可逆元当且仅当 $\sigma(\overline{a})$ 是 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ 的可逆元.

**问题 1.17** 设 $m = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$, 其中 $p_1, p_2, \dots, p_s$ 是两两不等的素数, 证明：

$$\varphi(m) = p_1^{r_1 - 1}(p_1 - 1) p_2^{r_2 - 1}(p_2 - 1) \dots p_s^{r_s - 1}(p_s - 1)$$

并求 $\varphi(360)$ 的值.

**习题 1.6**

**1.** 写出 $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ 的所有可逆元, 并分别求出 $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}, \mathbb{Z}_{27} \oplus \mathbb{Z}_{49}$ 的可逆元的个数.

**2.** 设 $\sigma : \overline{x} \longmapsto (\overline{x}, \tilde{\tilde{x}})$ 是 $\mathbb{Z}_{100}$ 到 $\mathbb{Z}_4 \oplus \mathbb{Z}_{25}$ 的一个映射. 求 $\mathbb{Z}_4 \oplus \mathbb{Z}_{25}$ 中的元素 $(\overline{3}, \tilde{\tilde{7}})$ 在 $\sigma$ 下的原像.

**3.** 求 $\varphi(100), \varphi(225), \varphi(56), \varphi(60), \varphi(1360), \varphi(420)$.

**4.** 设大于 1 的正整数 $m = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$, 其中 $p_1, p_2, \dots, p_s$ 是两两不等的素数. 证明:

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right)$$

**5.** 设 $\sigma : \overline{x} \longmapsto (\overline{x}, \tilde{\tilde{x}})$ 是 $\mathbb{Z}_{15}$ 到 $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ 的一个映射, 写出 $\mathbb{Z}_{15}$ 的每个元素在 $\sigma$ 下的像.

### 1.7.7　$\mathbb{Z}_m$ 的单位群 $\mathbb{Z}_m^*$, 欧拉定理, 循环群及其判定

这一节我们来研究 $\mathbb{Z}_m$ 的可逆元组成的集合 $\mathbb{Z}_m^*$ 的结构.

**问题 1.18**　写出 $\mathbb{Z}_{12}^*$ 的元素, 并验证 $\mathbb{Z}_{12}$ 的加法和乘法是否为 $\mathbb{Z}_{12}^*$ 的运算.

**问题 1.19**　对 $\mathbb{Z}_m^*$ 做如下验证:

(1) $\mathbb{Z}_m$ 乘法是 $\mathbb{Z}_m^*$ 的运算;

(2) $\mathbb{Z}_m$ 乘法满足结合律和交换律;

(3) $\mathbb{Z}_m^*$ 中有单位元;

(4) $\mathbb{Z}_m^*$ 中每个元素都有逆元.

这使我们抽象出下述概念:

**命题 1.7.36** (群)**.** 设 $G$ 是一个非空集合. 如果在 $G$ 上定义了一种代数运算, 通常称为乘法, 并且它满足下列条件:

(1) $(ab)c = a(bc), \forall a, b, c \in G$ (结合律);

(2) $G$ 中有一个元素 $e$ 使得 $ea = ae = a, \forall a \in G$, 称 $e$ 是 $G$ 的**单位元**;

(3) 对于 $a \in G$, 存在 $b \in G$, 使得 $ab = ba = e$, 称 $a$ **可逆**, 此时称 $b$ 是 $a$ 的**逆元**, 记做 $a^{-1}$,

那么称 $G$ 是一个**群 (group)**.

如果群 $G$ 的运算还满足交换律, 那么称 $G$ 是**交换群** (或**阿贝尔 (Abel) 群**).

如果群 $G$ 只含有有限多个元素, 那么称 $G$ 是**有限群**; 否则称 $G$ 是**无限群**. 有限群 $G$ 所含元素的个数称为 $G$ 的**阶**, 记做 $|G|$.

在群 $G$ 中, 规定

$$a^n := \underbrace{aa\dots a}_{n}, n \in \mathbb{N}^*$$

$$a^0 := e$$

$$a^{-n} := (a^{-1})^n, n \in \mathbb{N}^*$$

容易验证：

$$a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}$$

其中 $n, m$ 是任意整数.

在交换群 $G$ 中,

$$(ab)^n = a^n b^n, n \in \mathbb{Z}$$

在非交换群中上面这个式子不成立.

由上面的讨论知道,$\mathbb{Z}_m^*$ 是有限交换群, 称它为 $\mathbb{Z}_m$ 的单位群.$\mathbb{Z}_m^*$ 的阶为 $\varphi(m)$.

**问题 1.20**　对于 $\mathbb{Z}_9$, 填写下方的表格, 你观察到了什么规律?

| $\overline{a}$ | $\overline{a}^2$ | $\overline{a}^3$ | $\overline{a}^4$ | $\overline{a}^5$ | $\overline{a}^6$ |
|---|---|---|---|---|---|
| $\overline{1}$ | | | | | |
| $\overline{2}$ | | | | | |
| $\overline{4}$ | | | | | |
| $\overline{5}$ | | | | | |
| $\overline{7}$ | | | | | |
| $\overline{8}$ | | | | | |

由上表可看出,$\mathbb{Z}_9^*$ 中每个元素的 6 次方都等于 $\overline{1}$. 由此受到启发, 猜想有下述结论：

**命题 1.7.37.** 设 $G$ 是 $n$ 阶交换群, 则对任意 $a \in G$, 有 $a^n = e$, 其中 $e$ 是 $G$ 的单位元.

**证明.** 设 $G = \{g_1, g_2, \ldots, g_n\}$, 其中 $g_1 = e$.

任取 $G$ 的元素 $g$. 为出现 $g^n$, 用 $g$ 乘 $G$ 的每个元素得 $gg_1, gg_2, \ldots, gg_n \in G$.

对 $i \neq j$, 假如 $gg_i = gg_j$, 则 $g^{-1}(gg_i) = g^{-1}(gg_j)$, 从而 $(g^{-1}g)g_i = (g^{-1}g)g_j$, 由此得出 $g_i = g_j$, 矛盾. 因此当 $i \neq j$ 时,$gg_i \neq gg_j$.

令 $S = \{gg_1, gg_2, \ldots, gg_n\}$, 有 $|S| = n$, 而 $S \subseteq G$, 因此 $S = G$.

故

$$(gg_1)(gg_2)\cdots(gg_n) = g_1 g_2 \cdots g_n$$

由于 $G$ 是交换群, 因此可改写上式左侧

$$g^n g_1 g_2 \cdots g_n = g_1 g_2 \cdots g_n$$

两边右乘 $(g_1 g_2 \cdots g_n)^{-1}$, 得 $g^n e = e$. 从而 $g^n = e$.

□

命题 1 的证明中用到 $G$ 是交换群这一条件. 但这不等于说：当 $G$ 是非交换群时, 命题 1 的结论一定不成立. 事实上, 采用其他的方法可以证明对于非交换群, 命题 1 的结论也成立.

