第二章 同 余

同余理论是初等数论的堂奥，包含了数论特有的思想和方法。

同余理论在密码学，特别是公钥密码学中有重要的应用。

2.1 同余基本概念与性质

由整数的带余除法可知，如果n为正整数，则$\forall a \in Z$，有唯一的一组整数q以及r，使得

$$a = qn + r，其中 0 \le r < n。$$

记

$$A_r = \{x : x \in Z, f(x) = r\}，其中 0 \le r < n，\ r \in N .$$

定义 2.1.1 设$n \in N^+$，$a_1, a_2 \in Z$，$a_i = q_i n + r_i$，其中$q_i, r_i \in Z$，$0 \le r_i < n$，$i = 1$或2，如果$r_1 = r_2$，我们称a_1, a_2模n同余。这时记为$a_1 \equiv a_2 (\bmod n)$。

两个等价定义：

定义 2.1.1' 设$n \in N^+$，如果$n \mid (a_2 - a_1)$，我们称整数a_1, a_2模n同余。

定义 2.1.1" 设$n \in N^+$，如果$\exists k \in Z$，使得$a_2 = a_1 + kn$，我们称整数a_1, a_2模n同余。

同余的一些简单性质

定理 2.1.1 同余关系是一种等价关系，即它满足以下三条性质：

(1) 自反性 $a \equiv a \pmod n$；

(2) 对称性 如果 $a \equiv b \pmod n$，则 $b \equiv a \pmod n$；

(3) 传递性 如果 $a \equiv b \pmod n$，$b \equiv c \pmod n$，则 $a \equiv c \pmod n$。

定理 2.1.2 设$m\in N^+$，若$a\equiv b(\bmod m)$， $c\equiv d(\bmod m)$， $k\in Z$，

加减乘

(1) 则有$a+c\equiv b+d(\bmod m)$，特别地有$a+k\equiv b+k(\bmod m)$。

(2) 则有$ac\equiv bd(\bmod m)$，特别地有$ak\equiv bk(\bmod m)$以及$\forall n\in N^+$，$a^n\equiv b^n(\bmod m)$。

(3) 若$f(x)=a_nx^n+\cdots+a_1x+a_0$， $g(x)=b_nx^n+\cdots+b_1x+b_0$为整系数多项式，并且$\forall 0\le i\le n$， $a_i\equiv b_i(\bmod m)$，则$\forall x_1\equiv x_2(\bmod m)$，有$f(x_1)\equiv g(x_2)(\bmod m)$。

(4) 若n为非零整数，则有$a\equiv b(\bmod m)\Leftrightarrow an\equiv bn(\bmod nm)$。

(5) 若 $n|m$， 则 $a\equiv b(\bmod n)$。 特别地， 若 $l\in N^+$， $a\equiv b(\bmod m^l)$， 则有$a\equiv b(\bmod m)$。

定理 2.1.3 设$m\in N^{+}$，$\forall 1\le i\le n$，$m_i\in N^{+}$，

(1) 若$a\equiv b(\bmod m)$，则$(a,m)=(b,m)$；

(2) $\forall 1\le i\le n$，$a\equiv b(\bmod m_i)\Leftrightarrow a\equiv b(\bmod [m_1,\cdots,m_n])$。

证明：

(1) 注意到可设$a=b+sm$，$s\in Z$。

(2) 利用同余的定义和最小公倍数的性质。

为了求解形如 $ax \equiv b \pmod{m}$ 这样的同余方程，我们建立下述定理。

定理 2.1.4 设 $m \in N^{+}$，

(1) 若 $k \in Z$，$ak \equiv bk \pmod{m}$，则 $a \equiv b \pmod{\frac{m}{(k,m)}}$，

特别地，若 $(k,m)=1$，则 $a \equiv b \pmod{m}$；

(2) 若 $a \in Z$，$(a,m)=1$，则在模 m 的意义下存在唯一的整数 a^{-1}，使得

$$aa^{-1} = a^{-1}a \equiv 1 \pmod{m}。$$

证明：(1) 利用同余的定义及整除的性质。

(2) 先证存在性，再证唯一性。

我们把满足$ax = xa \equiv 1 \pmod{m}$的整数称为$a$模$m$的逆元（简称$a$的逆）。

推广的Euclid算法

定理 2.1.4' 设$m \in N^{+}$，若$(a,m)=1$，则a在模m的意义下存在唯一的逆元；若$(a,m)\neq 1$，则a没有模m的逆元。

前述的性质并不十分困难，但却是重要的。我们可以举出如下的例证：

整系数多项式同余方程 $a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$ 是同余理论中的一个核心课题，从前述的基本性质中，我们至少可以推知以下的认识：

