# 第六册

大青花鱼

# 目录

# 第一章　代数式的关系

## 1.1　代数恒等式

## 1.2　代数不等式

# 第二章　三段论（下）

## 2.1　三段论的规则

## 2.2　三段论的应用

# 第三章　投影和视图

## 3.1　平面和立体

## 3.2　三视图

## 3.3　表面的展开

# 第四章　同余

**例子 4.0.1.** $7^{65}$ 的个位数是多少?

**解答.** 从 $7^0, 7^1, 7^2, 7^3 \cdots$ 开始找规律。$7^0 = 1$，$7^1 = 7$，$7^2 = 49$，$7^3 = 343$，$7^4 = 2401$，$7^5 = 16807$。$7^4$ 和 $7^0$ 的个位数都是 1，$7^5$ 和 $7^1$ 的个位数都是 7。我们可以总结出这样的规律：个位数是 1 的，乘以 7 得到 7；个位数是 7 的，乘以 7 得到 9；个位数是 9 的，乘以 7 得到 3；个位数是 3 的，乘以 7 得到 1。

也就是说，如果把 $7^0, 7^1, 7^2, 7^3 \cdots$ 的个位数写成一列，应该是这个样子的：

$$1, 7, 9, 3, 1, 7, 9, 3, 1, 7, \cdots$$

用归纳法不难证明，这列数字以 4 为周期不断重复。所以，要求 $7^{65}$ 的个位数，可以看 65 在相关的周期里处于哪个位置。换句话说，只要看 65 除以 4 的余数。$65 = 16 \times 4 + 1$，所以 $7^{65}$ 的个位数和 $7^1$ 的个位数一样，都是 7。

从这个例子可以看出，两个整数除以同一个数得到相同的余数，是一个重要的性质。我们把这种性质称为**同余**。比如，65 和 1 除以 4 余数都是 1，我们就说 65 和 1 模 4 同余。$7^{65}$ 和 $7^1$ 除以 10 余数都是 7，我们说 $7^{65}$ 和 $7^1$ 模 10 同余，记为：

$$7^{65} \equiv_{10} 7^1$$

## 4.1 同余类

整数除以 3，余数有 $0, 1, 2$ 三种可能。整数除以 10，余数有 $0, 1, \cdots, 9$ 十种可能。一般来说，给定正整数 $n$，整数除以 $n$，余数有 $0, 1, \cdots, n-1$ 这 $n$ 种可能。因此，按除以 $n$ 的余数，可以把整数集分成 $n$ 类。同属一类的数，模 $n$ 同余，所以这 $n$ 类数叫作模 $n$ **同余类**。所有模 $n$ 同余类的集合，叫作模 $n$ **同余系**。

每个模 $n$ 同余类，可以写成 $\{kn + a \,|\, k \in \mathbb{Z}\}$ 的形式。也就是说，可以看成某个数 $a$ 不断加上或减去 $n$ 得到的所有数的集合。这个集合是无穷的。不同的模 $n$ 同余类，交集是空集，并集是 $\mathbb{Z}$。也就是说，它们是 $\mathbb{Z}$ 的分划。

为了方便，我们从每个模 $n$ 同余类中选一个元素，代表这个同余类。一般来说，可以选 $0, 1, \cdots, n-1$ 个数。我们给它们加个上划线，以和作为整数的 $0, 1, \cdots, n-1$ 区分：

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}$$

如果要强调 $n$，可以把 $n$ 加在右上角：

$$\overline{0}^n, \overline{1}^n, \cdots, \overline{n-1}^n$$

给定整数 $m$，我们可以把它对应到某个模 $n$ 同余类，称为对 $n$ **取模**。比如 $n = 5$ 时，$24 \equiv_5 4$，我们把 24 对应到 $\overline{4}^5$，或者说，24 对 5 取模，得 $\overline{4}^5$。

同余关系和相等关系很像，它们是否有一样的性质呢？我们可以验证，同余关系满足以下的性质：

1. $\forall\ a \in \mathbb{Z}, \quad a \equiv_n a$；
2. $\forall\ a, b \in \mathbb{Z}$，如果 $a \equiv_n b$，那么 $b \equiv_n a$；
3. $\forall\ a, b \in \mathbb{Z}$，如果 $a \equiv_n b$，$b \equiv_n c$，那么 $a \equiv_n c$。