利用命题 1 可以立即得到著名的欧拉定理：

**命题 1.7.38** (欧拉定理)**.** 设 $m$ 是大于 1 的正整数, 如果整数 $a$ 与 $m$ 互素, 那么

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

**证明.** 由 $(a,m)=1$ 可得 $\overline{a} \in \mathbb{Z}_m^*$.

由于 $|\mathbb{Z}_m^*| = \varphi(m)$, 据命题 1 有 $\overline{a}^{\varphi(m)} = \overline{1}$, 从而 $\overline{a^{\varphi(m)}} = \overline{1}$. 于是 $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

从问题 1.39 中的表可知：在 $\mathbb{Z}_9^*$ 中,

$$\overline{2}^6 = \overline{1}, \overline{2}^l \neq \overline{1}, 当1 \leqslant l < 6$$

$$\overline{4}^3 = \overline{1}, \overline{4}^l \neq \overline{1}, 当1 \leqslant l < 3$$

由此受到启发, 引出下述概念：

**定义 1.7.39.** 设 $G$ 是一个群, 对于 $a \in G$, 如果存在正整数 $n$ 使得 $a^n = e$, 那么称 $a$ 是**有限阶元素**, 使 $a^n = e$ 成立的最小正整数 $n$ 称为 $a$ 的**阶**, 记做 $|a|$；如果对于任意正整数 $n$ 都有 $a^n \neq e$, 那么称 $a$ 是**无限阶元素**.

当 $G$ 是交换群时, 常常把 $G$ 的运算记成**加法**. 此时 $G$ 的单位元也称为**零元**, 记成 0；元素 $a$ 的逆元称为 $a$ 的**负元**, 记成 $-a$；元素 $a$ 的 $n$ 次幂成为 $a$ 的 $n$ 倍, 记成 $na$, 即 $na := \underbrace{a+a+\cdots+a}_{n个}, n \in \mathbb{N}^*$.$a$ 的 0 倍规定为零元,$(-n)a := n(-a), n \in \mathbb{N}^*$.

**问题 1.21**　写出问题 1.39 中 $\mathbb{Z}_9^*$ 各元素的阶. 你发现了什么

由此猜测有下述结论：

**命题 1.7.40.** 群 $G$ 中, 如果元素 $a$ 的阶为 $n$, 那么

$$a^m = e \iff n \mid m$$

**证明. 充分性:** 设 $n \mid m$, 则 $m = kn, k \in \mathbb{Z}$, 于是 $a^m = a^{kn} = (a^n)^k = e^k = e$.

**必要性:** 设 $a^m = e$. 对 $m$ 和 $n$ 作带余除法：

$$m = kn + r, 0 \leqslant r < n$$

则 $e = a^m = a^{kn+r} = a^{kn}a^r = a^r$. 由于 $a$ 的阶为 $n$, 因此 $r = 0$. 从而 $n \mid m$.

□

从问题 1.39 的表中可以发现：在 $\mathbb{Z}_9^*$ 中,

$$\overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{8}, \overline{2}^4 = \overline{7}, \overline{2}^5 = \overline{5}, \overline{2}^6 = \overline{1}$$

因此

$$\mathbb{Z}_9^* = \{\overline{2}, \overline{2}^2, \overline{2}^3, \overline{2}^4, \overline{2}^5, \overline{2}^6\}$$

由此受到启发, 引出下述概念：

**定义 1.7.41** (循环群)**.** 如果群 $G$ 中有一个元素 $a$, 使得 $G$ 的每一个元素都能写成 $a$ 的方幂的形式, 那么称 $G$ 是**循环群**, 把 $a$ 叫做 $G$ 的一个**生成元**, 此时可以把 $G$ 记成 $\langle a \rangle$.

**问题 1.22** 回答下述问题：

（1）$\mathbb{Z}_9^*$ 是不是循环群？如果是, 请写出它的所有生成元；

（2）设 $G$ 是有限群, 如果 $G$ 中有一个元素 $a$, 使得 $a$ 的阶等于 $|G|$, 那么 $G$ 是循环群,$a$ 是 $G$ 的一个生成元；

（3）设 $G$ 是有限循环群, 则 $a$ 是 $G$ 的生成元当且仅当 $a$ 的阶等于 $|G|$.

（4）循环群一定是交换群吗？交换群一定是循环群吗？

### 习题 1.7

**1.** 写出 $\mathbb{Z}_{18}^*$ 的所有元素, 并且计算每两个元素的乘积.

**2.** 分别计算 $\mathbb{Z}_{13}^*, \mathbb{Z}_{24}^*$ 的每个元素的 $l$ 次方,$1 \leqslant l \leqslant 8$, 并且说出每个元素的阶是多少?

**3.** 设 $n = 17 \times 23, a = 3$, 求正整数 $b (b < n)$, 使得 $ab \equiv 1 \pmod{\varphi(n)}$.

**4.** 在第 3 题中, 设 $\overline{x} \in \mathbb{Z}_n^*$, 证明：$\overline{x}^{ab} = \overline{x}$.

**5.** 分别求出循环群 $\mathbb{Z}_7^*, \mathbb{Z}_{11}^*$ 的所有生成元.

**6.** 分别求出循环群 $\mathbb{Z}_{13}^*, \mathbb{Z}_{17}^*, \mathbb{Z}_{19}^*$ 的生成元的个数.

**7.** $\mathbb{Z}_{18}^*$ 是不是循环群？如果是, 它的一个生成元是什么？求 $\mathbb{Z}_{18}^*$ 的每个元素的阶, 并且写出它的所有生成元.

**8.** $\mathbb{Z}_{27}^*$ 是不是循环群？如果是, 求出它的所有生成元.

**9.** 利用欧拉定理证明费马小定理.

**10.** 群 $G$ 中, 元素 $a$ 的阶为 $n$, 证明：对于任意整数 $k$, 有 $|a^k| = \dfrac{n}{(n,k)}$.

**11.** 群 $G$ 中, 设 $a, b$ 的阶分别为 $n, m$, 且 $ab = ba$, 且 $(n, m) = 1$, 证明：$ab$ 的阶等于 $nm$.

**12.** 设 $G$ 为有限交换群, 证明：$G$ 中有一个元素的阶是其他元素的阶的倍数.

**13.** 设 $S \subseteq \mathbb{C}$ 是有限集，满足 $|S| = k$ 且对任意 $a, b \in S$ 有 $ab \in S$。

(1) 求证：$\forall a \in S : a^k = 1$；

(2) 求 $S$ 中所有元素之和。

# 拓展阅读：英雄时代的落幕

数学, 一个不需要现实实验验证, 仅靠一张纸和一支笔, 就能在逻辑推演中, 构建出完整理论体系的学科, 竟然能一路从结绳记事发展到今天这个样子, 既然这就是数学的特性, 所有定理和概念都能一步步往前找到理论来源, 而且不用操心现实因素, 那所有学过数学的人, 脑子里就会自然而然出现一个观念, 我们可不可以用一套完备而自洽的数学语言, 把全部数学知识和数学问题都完整的表达组织并证明呢, 数学家说, 哎, 你不能光盯着那些抽象概念而不把地基打牢, 大放厥词啊, 那至少一加一等于二, 这种自然数算术问题的底层基础, 不可能混乱吧, 是不可能混乱吧是不可能混乱吧, 各位不要慌, 自然数算术的地基, 当然不会混乱, 它根本从来就没有过地基, 被这 100 年来的, 这种将整个数学视为逻辑延伸的观念, 成为了我们今天要说的 20 世纪数学危机中, 登场的第一个也是思想最悠久的派系, 逻辑主义,

那想让逻辑主义者的目标真正达成, 首先就要确保目前数学里各个领域不存在模棱两可的悖论, 罗素从小就崇拜康托尔和他的集合论, 但罗素长大之后, 发现了朴素集合论里, 有着一个明显的悖论, 如果有一个集合, 它的元素是所有不包含自身的集合, 那么这个集合自身是否属于它的元素