(1) 若 x_0 为 $f(x) \equiv 0 \pmod{m}$ 的解，则 $\forall y \equiv x_0 \pmod{m}$，都有 $f(y) \equiv 0 \pmod{m}$，也就是整系数多项式同余方程的解数是模的意义下的；

(2) 一次同余方程 $ax \equiv b \pmod{m}$，在 $(a,m)=1$ 时的解为 $a^{-1}b \pmod{m}$，此时解数在模 m 的意义下为 1；

(3) 若 $(m,a_n)=1$，则 $a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$

与 $x^n + a_n^{-1}a_{n-1}x^{n-1} + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0 \equiv 0 \pmod{m}$

是同解方程；

(4) 若 $l \in N^+$，$f(x) \equiv 0 \pmod{m^l}$ 的解必为 $f(x) \equiv 0 \pmod{m}$ 的解，这就为探讨解的结构提供了一种可能性。

下面我们运用集合的语言刻画同余这一关系，引入同余类的概念。

对于整数i，记$\bar{i}=\{x: x\in Z, x\equiv i(\bmod n)\}$。

定义 2.1.2 我们把每个集合$\bar{i}$叫作模n的一个同余类。

如果$(i,n)=1$，这样的同余类叫模n的缩同余类。

由定义易知：

(1) 模n至多有n个两两不同的同余类，它们的并集就是Z；

(2) 由定理 2.1.3(1)知，缩同余类$\bar{i}$中每个整数均与n互素；

(3) 缩同余类的个数即为$0,1,2,\cdots,n-1$这n个数当中与n互素的数的个数，

我们把这个数表示成$\varphi(n)$，叫作 Euler 函数。

例 1 (1) $n=8$，模n有 8 个两两不同的同余类

(2) $n=7$，模n有 7 个两两不同的同余类

$$\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\text{，}$$

其中有 6 个缩同余类

$$\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\text{，}$$

所以$\varphi(7)=6$。

一般地，若 p 为素数，则模 p 共有 $p-1$个缩同余类$\overline{1},\overline{2},\cdots,\overline{p-1}$，即$\varphi(p)=p-1$。

恰当的分类能够促使人们更好地研究事物的特性，这一看法将在后续的内容中不断地得以印证。作为一个例子，我们来看如何通过恰当的分类获得 Euler 函数的一个性质。

定理 2.1.5 求证：对任意正整数 n 有 $\sum_{d|n,d>0}\varphi(d)=n$。

证明：设 m 是 $1,2,3,\cdots,n$ 中任意一个数，我们可以按照 (m,n) 的不同对 $1,2,\cdots,n$ 进行分类。

注意此时，

n 的正因子的个数即为所得的类的个数；

各类中正整数的个数之和即为 n。

对各类中正整数的个数进行计数即可。

取 $n = 20$，则下表给出整数集$\{1,2,3,\cdots,20\}$按照其与 20 的最大公约数进行的分类：

d	a: $(a,20)=d$
1	
2	
4	
5	
10	
20	

定义 2.1.3 n个整数$a_1,a_2,\cdots,a_n$叫作模n的完全剩余系（简称完系），是指

$a_1,a_2,\cdots,a_n$彼此模n不同余。

$\varphi(n)$个整数$b_1,b_2,\cdots,b_{\varphi(n)}$叫作模$n$的既约剩余系（简称缩系），是指

$b_1,b_2,\cdots,b_{\varphi(n)}$彼此模$n$不同余，且均与$n$互素。

由同余类、完系、缩系的定义，我们有

定理 2.1.6 设$m\in N^+$，$\overline{a},\overline{b}$为模$m$的同余类，则有

$$\overline{a}=\overline{b}\Leftrightarrow a\equiv b(\bmod m)。$$

定理 2.1.7 设 $m\ge 2$， $m\in N^+$， $(n,m)=1$，

$$\{r_k:1\le k\le \varphi(m)\}=\{l:1\le l\le m-1, 且(l,m)=1\},$$

则有

(1) $\overline{a_1},\overline{a_2}$ 为模 m 的两个不同的同余类 $\Leftrightarrow$ $\overline{na_1},\overline{na_2}$ 为模 m 的两个不同的同余类。

