第 2 章　同余

本章主要描述同余理论的基本概念及基本性质. 我们除了介绍与同余相关的基本概念如同余、同余式、同余类、完全剩余系、既约剩余系以外，还重点描述了几种构造完全剩余系、既约剩余系的方法. 另外，根据同余的基本性质，得到了两个重要的定理 Euler 定理与 Wilson 定理.

§1 同余

定义 1 给定正整数 m. 若 $m \mid a-b$，则称 a 同余于 b 模 m, b 是 a 对模 m 的剩余，记作

$$a \equiv b(\operatorname{mod} m). \tag{1}$$

否则，则称 a 不同余于 b 模 m，或 b 不是 a 对模 m 的剩余，记作 $a \not\equiv b(\operatorname{mod} m)$. 关系式（1）称为**模 m 的同余式**，简称**同余式**。当 $0 \le b < m$，称 b 是 a 对模 m **最小非负剩余**；当 $1 \le b \le m$，则称 b 是 a 对模 m 的**最小正剩余**；当 $-m/2 < b \le m/2$（或 $-m/2 \le b < m/2$），则称 b 是 a 对模 m 的**绝对最小剩余**.

定理 1　a 同余于 b 模 m 的充要条件是 a 和 b 被 m 除后所得的最小非负余数相等，即若

$$a = q_1 m + r_1, \quad 0 \le r_1 < m;$$

$$b = q_2 m + r_2, \quad 0 \le r_2 < m,$$

则 $r_1 = r_2$.

证明　由

$$a-b = (q_1 - q_2)m + (r_1 - r_2)$$

知 $m \mid a-b$ 的充要条件是 $m \mid r_1 - r_2$，由此及 $0 \le |r_1 - r_2| < m$，即得 $r_1 = r_2$.

从定理 1 看出，也可以用最小非负余数相等来定义同余. 给定模 m，根据定义立即推出同余式有以下简单的性质.

性质 1　同余是一种等价关系，即

（1）自反性　$a \equiv a(\operatorname{mod} m)$；

(2)　对称性　$a \equiv b(\operatorname{mod} m) \Leftrightarrow b \equiv a(\operatorname{mod} m)$；

(3)　传递性　$a \equiv b(\operatorname{mod} m), b \equiv c(\operatorname{mod} m) \Rightarrow a \equiv c(\operatorname{mod} m)$.

性质 2　同余式可以相加减，即若有

$$a \equiv b \pmod m, \quad c \equiv d \pmod m, \tag{2}$$

则 $a \pm c \equiv b \pm d \pmod m$.

性质 3　同余式可以相乘，即若式（2）成立，则有

$$ac \equiv bd \pmod m .$$

根据以上性质，我们立即可以得到

定义 2　设

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_n x^n + \cdots + b_0$$

是两个整系数多项式，满足

$$a_j \equiv b_j \pmod m, \qquad 0 \le j \le n .$$

则称**多项式 $f(x)$ 同余于多项式 $g(x)$ 模 m .**

显然，若 $a \equiv b \pmod m$ ，则

$$f(a) \equiv g(b) \pmod m .$$

性质 4　设 $d \ge 1$，$d \mid m$，若同余式（1）成立，则

$$a \equiv b \pmod d .$$

性质　5　同余式

$$ca \equiv cb \pmod m \tag{3}$$

等价于

$$a \equiv b \pmod{m/(c,m)} .$$

特别地，当 $(c,m) = 1$ 时，$a \equiv b \pmod m$.

证明　同余式（3）等价于 $m \mid c(a-b)$ ，从而等价于

$$\frac{m}{(c,m)} \left| \frac{c}{(c,m)}(a-b) \right. .$$

由 $(m/(c,m), c/(c,m)) = 1$ 知，这等价于

$$\frac{m}{(c,m)}\Big|a-b\,.$$

这就证明了所要的结论.

从性质 5 知，当$(c,m)=1$时，式（3）满足消去律.

性质 6　若$m\geq 1$，$(a,m)=1$，则存在c使得

$$ca\equiv 1(\mathrm{mod}\, m)\ .$$

我们把c称为a**对模**m**的逆**，记作$a^{-1}(\mathrm{mod}\, m)$或a^{-1}.

证明　由 Euclid 算法知，存在x_0,y_0，使得

$$ax_0+my_0=1,$$

取$c=x_0$即满足要求.

由此提供一种求$a^{-1}(\mathrm{mod}\, m)$有效的方法，这是 Euclid 算法的又一重要应用.

例 1 求模11的所有元的逆元.