罗素为了方便给外行人解释这个悖论, 还用了理发师做过例子, 这种悖论会出现的根本原因, 就是它产生了一种叫做自指的现象, 一个命题在否定它自身, 最简单的表述就是, 我这句话是错的, 这种悖论是不可能通过逻辑学内部定律和推导消除的, 如何解决这种简单粗暴的悖论呢? 答案可能出乎大家意料, 罗素悖论本身根本就不是什么大事, 光罗素自己一个人就提出了好几种消除它的方式, 自指设的问题不就出在自己会指自己吗, 我们直接规定不能指不就行了吗。罗素提出的其中一个方法叫做类型论, 就是给对象分层, 只有更高一层的东西可以指低层的东西, 不准同层互指。同在 20 世纪早期的策梅洛和弗伦克尔, 还借着解决罗素悖论的这个由头, 把康托尔的朴素集合论整理成了公理化集合论, 这个名字以策梅洛和弗伦克尔的名字首字母命名, 简称 ZF, 再加上后来融入的选择公理, 叫作 ZFC 公理系统。这个系统其实是一个毫无数学美感的东西, 它就像一堆不相关的砖头砌成的一堵墙, 每个砖头分别是一个公理, 同时这些公理分别都在防止一些问题的产生, 以及确保约定的合法, 比如这个 C 砖头本来就是一个无法证明, 且当时很多人不接受的观点, 但是策梅洛发现没它很麻烦, 所以咔一下就气上来了, 变成一个公理, 所以这堵墙只有你接不接受的问题, 没有什么证明它对不对的问题, 这个系统就是目前现代数学, 最广泛接受的默认基础, 从幼儿园到研究生的数学教育, 都是在承认它的前提上进行的, 虽然依然有不完美的地方, 但已经是如今数学, 兼顾全局下的最佳选择了,ZFC 这个规则外, 也直接通过一条分离公理, 强行禁止了罗素悖论的构造, 所以这个悖论本身, 到这里已经没有什么存在感了。

20 世纪发生过一场影响深远的数学危机, 它将导致数学界长期被分裂成三个阵营。逻辑主义希望将过往几千年数学成果纳入一个极端复杂的逻辑体系，它的这一努力在数学界遇到的最成建制的反对者就是直觉主义, 他们被称为一群激进而纯粹的疯子。直觉主义的精神来源可以追溯到克罗内克, 虽然他在各种讲述集合论的历史科普中都扮演着一个彻头彻尾的反面龙套, 但他在学术上, 他在代数和数论领域非常强大, 他打压康托尔也主要是因其从始至终都无法接受无穷集合的存在, 克罗内克的观点后来被布劳威尔所继承。直觉主义认为，数学是人类心智的活动, 只有人类心智所能把握能构造的对象才算真正的数学对象,19 世纪下半叶以

来，数学变得越来越像是逻辑和符号的游戏，康托尔把实无穷作为一个客观存在的数学对象，击穿了他们内心最后的防线，更别说接受拿无穷大去比较大小了。理由可以归结为一句质问，闭上眼睛，你觉得你的大脑真的能想象出来，宇宙中有无穷多个星体这句话吗，你哪怕有再丰富的想象力，你的心智所能把握的场景也只是成千上万，最多是一后面跟几十上百个零，但是你不可能真正的感知出实无穷，直觉主义另一个旗帜鲜明的立场是，他们不接受对涉及无穷的问题证明中，仅用反证法来证明某物存在，也就是说他们不接受非构造性的证明。

传统的数学里一直有一个不可撼动的逻辑定律，叫做排中律，即一个命题要么为真，要么为假，不存在第三种情况，反证法即是脱胎于此规律。直觉主义者不允许使用排中律来证明涉及无穷的存在性问题，难道数学命题可以是真或假以外的第三种状态吗，他们说：“可以。排中律预设了命题从诞生那天开始就具备一个明确的真假性。”在涉及无限对象的问题中，应该存在这样一种命题，在构造性证明出现之前，没人有权断言它的真假性，不知道本身是一种合法的数学状态。承认一些命题就是未知的，以及抵制排中律这两件事，还像话吗，回忆一下我们从小到大，数学这门课贯彻一个什么思想。于是第三个派系正式出现了，以希尔伯特为核心的形式主义，也是三股势力里最强大的派系。希尔伯特认为：“禁止数学家用排中律，就像在拳击比赛中禁用拳头一样。”

本着敌人的敌人，就是朋友的观点，希尔伯特和罗素的工作，几乎能归到同一个阵营里，但希尔伯特还是非常明确的和逻辑主义划清了借鉴和罗素的工作几乎跪到同一个阵营里但希尔伯特还是非常明确的，和逻辑主义划清了借鉴，因为罗素的野性，是要把数学彻底还原到逻辑层面上，一下一等于二这种东西，都不应该被当作原始对象，但希尔伯特自认为，自己没有那么魔争，他只要证明，整个数学是确定且一致的，就可以了，所以希尔伯特就像一个,16 到 19 世纪常见的，有神论科学家一样，相信有一套最高的法则在天上，但是各种科学实验还是要在学科领域内讨论的，但罗素在这里就像一个神学家，他试图要把所有物质所有定律，全都一路还原到他们全是上帝创造的。希尔伯特觉得没必要把逻辑学放到万物本源那个地位，所以当时的数学界就形成了，这样一种三足鼎立的状态，这三个势力没一个省油的灯，但是当年确实存在势力上的不对等，当时的希尔伯特，已经不是年轻的时候，只能看着前辈康托尔，受克罗内克欺负而无能威力的年轻人了，他现在已经成长为德国乃至整个欧洲地区的数学霸主了，而且就是在我们熟悉的哥廷根大学

所以直觉主义与逻辑和形式主义的争论，在数学史上又被称为布劳威尔—希尔伯特之争，虽然无论是希尔伯特，还是此刻大部分的观众朋友，都觉得直觉主义坚持的立场很没道理，其实他们也有苦衷，因为如果真的让逻辑主义和形式主义，为所欲为，接受存在但不可构造的对象的话，数学就会出现很多，现实世界无法接受的结论，比如前文提到的选择公理，选择公理，它会导致巴拿赫—塔斯基悖论，这个悖论简要说就是，集合论能够证明出存在一种方式，但是给不出这种方式，把一个普通的三维实心球进行切割，平移和旋转，变成两个和原来大小密度质量，完全一样的实心球，数学里是完全成立的，如果这事真能做到我们就可以把一颗石子变成一实心球数学里是完全成立的如果这事真能做到，我们就可以把一颗石子，变成一颗星球了，直觉主义者认为，这就是把数学，仅仅当做纯粹的逻辑与符号游戏要付出的代价，问题在于，如果数学真的和现实世界毫无关系，只是一套自我封闭的符号系统，那么就很难解释这样一个历史事实，自中世纪以来，数学为什么能在力学，天文学，电磁学，乃至现代物理的发展中，

反复展现出惊人的有效性, 所以说, 直觉主义者并非单纯的反对逻辑或形式化, 而是在提醒所有人, 数学之所以有存在的必要, 能成为科学里有意义的语言, 恰恰是因为, 它在某种程度上, 仍然保留着与人类直觉, 构造过程, 以及现实可操作性的联系, 而且也正是希尔伯特本人, 在他著名的 23 个问题中, 也留下了一个与此密切相关的要求, 希尔伯特第六问题要求将物理学公理化, 用严格的数学公理体系为物理学奠基, 这个问题本身恰恰默认了一个前提, 数学并不是一套与现实毫无关联的纯符号游戏, 而应该能够为现实世界的基本规律, 提供清晰、稳定且可理解的结构框架, 这才是第三次数学危机真正的分歧点——一场关于数学为何存在, 未来又要走向何处的深刻反思, 各个阵营在这场持续的争论和对抗中, 不断催生出各种新的思想与技术成果, 而它对现代数学发展所造成的最直观的影响, 却不是在数学范畴里, 甚至不是在科学范畴里, 只是一个社会学层面的改变。