满足以上三个性质的二元关系（两个元素之间的关系）称为**等价关系**。数与数的等于关系是等价关系，数与数的同余关系也是等价关系。因此，我们可以把同余关系用作同余类之间的等于关系。

整数之间有四则运算，模 $n$ 同余类之间，也可以进行运算。以 $n=5$ 为例子。我们分别计算 24 和 37 除以 5 的余数，以及它们的和 61 除以 5 的余数：

$$24 \equiv_5 4,\ \ 37 \equiv_5 2,\ \ 61 \equiv_5 1$$

可以发现：$4+2 \equiv_5 1$，也就是说，取模和加法可以交换顺序。可以验证，两个同余类中各取一个元素相加，和所在的同余类，就是两者模 $n$ 余数的和所在的同余类。用集合的语言，可以写成：

$$\{kn+a+ln+b \,|\, k \in \mathbb{Z}, l \in \mathbb{Z}\} = \{kn+a+b \,|\, k \in \mathbb{Z}\}$$

所以，可以定义同余类的加法：

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

其中的 $\overline{a+b}$ 指的是 $a+b$ 所在的同余类。为了方便，我们用 $a+b$ 作为代表。

可以验证，同余类的加法也满足结合律和交换律。这里我们只证明同余类的加法满足结合律，交换律的证明留做习题：

**证明：** 由上可知 $\overline{a}+\overline{b} = \overline{a+b}$，所以

$$(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{a+b+c}.$$

类似可得：

$$\overline{a}+(\overline{b}+\overline{c}) = \overline{a}+\overline{b+c} = \overline{a+b+c}.$$

于是

$$(\overline{a}+\overline{b})+\overline{c}=\overline{a+b+c}=\overline{a}+(\overline{b}+\overline{c}).$$

□

类似可以定义同余类的减法和乘法：

$$\overline{a}-\overline{b}=\overline{a-b},\ \ \overline{a}\cdot\overline{b}=\overline{a\cdot b}$$

可以验证，同余类的减法性质和整数减法一样，同余类的乘法也满足结合律、交换律和分配律。

能否定义同余类的除法呢？我们来看一个例子。设 $n=6$，考虑等式 $12\div 4=3$。12、4 和 3 对 6 取模，得到 0、4 和 3。考虑等式 $60\div 10=6$。60、10 和 6 对 6 取模，得到 0、4 和 0。也就是说，两个模 6 同余类中各取元素相除，商所在的同余类不是唯一的。所以，我们没法定义模 6 同余类的除法。

再看另一个例子。设 $n=5$，考虑以下的“乘法表”：

| $\times$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

可以看出，任何模 5 同余类乘以 $\overline{0}$ 都得到 $\overline{0}$，非 $\overline{0}$ 同余类乘以不同的同余类，结果也不同。这说明每个同余类除以另一个同余类（非 $\overline{0}$），都必然有唯一的结果。这样我们就定义了模 5 同余系里的除法。

**习题 4.1.1.**
动手做一做：

*1.* 证明同余关系满足等价关系所要求的三个性质。

*2.* 证明同余类的加法满足交换律。

*3.* 证明同余类的减法是加法的逆运算。

*4.* 证明同余类的乘法满足结合律和交换律。

*5.* 证明同余类的乘法满足分配律。

*6.* 证明：如果某模 $n$ 同余类的代表与 $n$ 的最大公因数是 $d$，则其中所有元素与 $n$ 的最大公因数都是 $d$。

*7.* 分别画出模 3 同余系和模 4 同余系的“乘法表”。它们和模 5 同余系的“乘法表”哪些地方相同，哪些地方不同?