(2) $a_1,\cdots,a_m$ 为模 m 的一个完系 $\Leftrightarrow$ $na_1,\cdots,na_m$ 为模 m 的一个完系；

$a_1,\cdots,a_{\varphi(m)}$ 为模 m 的一个缩系 $\Leftrightarrow$ $na_1,\cdots,na_{\varphi(m)}$ 为模 m 的一个缩系。

(3) $a_1,\cdots,a_m$ 为模 m 的一个完系 $\Leftrightarrow$ $\{\overline{a_1},\cdots,\overline{a_m}\}=\{\overline{0},\cdots,\overline{m-1}\}$；

$a_1,\cdots,a_{\varphi(m)}$ 为模 m 的一个缩系 $\Leftrightarrow$ $\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}=\{\overline{r_1},\cdots,\overline{r_{\varphi(m)}}\}$。

(4) $a_1,\cdots,a_m$ 为模 m 的一个完系 $\Leftrightarrow$ $\{\overline{na_1},\cdots,\overline{na_m}\}=\{\overline{0},\cdots,\overline{m-1}\}$；

$a_1,\cdots,a_{\varphi(m)}$ 为模 m 的一个缩系 $\Leftrightarrow$ $\{\overline{na_1},\cdots,\overline{na_{\varphi(m)}}\}=\{\overline{r_1},\cdots,\overline{r_{\varphi(m)}}\}$。

例 **2** (1) $n=6$时，

$0,1,2,3,4,5$为模 6 的完系，对应的

(2) $n=11$时，

定理 2.1.8（Wilson 定理）若 p 为素数，则 $(p-1)! \equiv -1 (\bmod p)$。

证明：当 $p=2$ 时结论显然成立。

当 $p \geq 3$ 时，对于每个 a，$1 \leq a \leq p-1$，考虑其唯一的逆 $a^{-1}, 1 \leq a^{-1} \leq p-1$。

例 3 $p=11$时，在$1,2,3,4,5,6,7,8,9,10$中，只有

下面我们定义同余类的加法以及乘法，并揭示出其可能的代数结构。

定义 2.1.4 设$\overline{a},\overline{b}$为模$m$的同余类，定义加法（“$\oplus$”）为

$$\overline{a}\oplus\overline{b}=\overline{a_1+b_1},$$

其中$a_1\in\overline{a}$，$b_1\in\overline{b}$；定义乘法（“$\odot$”）为

$$\overline{a}\odot\overline{b}=\overline{a_1b_1},$$

其中$a_1\in\overline{a}$，$b_1\in\overline{b}$。

由同余的性质以及定理 2.1.6 知上述的定义与a_1,b_1的选择无关。

定理 2.1.9 设$a_1,\cdots,a_{\varphi(m)}$为模$m$的一个缩系，则有

(1) $\forall\overline{x},\overline{y}\in\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$，有$\overline{x}\odot\overline{y}\in\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$；

(2) $\forall\overline{x}\in\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$，有$\overline{x^{-1}}\in\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$。

设$a_1,\cdots,a_p$为模素数p的一个完系，则在集合$\{\overline{a_1},\cdots,\overline{a_p}\}$中，同余类的加法满足：

I(1) 可交换 $\overline{a}\oplus\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}\oplus\overline{a}$；

I(2) 可结合 $(\overline{a}\oplus\overline{b})\oplus\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}\oplus\overline{b+c}=\overline{a}\oplus(\overline{b}\oplus\overline{c})$；

I(3) 存在零元 $\exists\overline{0}\in\{\overline{a_1},\cdots,\overline{a_p}\}$，$\forall\overline{a}$，有$\overline{a}\oplus\overline{0}=\overline{0}\oplus\overline{a}=\overline{a}$；

I(4) 存在负元 $\forall\overline{a}$，$\exists\overline{-a}\in\{\overline{a_1},\cdots,\overline{a_p}\}$，使得$\overline{a}\oplus\overline{-a}=\overline{-a}\oplus\overline{a}=\overline{0}$。

同余类乘法满足：

II(1) 可交换 $\overline{a}\cdot\overline{b}=\overline{ab}=\overline{ba}=\overline{b}\cdot\overline{a}$；

II(2) 可结合 $(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{ab}\cdot\overline{c}=\overline{(ab)c}=\overline{a(bc)}=\overline{a}\cdot\overline{bc}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$；

II(3) 存在单位元 $\exists\overline{1}\in\{\overline{a_1},\cdots,\overline{a_p}\}$，$\forall\overline{a}$，有$\overline{a}\cdot\overline{1}=\overline{1}\cdot\overline{a}=\overline{a}$；