在 20 世纪初, 数学领域里正式出现了具有核心领袖和共同纲领的学派。虽然必须承认数学是一个依赖于天才推动的学科, 但只寄希望于可遇不可求的天才来推动一个地区或民族的数学视野是不可能的。试想，如果牛顿在没有费马巴罗和加利略开普勒指引的情况下, 以近乎从零开始的状态, 独自一个人写出了数学原理, 但他的身后没有大学, 没有皇家学会, 同时也没有任何一个普通的数学家, 也许不出一代人, 整个欧洲就没有人能看懂这本书, 这些晦涩的数学推导不久就将失传, 牛顿的出身与否对欧洲的数学发展将不会有任何影响, 最多是在几百年后被人

到了 19 世纪末, 数学的复杂性已经不再允许一个人通晓它的全部领域, 数学研究不可避免的走向分工与协作, 在第三次数学危机的历史背景下, 希尔伯特在哥廷根系统性地组织起一个现代意义上的数学共同体, 即后来的哥廷根学派。此前近 200 年的数学史几乎被英法两国所垄断, 而在希尔伯特的推动下, 数学研究的重心逐渐转移到德国, 高斯和黎曼固然是划时代的天才, 但真正具有历史决定性意义的, 是一个成建制可持续运作的学派, 他不再完全依赖于天才的出现, 而是拥有持续生产, 改变数学面貌之人的能力。希尔伯特为了稳固德国在世界数学版图中的话语权, 团结了一切可以团结的力量, 他呼吁放下民族与性别的偏见, 把注意力重新集中在数学问题上, 正是在希尔伯特这样的理念支持下, 历史上最伟大的女数学家诺特才得以在重重制度性阻碍下进入数学界核心, 尽管她因学术界深入骨髓的性别歧视长期无法获得正式教职, 但她的成就的重要性并未因此而减弱, 她在理论物理中提出了诺特定理, 第一次从严格的数学层面揭示了对称性与守恒定律之间的深刻对应关系, 成为了现代物理最底层的核心之柱。诺特并不仅仅是一位天才的个体, 围绕她形成的研究共同体——诺特学派, 培养出了一大批深刻影响 20 世纪数学走向的数学家, 它使得抽象代数从一门零散的技巧集合成长为一套高度统一的理论体系, 诺特是真正意义上的抽象代数之母, 伽罗瓦和阿贝尔是我们前文所述的那种不世出的天才, 而艾米 · 诺特是将抽象代数学科化建制化的第一人。

然而好景不长, 第一次世界大战所造成的深层社会创伤在停战后的 20 年间持续发酵, 使德国乃至整个欧洲社会逐步走向一种难以调和的紧张局面。1933 年，希特勒上台, 纳粹随即开始在国内进行种族清洗, 同年 4 月 13 日, 哥廷根数学世界的乌托邦时代宣告结束, 包括诺特在内的大量学者在纳粹的迫害下流亡海外, 希尔伯特竭力维护哥廷根的学术传统, 却依然无力回天。在时代的暴力面前, 再伟大的学者也只是历史巨轮下微小而无助的个体, 清洗一年之后, 重病在身的希尔伯特参加了一场德国政界的宴会, 学术清洗的始作俑者之一, 纳粹德国的教育

部长鲁斯特问希尔伯特：“哥廷根数学研究所真的因为这场清洗而遭受很大损失吗?”

希尔伯特回答道：“受损？它已经不存在了。”

希尔伯特于二战期间去世，他去世时，哥廷根大学已经在纳粹的控制下全面重组，曾经的哥廷根学派也不复存在。希尔伯特葬礼的出席者不足十人，直到数月之后，其他国家的数学家们才陆续得知，这位 20 世纪初世界数学中心的缔造者，竟然在无人知晓的情况下，死在了他曾亲手建设并寄予厚望的哥廷根。

希尔伯特出生于东普鲁市省的哥尼斯堡，这里是欧拉研究图论[2]的起源地，同时也是康德的故乡。康德出生的时代，数学在解释世界如何运作这个问题上，获得了前所未有的成功，但另一方面，形而上学却陷入了无休止的争论. 康德发现，围绕某些问题所形成的两种不同的理论和学说，在同样的理性框架下各自成立，但却相互矛盾，比如假设宇宙的时间有一个开端，那么开端之前，就不会存在变化，也就不可能有动机，去产生这样的第一刻，但是如果宇宙的时间，没有开端，那就意味着，在现在之前已经过去了无限长的时间，但无限长的时间不可能一步一步走完，所以现在不可能到达，这种通过理性推导出两种对立结论的现象叫做二律背反，康德敏锐地意识到，出现这种问题的原因是人们滥用了自己的理性，于是他写下了纯粹理性批判，第一次系统地划定了理性的边界，向人们宣布，人类的认知能力具有不可逾越的节骨心限制，这个世界上有些超越经验的问题，人的理性是无法认知的。

一百多年后，希尔伯特站在了康德的对立面，在他所处的时代，人类改造和认识世界的能力已远非康德时代所能想象。康德为理性划定了不可逾越的边界，希尔伯特纲领则试图证明这种边界在数学中并不存在。他在柯尼斯堡演讲的最后，坚定有力地说出来最后一句话

*Wir müssen wissen, wir werden wissen.*

我们必须知道，我们必将知道。

然而，生命并不总是以伟大而有决定意义的诗句告终的。

几乎在希尔伯特发表柯尼斯堡演讲的同时，有一项研究工作完成了，其作者叫哥德尔，这一工作证明了希尔伯特纲领在原则上不可能成立，其结论被称为哥德尔不完备定理，从罗素悖论可以得知，击碎一个逻辑体系的最简便方式就是建立自指问题，但数学问题在现实语境中总会被模糊的语意和新的规约所消解，所以哥德尔帮希尔伯特完成了一个工作，他把推理和命题本身变成了可以被数学精确处理的对象。所有的数学命题都可以写成符号形式，哥德尔给每个符号指派了一个自然数作为其编码，为了确定这几个数字的位置，哥德尔把这几个符号的编码，依次放在从二开始的质数的乘方上，最后把它们乘起来，因为一个数字的质因数分解是唯一的，所以这个大数在技术上，可以和质数乘方的乘积等价替换，这种和命题一一对应的天文数字叫做哥德尔数，它第一次让数学里的所有命题落入了只由自然数构成的世界之中，到这一步为止，所有事情的发展都在希尔伯特的设想之中，每一个命题都被分配了一段和它自身意义无关的身份编码，命题在一边，数字在另一边，两者互不干扰，只要这种关系不被打破，数学就仍然是安全的，不能让某一个命题在系统内部说出属于他自己的那串编号，因为一旦发生这种情形，命题就不再只是被描述的对象，而会开始参与对自身的判断，希尔伯特极力避免的