## 4.2 完全同余系和简化同余系

上一节我们提到模 6 同余系无法定义除法，而模 5 同余系可以定义除法。两者有什么不同呢? 我们画出模 6 同余系的“乘法表”:

| $\times$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{2}$ | $\overline{0}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{5}$ | $\overline{0}$ | $\overline{5}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

可以看到，这个“乘法表”和模 5 同余系的大有不同。同一行或同一列常有重复。这说明不同的同余类乘同一个同余类得到同一个结果。比如

$$\overline{2} \times \overline{4} = \overline{5} \times \overline{4} = \overline{2}.$$

这就使我们没法定义除法。

如果我们把上面的等式稍作变化，会得到：

$$\overline{0} = (\overline{5} - \overline{2}) \times \overline{4} = \overline{3} \times \overline{4}.$$

也就是说，有非 $\overline{0}$ 的同余类相乘等于 $\overline{0}$。同余类乘法的这个性质和整数乘法完全不同。我们把这种非 $\overline{0}$ 同余类叫做**零因子**。整数中没有零因子：非 0 的整数相乘必然不是 0。而只要有这种零因子存在，同余系中就会发生“不同的同余类乘同一个同余类得到同一个结果”的现象，从而无法定义除法。

有什么办法在模 6 同余系中定义除法呢? 我们可以选一部分同余类，在其中定义除法。如果同余类 $\overline{a}$ 的代表 $a$ 与 6 不互素，设最大公因数是 $b$，那么

$$\frac{a}{b} \times 6 = a \times \frac{6}{b}$$

于是有 $\overline{a} \times \overline{\frac{6}{b}} = \overline{0}$，出现零因子。因此，为了避免零因子问题，我们只选和 6 互素的数所在的同余类，也就是 $\overline{1}$ 和 $\overline{5}$。我们发现 $\{\overline{1}, \overline{5}\}$ 中可以定义乘法和除法（但不再满足加减法）。

| $\times$ | $\overline{1}$ | $\overline{5}$ |
|---|---|---|
| $\overline{1}$ | $\overline{1}$ | $\overline{5}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{1}$ |

我们把模 6 同余系称为模 6 的**完全同余系**，把 $\{\overline{1}, \overline{5}\}$ 称为模 6 的**简化同余系**。

一般来说，我们把模 $n$ 同余系称为模 $n$ 的完全同余系，在其中可以定义加减法和乘法；把其中所有和 $n$ 互素的同余类的集合称为模 $n$ 的简化同余系 [1]。

**定理 4.2.1.** 给定正整数 $n$，在模 $n$ 的简化同余系中可以定义乘法和除法。

[1]通常不把 $\overline{0}$ 计入简化剩余系，以省去讨论除以 $\overline{0}$ 的问题。

**证明：** 模 $n$ 同余类的乘法已经定义好了。我们只需要说明：简化同余系中的同余类相乘，仍然在简化同余系中。这是因为与 $n$ 互素的整数相乘，结果还是与 $n$ 互素。
接下来定义除法。除法是乘法的逆运算。比照数的除法：$a \div b = a \times \frac{1}{b}$。因此，只要将简化同余系中每个同余类都对应一个“倒数”，就可以用“乘以倒数”来定义除法。
我们把模 $n$ 简化同余系中的同余类用小于 $n$ 且与 $n$ 互素的正整数来代表，记为

$$1 = b_1 < b_2 < \cdots < b_{\varphi(n)} = n - 1.$$

其中 $\varphi(n)$ 是模 $n$ 简化同余系的元素个数。考虑任一元素 $b_i$，我们接下来会证明：$b_ib_1, b_ib_2, \cdots, b_ib_{\varphi(n)}$ 模 $n$ 两两不同余。于是，它们中恰有一个模 $n$ 余 1。设 $b_ib_j \equiv_n 1$，那么 $b_j$ 就是 $b_i$ 的“倒数”。
最后用反证法证明命题：$b_ib_1, b_ib_2, \cdots, b_ib_{\varphi(n)}$ 模 $n$ 两两不同余。
反设命题不成立，即存在 $b_j, b_k$ 使得 $b_ib_j \equiv_n b_ib_k$。这说明 $n | b_i(b_j - b_k)$。由于 $b_i$ 和 $n$ 互素，根据倍和析因定理，存在整数 $p, q$，使得：

$$b_ip + nq = 1.$$

两边乘以 $b_j - b_k$，就得到：

$$b_i(b_j - b_k)p + nq(b_j - b_k) = b_j - b_k.$$

等式左边是 $n$ 的倍数，因此 $b_j$ 和 $b_k$ 模 $n$ 同余，这与它们的定义矛盾。
因此命题的否定为假，原命题为真。 □

简化同余系的除法和整数不同，任何同余类都能整除另一个同余类，不需要余数、带余除法的概念。每个同余类都有自己的“倒数”，比如在模 6 简化同余系中，$\overline{5} \times \overline{5} = \overline{1}$。我们把同余类的“倒数”称为它的（乘法）**逆**。

**习题 4.2.1.**

*1.* 写出模 12 的简化同余系。写出 $\overline{7}^{12}$ 的逆。

*2.* 比较模 12 简化同余系中的乘除法和模 4 完全同余系中的加减法，

它们有何异同?