解 由$1\times(-10)+11=1$ 得

$$1^{-1}\equiv(-10)\equiv 1(\mathrm{mod} 11)\ ;$$

由$2\times(-5)+11=1$ 得

$$2^{-1}\equiv(-5)\equiv 6(\mathrm{mod} 11)\ ;$$

同样计算得

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

性质 7　同余式组

$$a\equiv b(\mathrm{mod}\, m_j),\quad j=1,\ 2\cdots,\ k$$

同时成立的充要条件是

$$a\equiv b(\mathrm{mod}[m_1,\cdots,m_k])\,.$$

证明　由公倍数一定是最小公倍数的倍数知，

$$m_j \mid a-b\,,\quad j=1,\cdots,k$$

同时成立的充要条件是

$$[m_1,\cdots,m_k] \mid a-b\,.$$

下面例子提供了一种利用同余运算判断一个数 n 能否被 9 整除的判别法.

例 2 设 n 为整数，试求出它能为 9 整除的判别法.

解 设

$$n = a_0 10^k + a_1 10^{k-1} + \cdots + a_{k-1}10 + a_k\,.$$

因为

$$10^i \equiv 1 \pmod 9, 1 \le i \le k\,,$$

所以由性质 4 得

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod 9\,.$$

故只要

$$0 \equiv a_0 + a_1 + \cdots + a_k \pmod 9\,,$$

则 n 可被 9 整除．从例 2 同样也可以推出 n 被 3 整除的充要条件为

$$0 \equiv a_0 + a_1 + \cdots + a_k \pmod 3\,,$$

这就是我们早已熟知的判断整数被 3 整除的方法.

例 3 求 $6^{125} \bmod 41$ 和 $5^{111} \bmod 23$.

解 首先找到一个正整数 d，满足

$$6^d \equiv 1 \pmod{41}\,.$$

由

$$6^2 \equiv -5 \pmod{41}\,;\quad 6^4 \equiv 25 \pmod{41}\,;\quad 6^5 \equiv 27 \pmod{41}\,;$$

$$6^{10} \equiv -9 \pmod{41}\,;\quad 6^{20} \equiv -1 \pmod{41}\,;\quad 6^{40} \equiv 1 \pmod{41}\,.$$

可取 $d = 40$，从而

$$6^{40\times 3+5} \equiv 27 \pmod{41}\,.$$

由

$$5^2 \equiv 2 \pmod{23}\,;\quad 5^4 \equiv 4 \pmod{23}\,;\quad 5^8 \equiv -7 \pmod{23}\,;$$

$$5^{16} \equiv 3 \pmod{23}；\quad 5^{20} \equiv 12 \pmod{23}；\quad 5^{22} \equiv 1 \pmod{23}；$$

取 $d = 22$，所以

$$5^{22\times5+1} \equiv 5 \pmod{23}.$$

注 关于模 m 的幂运算 $a^x \pmod{}$，第 12 章将给出一种有效的计算并给出时间估计.

例 4 求最小的 $m+n$，使得 $104 \mid 168^m - 168^n$.

解 求 $104 \mid 168^m - 168^n$ 即要求如下同余式

$$168^n \times (168^{m-n} - 1) = (2^3 \times 3 \times 7)^n \times (168^{m-n} - 1) \equiv 0 \pmod{2^3 \times 13}$$

等价于

$$\begin{cases} (2^3 \times 3 \times 7)^n \times (168^{m-n} - 1) \equiv 0 \pmod{2^3}, \\ (2^3 \times 3 \times 7)^n \times (168^{m-n} - 1) \equiv 0 \pmod{13}. \end{cases}$$

由于

$$(2^3, (3\times7)^n \times (168^{m-n} - 1)) = 1，\quad (2^3 \times 3 \times 7)^n, 13) = 1，$$

满足性质 4 中消去律的条件．所以同余式等价于

$$\begin{cases} 2^{3n} \equiv 0 \pmod{2^3}, \\ 168^k - 1 \equiv 0 \pmod{13}. \end{cases}$$

容易验证第一个方程有解的最小的 n 为 1；第二个方程有解的最小 k 为 2，所以使 $104 \mid 168^m - 168^n$ 成立的最小的 $m+n = (1+2)+1 = 4$.

§2 剩余类与剩余系

根据同余的定义，可以对整数进行分类-剩余类（同余类）．本节主要描述与剩余类有关的概念与特性．

定义 1 所有对 m 同余的数组成的集合称为是**模 m** 的一个**剩余类（同余类）**，我们以 $r \bmod m$ 表 r 所属的模 m 的剩余类．如果 $(r, m) = 1$，模 m 的同余类 $r \bmod m$ 称为是模 m 的既约（或互素）剩余类．模 m 的所有既约剩余类的个数记为 $\phi(m)$，$\phi(m)$ 通常称为 **Euler 函数.**