[2]即哥尼斯堡七桥问题。

情形, 恰恰是哥德尔这篇论文, 真正的致命一击。在经过一系列极端繁琐而谨慎的形式构造后, 哥德尔最终在论文里写下了一条, 叫做 17 Gen r 的命题, 希尔伯特竭力回避的噩梦, 终于在这个系统内部合法的降临, 一个命题在镜子里看到了自己, 哥德尔数等于计的命题无法被证明, 这一命题, 他自己的哥德尔数等于计哥德尔就此证明这一命题他自己的哥德尔数等于计, 哥德尔就此证明了, 任何一个一致的形式系统, 只要其表达能力足以涵盖皮亚诺算术, 就可以在其中构造, 在体系中不能被证明的真命题, 因此, 通过推理演绎, 不能得到所有真命题, 哥德尔不完备定理, 以及随后相继出现的, 第二不完备定理, 与图灵关于不可判定性的工作, 从根本上击碎了希尔伯特纲领的哲学构想, 而且这种崩塌, 并不单独来自于宏大的理论, 而是全方位的事实冲击, 其中最具象征意义的例子, 正是希尔伯特在 1900 年, 提出的第一个问题, 连续统假设。1940 年, 哥德尔证明了连续统假设与 ZFC 公理系统的相对一致性, 即如果 ZFC 本身是一致的, 那么在 ZFC 中无法证明连续统假设是错误的。1963 年, 科恩进一步证明了连续统假设无法由 ZFC 推导成立, 由此, 连续统假设成为了一个在 ZFC 框架内永远无法证明的问题。

以 20 世纪中叶希尔伯特时代的终结为分水岭,20 世纪前后的两段数学史, 就像在两个遥远而陌生的世界之中所发生的故事, 此前的数学世界仍深陷于关于基础, 本体论与合法性的哲学争论, 但随着学科的成熟与分化, 哲学观念与宗教式的狂热逐渐从现代数学研究中退场, 第三次数学危机以没有任何一方胜利的结局而告终。

魔笛手那甜蜜的笛声似乎永远停息了。但是，整个世界遍布着希尔伯特的学生，以及希尔伯特学生的学生。赫尔曼 · 外尔正以他特有的热情，试图把普林斯顿高等研究所办成另一个伟大的充满热情的科学中心——要像他年轻时所在的哪个哥廷根一样。在纽约，库朗被安置在一所废弃不用的帽子工厂里，朋友们风趣地把这个地方叫做 “库朗研究所”，在这里，希尔伯特的精神也同样闪耀着。

现代数学不再只在欧洲少数城市内部传承, 而是开始真正成为一项全球性的事业。这之后的数学分支, 已经复杂到, 任何人都无法通晓全貌, 欧拉和高斯那种全才式的英雄时代已经彻底结束, 高度抽象的现代数学, 除了个人天赋之外, 更依赖长期, 稳定, 系统性的智力投入, 它没有时空和资源上的限制, 没有人种和性别上的垄断, 作为一个没有入门条件, 却有着最高智慧门槛的学科, 它真正需求的成本, 只有持续的思考, 以及为之付出的心血。

# 第一章　集合、映射与逻辑初步

## 1.7　拓展阅读：从星期到模 $m$ 剩余类环

# 第一章　集合、映射与逻辑初步

## 1.7　拓展阅读：从星期到模 $m$ 剩余类环

# 第一章　集合、映射与逻辑初步

## 1.7　拓展阅读：从星期到模 $m$ 剩余类环

## 1.8　杂　　题

**1.【2020 全国 II 卷 12】**若序列 $a_1a_2\cdots a_n\cdots$ 满足 $a_i\in\{0,1\}(i=1,2,\cdots)$, 且存在正整数 $m$, 使得 $a_{i+m}=a_i(i=1,2,\cdots)$ 成立, 则称其为 0-1 周期序列. 并称满足 $a_{i+m}=a_i(i=1,2,\cdots)$ 的最小正整数 $m$ 为这个序列的周期. 对于周期为 $m$ 的 0-1 序列 $a_1a_2\cdots a_n\cdots$,$C(k)=\dfrac{1}{m}\sum\limits_{i=1}^{m}a_ia_{i+k}(k=1,2,\cdots,m-1)$ 是描述其性质的重要指标. 下列周期为 5 的 0-1 序列中, 满足 $C(k)\leqslant\dfrac{1}{5}(k=1,2,3,4)$ 的序列是

(A) $11010\cdots$　　(B) $11011\cdots$　　(C) $10001\cdots$　　(D) $11001\cdots$

**2.【2007 福建文 16 理 16】(多选)**中学数学中存在许多关系，比如“相等关系”、“平行关系”等，如果集合 $A$ 中的元素之间的一个关系“$\sim$”满足以下三个条件：

(1) 自反性：对于任意 $a\in A$，都有 $a\sim a$；

(2) 对称性：对于 $a,b\in A$，若 $a\sim b$，则有 $b\sim a$；

(3) 传递性：对于 $a,b,c\in A$，若 $a\sim b,b\sim c$，则有 $a\sim c$，

则称“$\sim$”是集合 $A$ 的一个等价关系。下列关系中，是等价关系的有

(A) 三角形的全等　　(B) 整数的整除　　(C) 向量的共线　　(D) 整数的同余

**3.【2019 命题标准样题 15 改编】(多选)**要合理地刻画三角形三个顶点的“集中程度”, 可以使用

(A) 三角形的周长　　(B) 三角形的面积　　(C) 三角形的外接圆半径　(D) 三角形的最大边长

**4.【2021 新高考 II 卷 12】(多选)**设正整数 $n=a_0\cdot2^0+a_1\cdot2^1+\cdots+a_{k-1}\cdot2^{k-1}+a_k\cdot2^k$, 其中 $a_i\in\{0,1\},i=0,1,2,\ldots,k$. 记 $\omega(n)=a_0+a_1+\cdots+a_k$, 则

(A) $\omega(2n)=\omega(n)$　　(B) $\omega(2n+3)=\omega(n)+1$

(C) $\omega(8n+5)=\omega(4n+3)$　　(D) $\omega(2^n-1)=n$

**5.【2014 北京 8】**学生的语文、数学成绩均被评定为三个等级, 依次为“优秀”“合格”“不合格”. 若学生甲的语文、数学成绩都不低于学生乙, 且其中至少有一门成绩高于乙, 则称“学生甲比学生乙成绩好”. 如果一组学生中没有哪位学生比另一位学生成绩好, 并且不存在语文成绩相同、数学成绩也相同的两位学生, 则这一组学生最多有多少个?

**6.【2017 北京文 14】**某学习小组由学生和教师组成, 人员构成同时满足以下三个条件:

(1) 男学生人数多于女学生人数;

(2) 女学生人数多于教师人数;

（3）教师人数的两倍多于男学生人数.

若教师人数为 4, 则女学生人数的最大值为 (△); 该小组人数的最小值为 (△).

**7.【2009 江西 3】**已知全集 $U=A\cup B$ 中有 $m$ 个元素,$(\complement_U A)\cup(\complement_U B)$ 中有 $n$ 个元素. 若 $A\cap B$ 非空, 求 $A\cap B$ 的元素个数。（用 $m,n$ 表示）

**8.【2015 广东文 10】**已知集合

$$E=\{(p,q,r,s)|0\leqslant p<s\leqslant 4,0\leqslant q<s\leqslant 4,0\leqslant r<s\leqslant 4且p,q,r,s\in\mathbb{N}\}$$
$$F=\{(t,u,v,w)|0\leqslant t<u\leqslant 4,0\leqslant v<w\leqslant 4且t,u,v,w\in\mathbb{N}\},$$

求 $|E|+|F|$.