II(4) 非零元有逆元

$\forall\overline{a}\neq\overline{0}$，由于$(a,p)=1$，故存在$a^{-1}$使得$aa^{-1}=a^{-1}a\equiv 1(\mathrm{mod}\ p)$，所以

$\exists\overline{a^{-1}}$使得$\overline{a}\cdot\overline{a^{-1}}=\overline{a^{-1}}\cdot\overline{a}=\overline{1}$。

乘法对于加法还满足：

III(1) 左分配律

$$\overline{a}\odot(\overline{b}\oplus\overline{c})=\overline{a(b+c)}=\overline{ab+ac}=\overline{ab}\oplus\overline{ac}=(\overline{a}\odot\overline{b})\oplus(\overline{a}\odot\overline{c});$$

III(2) 右分配律

$$(\overline{b}\oplus\overline{c})\odot\overline{a}=\overline{(b+c)a}=\overline{ba+ca}=\overline{ba}\oplus\overline{ca}=(\overline{b}\odot\overline{a})\oplus(\overline{c}\odot\overline{a})。$$

特殊地考虑 $p=2$ 时的情形。

这时集合 $\{\overline{0},\overline{1}\}$ 中的加法，乘法的具体运算如下：

$\overline{0}\oplus\overline{0}=\overline{0}$，$\overline{0}\oplus\overline{1}=\overline{1}$，$\overline{1}\oplus\overline{0}=\overline{1}$，$\overline{1}\oplus\overline{1}=\overline{0}$

$\overline{0}\odot\overline{0}=\overline{0}$，$\overline{0}\odot\overline{1}=\overline{0}$，$\overline{1}\odot\overline{0}=\overline{0}$，$\overline{1}\odot\overline{1}=\overline{1}$

这是元素最少的一个域。

如果设 $m\in N^{+}$，$a_1,\cdots,a_m$ 为模 m 的一个完系，那么定义在 $\{\overline{a_1},\cdots,\overline{a_m}\}$ 中的同余类的加法和乘法满足

I(1), I(2), I(3), I(4), II(2), III(1), III(2)，

这时构成了一个有限环。由于乘法还满足 II(1), II(3)，所以更确切地讲，它是一个含单位元的有限交换环。

如果只考虑 $\{\overline{a_1},\cdots,\overline{a_m}\}$ 以及定义在其中的加法运算，由于其满足

I(2), I(3), I(4)，

这时构成一个有限加法群。由于它还满足 I(1)，所以这个加法群是 Abel 群。

如果 $a_1,\cdots,a_{\varphi(m)}$ 为模 m 的一个缩系，考虑 $\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$ 以及定义在其中的乘法运算，易知其满足 II(2), II(3)，由定理 2.1.9 可知 $\{\overline{a_1},\cdots,\overline{a_{\varphi(m)}}\}$ 对于乘法运算是封闭的并且满足 II(4)，这时构成一个有限乘法群。由于它还满足 II(1)，所以这个乘法群是 Abel 群。

如果不产生歧义，我们可以用$\overline{a}+\overline{b}$替代$\overline{a}\oplus\overline{b}$，用$\overline{a}\,\overline{b}$替代$\overline{a}$□ $\overline{b}$。

例 4 $n=10$，$\{\overline{1},\overline{3},\overline{7},\overline{9}\}$为模 10 的缩同余类集合，构造其乘法表如下：

	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$				
$\overline{3}$				
$\overline{7}$				
$\overline{9}$				

例 5 求解一次同余方程$3x \equiv 9 \pmod{10}$

解：对于同余方程$3x \equiv 9 \pmod{10}$的求解，可在其两边同时乘上 3 模 10 的逆元 7，即

例 6 求解一次同余方程$60x \equiv 7 \pmod{37}$。

解： 因为$(60,37)=1$，所以该同余方程有解。

下面我们用两种方法来求解。

方法一：利用推广的 Euclid 算法可求得$60^{-1} \equiv -8 \pmod{37}$,故而该同余方程的解为

$$x \equiv 7 \times (-8) \equiv -56 \equiv 18 \pmod{37}。$$

方法二：由于$(60,37)=1$，由前面的讨论知此时可以作除法，即 60 可以作分母，从而

$$x \equiv \frac{7}{60} \equiv$$

在解决整除问题时，

同余符号的应用有时比整除符号更为方便。