*3.* 写出模 10 的简化同余系。写出 $\overline{7}^{10}$ 的逆。

*4.* 比较模 10 简化同余系中的乘除法和模 4 完全同余系中的加减法，它们有何异同?

*5.* 给定素数 $n$，写出模 $n$ 简化同余系。

## 4.3 方余定理

与模 $n$ 简化同余系密切相关的一个定理是方余定理[2]。

**定理 4.3.1. 方余定理** 设 $a$ 是模 $n$ 简化同余系中某个同余类中的元素，则:

$$a^{\varphi(n)} \equiv_n 1$$

其中 $\varphi(n)$ 是模 $n$ 简化同余系中同余类的个数。

比如，模 10 简化同余系有 4 个元素: $\overline{1}, \overline{3}, \overline{7}, \overline{9}$。7 属于同余类 $\overline{7}$，则 $7^4 \equiv_{10} 1$。

**证明:** 我们把模 $n$ 简化同余系中的同余类用小于 $n$ 且与 $n$ 互素的正整数来代表，记为

$$1 = b_1 < b_2 < \cdots < b_{\varphi(n)} = n - 1.$$

它们两两不同余。把它们各自乘以 $a$, 得到 $\varphi(n)$ 个整数: $ab_1, ab_2, \cdots, ab_{\varphi(n)}$。前面我们已经证明了，它们仍然两两不同余。
这说明这 $\varphi(n)$ 个整数也分别代表模 $n$ 简化同余系中的各个同余类。
考虑乘积: $b_1 b_2 \cdots b_{\varphi(n)}$。$(ab_1)(ab_2)\cdots(ab_{\varphi(n)})$ 和它同余。也就是说:

$$b_1 b_2 \cdots b_{\varphi(n)} \equiv_n (ab_1)(ab_2)\cdots(ab_{\varphi(n)}) \equiv_n a^{\varphi(n)} b_1 b_2 \cdots b_{\varphi(n)}.$$

[2]这个定理也称为欧拉定理。但以欧拉命名的定理太多了。为了避免混淆，这里不采用。

由于 $b_1b_2\cdots b_{\varphi(n)}$ 也与 $n$ 互素，我们把等式两边除以 $b_1b_2\cdots b_{\varphi(n)}$，就得到：

$$a^{\varphi(n)} \equiv_n 1.$$

□

如果 $n$ 是素数，那么 $1, 2, \cdots, n-1$ 都和它互素，于是模 $n$ 的简化同余系就是 $\{\overline{1}, \overline{2}, \cdots, \overline{n-1}\}$，$\varphi(n) = n-1$。根据方余定理，只要 $a$ 不是 $n$ 的倍数，就有：

$$a^{n-1} \equiv_n 1.$$

这个结论也叫做费马小定理。

**习题 4.3.1.**

给定素数 $n$，证明：

*1.* 除了 $\overline{1}$ 和 $\overline{n-1}$，其它同余类的逆都不是自己。

*2.* $(n-1)! \equiv_n -1$.

设 $a$ 与 $n$ 互素，称使得 $a^m \equiv_n 1$ 的最小正整数 $m$ 为 $a$ 模 $n$ 的**阶**。

*3.* 证明 $a$ 的阶整除 $\varphi(n)$。

*4.* 如果 $a$ 的阶等于 $\varphi(n)$，就说 $a$ 是模 $n$ 的**原根**。证明：如果 $a$ 是模 $n$ 的原根，那么模 $n$ 简化同余系可以写成：$\{\overline{a^0}, \overline{a^1}, \cdots, \overline{a^{\varphi(n)-1}}\}$。

*5.* 找出所有模 7 的原根。

# 第五章　用数据说话

## 5.1　样本和特征

## 5.2　描述和分析

## 5.3　数据的结构

# 第六章　数学和社会

## 6.1　随时代变化的数学

## 6.2　数学和科学

## 6.3　数学和现代化