**9.【2012 安徽 10】** 6 位同学在毕业聚会活动中进行纪念品的交换，任意两位同学之间最多交换一次，进行交换的两位同学互赠一份纪念品，已知 6 位同学之间共进行了 13 次交换，求收到 4 份纪念品的同学人数。

**10.【2011 陕西 14】**植树节某班 20 名同学在一段直线公路一侧植树，每人植一棵，相邻两棵树的距离是 10. 开始时需将树苗集中放置在某一树坑旁边，使每位同学从各自树坑出发前来领取树苗往返所走的路程总和最小，求该最小值.

**11.【2015 年新题型测试】**甲、乙、丙、丁四人商量去看电影. 甲说：乙去我才去；乙说：丙去我才去；丙说：甲不去我就不去；丁说：乙不去我就不去. 最后有人去看了电影，有人没去看电影，去的人是谁?

**12.【2023 四省联考 15】**数学家祖冲之曾经给出圆周率 $\pi$ 的两个近似值：“约率” $\dfrac{22}{7}$ 与 “密率” $\dfrac{355}{113}$. 它们可用 “调日法” 得到：称小于 3.1415926 的近似值为弱率, 大于 3.1415927 的近似值为强率. 由 $\dfrac{3}{1}<\pi<\dfrac{4}{1}$, 取 3 为弱率,4 为强率, 得 $a_1=\dfrac{3+4}{1+1}=\dfrac{7}{2}$, 故 $a_1$ 为强率, 与上一次的弱率 3 计算得 $a_2=\dfrac{3+7}{1+2}=\dfrac{10}{3}$, 故 $a_2$ 为强率, 继续计算,……. 若某次得到的近似值为强率, 与上一次的弱率继续计算得到新的近似值; 若某次得到的近似值为弱率, 与上一次的强率继续计算得到新的近似值, 以此类推. 已知 $a_m=\dfrac{22}{7}$, 则 $m=$ (△) ; $a_8=$ (△).

**13.【2015 福建理 15】**一个二元码是由 0 和 1 组成的数字串 $x_1x_2\ldots x_n$ $(n\in\mathbb{N}^*)$, 其中 $x_k(k=1,2,\ldots,n)$ 称为第 $k$ 位码元. 二元码是通信中常用的码, 但在通信过程中有时会发生码元错误（即码元 0 变为 1, 或者由 1 变为 0）. 已知某种二元码 $x_1x_2\cdots x_7$ 的码元满足如下校验方程组：

$$\begin{cases}x_4\oplus x_5\oplus x_6\oplus x_7=0\\ x_2\oplus x_3\oplus x_6\oplus x_7=0\\ x_1\oplus x_3\oplus x_5\oplus x_7=0\end{cases}$$

其中运算 $\oplus$ 定义为：$0\oplus 0=0$, $0\oplus 1=1$, $1\oplus 0=1$, $1\oplus 1=0$.

已知某个符合上述特征的二元码在通信过程中仅在第 $k$ 位发生码元错误后变成了 1101101, 利用上述校验方程组求出 $k$.

**14.【2013 湖北文 17】**在平面直角坐标系中, 若点 $P(x,y)$ 的坐标 $x,y$ 均为整数, 则称点 $P$ 为格点. 若一个多边形的顶点全是格点, 则称该多边形为格点多边形. 格点多边形的面积记为 $S$, 其内部的格点数记为 $N$, 边界上的格点数记为 $L$. 例如图中 $\triangle ABC$ 是格点三角形, 对应的 $S=1,N=0,L=4$.

(1) 求图中格点四边形 $DEFG$ 对应的 $S,N,L$;

(2) 已知格点多边形的面积可表示为 $S=aN+bL+c$, 其中 $a,b,c$ 为常数, 若某格点多边形对应的 $N=71,L=18$, 求它的 $S$。

(3) **（选做）**第（2）问给出的公式是 Pick 定理，利用 2.3 习题 B 组中介绍的第二类数学归纳法完成该定理的证明

提示：关于奠基步骤，首先对矩形证明定理成立，然后对直角三角形证明定理成立，最后注意到：一个三角形区域是由包含该三角形在内的一个较大的矩形区域减去之多三个角形区域所得到的结果，关于归纳步骤，可利用下述引理：

**引理**：每个简单的至少四边的多边形都存在一条内部对角线。

**15.** **【2008 福建文 15】【2009 福建文 16】**五位同学围成一圈依序循环报数, 规定：

(1) 第一位同学首次报出的数为 1, 第二位同学首次报出的数也为 1, 之后每位同学报出的数都是前两位同学所报出的数之和；

(2) 若报出的数为 3 的倍数, 则报该数的同学需拍手一次,

已知甲同学第一个报数, 当五位同学依序循环报到第 100 个数时, 求五位同学拍手的总次数与甲同学拍手的总次数.

**16.** **【2012 湖南理 16】**设 $N=2^n$ $(n\in\mathbb{N}^*,n\geqslant 2)$, 将 $N$ 个数 $x_1,x_2,\ldots,x_N$ 依次放入编号为 $1,2,\ldots,N$ 的 $N$ 个位置, 得到排列 $P_0=x_1x_2\cdots x_N$. 将该排列中分别位于奇数与偶数位置的数取出, 并按原顺序依次放入对应的前 $\dfrac{N}{2}$ 和后 $\dfrac{N}{2}$, 得到排列 $P_1=x_1x_3\cdots x_{N-1}x_2x_4\cdots x_N$, 将此操作称为 $C$ 变换. 将 $P_1$ 分成两段, 每段 $\dfrac{N}{2}$ 个数, 得到 $P_2$; 当 $2\leqslant i\leqslant n-1$ 时, 将 $P_i$ 分成 $2^{i-1}$ 段, 每段 $\dfrac{N}{2^{i-1}}$ 个数, 对每一段进行 $C$ 变换得到 $P_{i+1}$. 例如, 当 $N=8$ 时, $P_2=x_1x_5x_3x_7x_2x_6x_4x_8$, 此时 $x_7$ 位于 $P_2$ 中的第 4 个位置.

当 $N=16$ 时, $x_7$ 位于 $P_2$ 中的第 (△) 个位置；当 $N=2^n$ $(n\geqslant 8)$ 时, $x_{173}$ 位于 $P_4$ 中的第 (△) 个位置.

**17.** **【2025 深圳一模 14】**某次考试共 5 道试题, 均为判断题. 计分的方法是：每道题答对的给 2 分, 答错或不答的扣 1 分, 每个人的基本分为 10 分. 已知赵、钱、孙、李、周、吴 6 人的作答情况及前 5 个人的得分情况如下表, 则吴的得分为 (△).

| 人 / 题号 | 赵 | 钱 | 孙 | 李 | 周 | 吴 |
|---|---|---|---|---|---|---|
| 1 | ✓ | ✓ | × | × | ✓ | ✓ |
| 2 | × | ✓ | × | ✓ | ✓ | ✓ |
| 3 | ✓ | × | × | ✓ | × | × |
| 4 | ✓ | × | × | × | ✓ | × |
| 5 | × | × | ✓ | ✓ | ✓ | ✓ |
| 得分 | 14 | 11 | 14 | 14 | 11 | |

**18.** **【2015 高联一试 10A】**设 $a_1,a_2,a_3,a_4$ 为四个有理数, 使得 $\{a_ia_j\mid 1\leqslant i<j\leqslant 4\}=\left\{-24,-2,-\dfrac{3}{2},-\dfrac{1}{8},1,3\right\}$. 求 $a_1+a_2+a_3+a_4$ 的值.

**19.** 某次知识竞赛包括甲、乙、丙三个问题，在所有 25 名参加的学生中，每名学生至少回答出了一题。在没有答出甲题的学生中，答出乙题的人数是答出丙题人数的 2 倍；只答出甲题的人数比余下的学生中答出甲题的人数多 1 人；只答出 2 题的学生中，有一半没有答出甲题。求学生的答题情况的所有不同可能数。

**20.** **【2023"fiddie"模拟考 16】**正方形 $ABCD$ 位于平面直角坐标系上，其中 $A(1,1),B(-1,1),C(-1,-1),D(1,-1)$。考虑对这个正方形执行下面三种变换：

（1）$L$：逆时针旋转 $90^\circ$。（2）$R$：顺时针旋转 $90^\circ$。（3）$S$：关于原点对称。

上述三种操作可以把正方形变换为自身，但是 $A,B,C,D$ 四个点所在的位置会发生变化。例如，对原正方形作变换 $R$ 之后，顶点 $A$ 从 $(1,1)$ 移动到 $(1,-1)$，然后再作一次变换 $S$ 之后，$A$ 移动到 $(-1,1)$。对原来的正方形按 $a_1,a_2,\ldots,a_k$ 的顺序作 $k$ 次变换记为 $a_1a_2\ldots a_k$，其中 $a_i\in\{L,R,S\},i=1,2,\ldots,k$。如果经过 $k$ 次变换之后，顶点的位置恢复为原来的样子，那么我们称这样的变换是 $k$-恒等变换。例如，$RRS$ 是一个 3-恒等变换。

则 3-恒等变换共 (△) 种；对于正整数 $n$，$n$-恒等变换共 (△) 种。

**21.** **【2024 北京第一次学考 28】**已知 $\boldsymbol{\alpha}_0=(a_0,b_0,c_0,d_0)$ 和数表 $\boldsymbol{A}=\begin{pmatrix}a_1&b_1&c_1&d_1\\a_2&b_2&c_2&d_2\\a_3&b_3&c_3&d_3\end{pmatrix}$，其中 $a_i,b_i,c_i,d_i\in\mathbb{N}^*$ $(i=0,1,2,3)$. 若数表 $\boldsymbol{A}$ 满足如下两个性质，则称数表 $\boldsymbol{A}$ 由 $\boldsymbol{\alpha}_0$ 生成.

（1）任意 $i\in\{0,1,2\}$，$a_{i+1}-a_i,b_{i+1}-b_i,c_{i+1}-c_i,d_{i+1}-d_i$ 中有三个 $-1$，一个 3；

（2）存在 $k\in\{1,2,3\}$，使 $a_k,b_k,c_k,d_k$ 中恰有三个数相等.

（1）判断数表 $\boldsymbol{A}=\begin{pmatrix}5&6&6&6\\4&5&5&9\\3&8&4&8\end{pmatrix}$ 是否由 $\boldsymbol{\alpha}_0=(6,7,7,3)$ 生成；（结论无需证明）

（2）是否存在数表 $\boldsymbol{A}$ 由 $\boldsymbol{\alpha}_0=(6,7,7,4)$ 生成？说明理由；

（3）若存在数表 $\boldsymbol{A}$ 由 $\boldsymbol{\alpha}_0=(7,12,3,d_0)$ 生成，写出 $d_0$ 所有可能的值.

**22.** **【2025 北京第二次学考 25】**给定正整数 $n\geqslant 3$，按一定顺序排列的向量 $(x_1,y_1)$，$(x_2,y_2)$，$\cdots$，$(x_m,y_m)$ 记为向量序列 $S$：$(x_1,y_1)$，$(x_2,y_2)$，$\cdots$，$(x_m,y_m)$，其中 $x_i\in\{1,2,\cdots,n\}$，$y_i\in\{1,2\}$，$i=1,2,\cdots,m$。

给出两个性质：

i.$x_1=y_1=1$，$x_m=n$，且 $S$ 中的向量互不相等；

ii. 已知向量集合 $T=\{(1,0),(0,1),(0,-1)\}$。记 $\alpha_i=(x_i,y_i)$，对于 $S$ 中的任意两个向量 $\alpha_i,\alpha_j$ $(i<j)$，"$\alpha_j-\alpha_i\in T$" 的充要条件是 "$j=i+1$"。

(1) 当 $n=3$ 时，分别判断向量序列

$$A:(1,1),(2,1),(2,2),$$

$$B:(1,1),(1,2),(2,2),(2,1),(3,1)$$

是否满足性质 i；（结论无需证明）

(2) 当 $n=3$ 时，写出一个同时满足性质 i 和性质 ii 的向量序列 $S$；

(3) 当 $n=5$ 时，若向量 $(4,1)$，$(4,2)$ 不同时在向量序列 $S$ 中，且 $S$ 同时满足性质 i 和性质 ii，求证：$S$ 的个数为偶数。

**1.** **C.**

**2.**

**3.** **AD.**

**4.** **ACD.** $\omega(n)$ 指的是 10 进制数 $n$ 对应的二进制序列中 1 的个数，记十进制数 $n$ 的二进制表示为 $B(n)=(a_0a_1\cdots a_k)_2$. 对于 A，$2n$ 的二进制序列相当于将 $n$ 的二进制序列左移一位，末尾添一个 0，所以 $\omega(2n)=\omega(n)$，A 正确。对于 B，当 $n=3$ 时，$\omega(2n+3)=2,\omega(n)+1=3$，二者不相等，故 B 错误。

对于 C，分别将 $8n+5$ 与 $4n+3$ 写成二进制形式：

$$B(8n+5)=(\underbrace{\cdots\cdots}_{n\text{的二进制表示}}101)_2,\quad B(4n+3)=(\underbrace{\cdots\cdots}_{n\text{的二进制表示}}11)_2,$$

可知 $\omega(8n+5)=\omega(4n+3)=\omega(n)+2$.C 正确。

$2^n-1$ 的二进制表示是 $n$ 个 1，所以 $\omega(2^n-1)=n$，D 错误。

**5.** **3.** 为方便起见, 把优秀、合格、不合格记为 $3,2,1$ 分. 由于不存在语文成绩相同、数学成绩也相同的学生, 所以最多只可能有 9 个学生, 我们可以把所有可能的学生列出来:

$$\begin{matrix}P_{33} & P_{32} & P_{31}\\ P_{23} & P_{22} & P_{21}\\ P_{13} & P_{12} & P_{11}\end{matrix}$$

其中学生 $P_{ij}$ 表示语文是 $i$ 分, 数学是 $j$ 分. 我们逐步排除掉不可能出现的学生.

因为一组学生中没有哪位学生比另一位学生成绩好, 所以不可能有 $P_{33}$ 和 $P_{11}$(一定是最好或最差). 根据对称性, 接下来只需考虑 $P_{32}$ 和 $P_{31}$ 是否存在.

如果有 $P_{32}$, 则不可能有 $P_{31},P_{22},P_{21},P_{12}$, 必须有 $P_{23}$ 或 $P_{13}$(不可能都有), 此时这一组学生最多只有 2 个, 为 $\{P_{32},P_{23}\}$ 或 $\{P_{32},P_{13}\}$.

如果有 $P_{31}$, 则不可能有 $P_{21}$ 和 $P_{32}$. 所以这一组学生人数最多的情况只可能是 $\{P_{31},P_{22},P_{13}\}$.

综上, 这一组学生最多有 3 个.

**6.** **6;12.** 设男学生人数为 $a$, 女学生人数为 $b$, 教师人数为 $c$. 由条件, $a\geqslant b+1$, $b\geqslant c+1$, $2c\geqslant a+1$.

若教师人数为 4, 则 $a+1\leqslant 2c=8$, $a\leqslant 7$, $b\leqslant a-1=6$. 而当 $b=6$ 时, $a=7,c=4$ 满足三个条件. 故女学生人数最大值为 6.

$a+b+2c\geqslant(b+1)+(c+1)+(a+1)$, 因此 $c\geqslant 3$, 从而 $b\geqslant 4,a\geqslant 5$. 当 $c=3,b=4,a=5$ 时, 满足三个条件. 故小组人数最小值为 12.

**7.** **$m-n$** 由德摩根律，$(\complement_U A)\cup(\complement_U B)=\complement_U(A\cap B)$, 因而

$$n=|\complement_U(A\cap B)|=|U|-|A\cap B|=m-|A\cap B|$$

即 $|A\cap B|=m-n$。

**8.** **200.**

**9.** **2 或 4.**

**10.** **2000.** 设树苗放在第 $k$ 棵树下，用 $a_n$ 表示第 $n$ 棵树与第 $k$ 棵树的距离，则 $a_n=10|n-k|$，其中 $n=1,2,\cdots,20$. 所以往返路程总和为

$$\begin{aligned}2\sum_{n=1}^{20}10|n-k| &= 20\sum_{n=1}^{k}(k-n)+20\sum_{n=k+1}^{20}(n-k)\\ &= 20\frac{(k-1)k}{2}+20\frac{(21-k)(20-k)}{2}\\ &= 10(2k^2-42k+420).\end{aligned}$$

函数 $y=2x^2-42x+420$ 的对称轴是直线 $x=\dfrac{21}{2}$，但是 $k$ 是正整数，所以当 $k=10$ 或 $k=11$ 时往返路程取最小值 2000.

**11.**

**12.** **6;47/15** ，列表如下：

| 序号 | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ |
|---|---|---|---|---|---|---|---|---|
| 分数 | $\frac{3+4}{1+1}$ | $\frac{3+7}{1+2}$ | $\frac{3+10}{1+3}$ | $\frac{3+13}{1+4}$ | $\frac{3+16}{1+5}$ | $\frac{3+19}{1+6}$ | $\frac{3+22}{1+7}$ | $\frac{22+25}{7+8}$ |
| 近似值 | $\frac{7}{2}$ | $\frac{10}{3}$ | $\frac{13}{4}$ | $\frac{16}{5}$ | $\frac{19}{6}$ | $\frac{22}{7}$ | $\frac{25}{8}$ | $\frac{47}{15}$ |
| 强弱率 | 强率 | 强率 | 强率 | 强率 | 强率 | 强率 | 弱率 | 弱率 |

**13.** **5.** 接收码为 1101101，即 $(x_1,x_2,x_3,x_4,x_5,x_6,x_7)=(1,1,0,1,1,0,1)$，将其代入三个校验式，得到校验结果

$$\begin{aligned}s_1 &= x_4\oplus x_5\oplus x_6\oplus x_7 = 1\oplus 1\oplus 0\oplus 1 = 1\\ s_2 &= x_2\oplus x_3\oplus x_6\oplus x_7 = 1\oplus 0\oplus 0\oplus 1 = 0\\ s_3 &= x_1\oplus x_3\oplus x_5\oplus x_7 = 1\oplus 0\oplus 1\oplus 1 = 1\end{aligned}$$

若只有第 $k$ 位发生错误，那么所有包含该位的校验式均会变为 1，根据上述结果，发生错误的码元应当只出现在第 1 个与第 3 个方程中，观察得到 $k=5$.

**14.** **$S=3,N=1,L=6;S=79$** 代入格点三角形 $ABC$ 与四边形 $DEFG$ 的数据，得到方程 $\begin{cases}4b+c=1\\ a+6b+c=3\end{cases}$

要解出 $a,b,c$，还需再找一个例子：如果某个格点四边形由两个小正方形构成，此时 $S=2,N=0,L=6$，因此 $6b+c=2$. 结合上述三个方程解得 $a=1,b=\dfrac{1}{2},c=-1$，因此 $S=N+\dfrac{1}{2}L-1$，代入 $N=71,L=18$ 可得 $S=79$.

**15.** **25;5.** 报数序列为斐波那契型数列：

$$1,1,2,3,5,8,13,21,34,55,\ldots$$

模 3 计算得到

$$1,1,2,0,2,2,1,0,1,1,2,0,\ldots$$

从第一个数开始每八项循环一次，且其中有两项为 0，即每八次报数有两次拍手，计算得到前 100 次报数中拍手 25 次。

甲在第 $1,6,11,16,\ldots$ 次报数，即报数序号模 5 为 1 时拍手，求甲在前 100 次中拍手的次数等价求满足下述条件的 $x(1\leqslant x\leqslant 100)$ 的个数

$$\begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 0 \pmod 4 \end{cases}$$

解得 $x=16,36,56,76,96$, 于是甲在前 100 次中拍手 5 次。

**16.** $\underline{\mathbf{6;3\times 2^{N-4}+11}}$ 当 $N=16$ 时，只考虑每次变换序列的下标，有

$$\begin{aligned} P_0&:1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\\ P_1&:1,3,5,7,9,11,13,15,2,4,6,8,10,12,14,16\\ P_2&:1,5,9,13,3,7,11,15,2,6,10,14,4,8,12,16 \end{aligned}$$

于是 $x_7$ 位于第 6 个位置。

可以发现，每次进行 $C$ 变换后，当前的所有段都会按照奇偶编号被平均划分为 2 段，在下一次 $C$ 变换时，若要考察某个数所处位置的编号，只需注意它所处的段编号的奇偶性即可.

进行 $P_1$ 变换后，$x_{173}$ 处于第 87 号位置；进行 $P_2$ 变换后，$x_{173}$ 处于第 44 号位置，且位于分别含有 $2^{N-2}$ 个元素的 4 个段中的第一段，进行 $P_3$ 变换后，$x_{173}$ 处于第 $2^{N-3}+22$ 号位置，且位于分别含有 $2^{N-3}$ 个元素的 8 个段中的第二段，进行 $P_4$ 变换后，$x_{173}$ 处于 $2^{N-3}+2^{N-4}+11$ 号位置，即 $3\times 2^{N-4}+11$ 号位置。

**17.**

**18.** $\underline{\mathbf{14.}}$ 可知，得 14 分表示其答对 3 题，答错 2 题；得 11 分表示其答对 2 题，答错 3 题，现假设：若赵同学答对第 $i$ 题，则记 $a_i=1$，否则记 $a_i=0$，尝试利用已知条件解出 $a_1,a_2,a_3,a_4,a_5$，记 $\overline{a_i}=1-a_i$，于是列出方程组

$$\begin{cases} a_1+a_2+a_3+a_4+a_5=3 & (1)\text{赵同学的答题情况}\\ a_1+\overline{a_2}+\overline{a_3}+\overline{a_4}+a_5=2 & (2)\text{钱同学的答题情况}\\ \overline{a_1}+a_2+\overline{a_3}+\overline{a_4}+\overline{a_5}=3 & (3)\text{ 孙同学的答题情况}\\ \overline{a_1}+\overline{a_2}+a_3+\overline{a_4}+\overline{a_5}=3 & (4)\text{ 李同学的答题情况}\\ a_1+\overline{a_2}+\overline{a_3}+a_4+\overline{a_5}=2 & (5)\text{ 周同学的答题情况} \end{cases}$$

可知，$a_i+\overline{a_i}=1$，(1)+(2) 化简得到 $a_1+a_5=1$，(1)+(3) 化简得到 $a_2=1$,(1)+(4) 化简得到 $a_3=1$,(1)+(5) 化简得到 $a_1+a_4=1$，同时考虑 (1) 式，可以解得 $a_1=a_2=a_3=1,a_4=a_5=0$, 于是 1-5 题的正确答案分别为 “对，错，对，错，对”，故吴同学答对 3 道，得分为 14。

**19.**

**20.**

**21.**

**22.**

**23.**

# 第一章　集合、映射与逻辑初步

## 1.7　拓展阅读：从星期到模 $m$ 剩余类环