显然$\phi(m)$等于不超过m的正整数中所有与m互素的整数的个数．关于模m的剩余类，有下列性质．

性质 8　给定模m，有且仅有m个不同的模m的剩余类，且满足

(1) $Z=\bigcup_{r=0}^{m-1} r \bmod m$；

(2) $i \bmod m \bigcap j \bmod m=\phi,\ 0\le i,\ j<m, i\ne j$．

性质 8 即为第 1 章第 1 节中描述的将全体整数按最小非负余数进行分类的另一种描述形式．通常

$$0 \bmod m, 1 \bmod m, \cdots, (m-1) \bmod m$$

也简记为$\bar{0}, \bar{1}, \cdots, \overline{m-1}$或$0,1,\cdots,(m-1)$．

定义 2 在模m每个剩余类$\bar{i}$中，任取$a_i\in\bar{i}, 0\le i<m$，则$a_0, a_1, ..., a_{m-1}$为模m的一个**完全剩余系**，记作Z_m．通常，称$0,1,2,\cdots,m-1$为**模m最小非负（完全）剩余**；$1,2,3,\cdots,m-1,m$为**模m最小正剩余系**；$-[\frac{m}{2}],-[\frac{m}{2}]+1,...,0,1,...[\frac{m}{2}]-1$或$-[\frac{m}{2}]+1,-[\frac{m}{2}]+2,...,0,1,...[\frac{m}{2}]$为**模$m$绝对最小剩余系**。

显然，若$a_0,a_1,...,a_{m-1}$为一个完全剩余系，任给$a\in Z$，有且仅有一个$a_i, 0\le i<m-1$是a对模m的剩余．

定义 3 设在模m每个简化剩余类$\overline{k_i}$中，任取$a_i\in\overline{k_i}, 0\le i<\varphi(m),$，则$a_0,a_1,...,a_{\varphi(m)-1}$一组数称为是模$m$的**简化（既约）剩余系**，记作$Z_m^*$．

显然，若$a_0,a_1,...,a_{\varphi(m)}$为一个简化剩余系，任给$a\in Z, (a,m)=1$，有且仅有一个$a_i, 0\le i<\varphi(m)$是$a$对模$m$的剩余．

以下定理提供了一种判断模m完全剩余系与简化剩余系的一种最为常用的方法．

定理 1　(1)　m个整数组成模m的一个完全剩余系的充要条件是m个数两两对模m不同余．

(2)　$\phi(m)$个整数组成模m的一个既约剩余系的充要条件是$\phi(m)$个数两两对模m不同

余，且这$\phi(m)$个数都与m互素.

证明 （1）设$y_0,\cdots,y_{m-1}$两两不同余，则由鸽巢原理知，$y_0,\cdots,y_{m-1}$分别属于m个不同的剩余系中，由完全剩余系的定义知，$y_0,\cdots,y_{m-1}$构成一个完全剩余系.

（2）证明与(1)类似.

定理 2 （1）设a, b是任意整数，且$(a, m)=1$，那么x遍历模m的一组完全剩余系时，$ax+b$遍历模m的一组完全剩余系.

（2）设a, b是任意整数，且$(a,m)=1$，那么x遍历模m的一组简化剩余系时，$ax+bm$也遍历模m的一组简化剩余系.

证明（1)假设$x_0,x_1,\cdots,x_{m-1}$为模m的一个完全剩余系，则$x_0,x_1,\cdots,x_{m-1}$两两不同余. 由$(a,m)=1$知 $ax_i+b\equiv ax_j+b$ 当且仅当 $x_i\equiv x_j$， 所以

$$ax_0+b,\ldots, ax_{m-1}+b$$

两两不同余．再由定理 1 即可推出（1）成立.

（2）若$x_0,x_1,\cdots,x_{\varphi(m)-1}$为模$m$简化剩余系，则$x_0,x_1,\cdots,x_{\varphi(m)-1}$两两不同余．由$(a,m)=1$知，

$$ax_0+bm,\cdots,\quad ax_{\varphi(m)-1}+bm$$

两两不同余，且满足

$$(ax_i+bm,m)=1,\quad 0\le i\le\varphi(m)\text{，}$$

同样由定理 1 即可推出（2）成立.

定理 3 设$m=m_1m_2$， $(m_1,m_2)=1$．当 $x_i^{(1)}(0\le i\le m_1-1)$遍历模$m_1$的完全（既约）剩余系，$x_j^{(2)}$（$0\le j\le m_2-1$）遍历模$m_2$的完全（既约）剩余系时，

$$x_{ij}=m_2x_i^{(1)}+m_1x_j^{(2)}$$

遍历模m的完全（既约）剩余系.

证明 首先证明当$x_i^{(1)}(0\le i\le m_1-1)$，$x_j^{(2)}$（$0\le j\le m_2-1$）分别为模$m_1$、$m_2$的完全剩余系时，

$$x_{ij}=m_2x_i^{(1)}+m_1x_j^{(2)},0\le i<m_1,0\le j<m_2$$

构成模 m 的完全剩余系．显然 x_{ij} 共有 $m=m_1m_2$ 个数，因此只要证明它们两两对模 m 不同余．若

$$m_2x_{i_1}^{(1)}+m_1x_{j_1}^{(2)}\equiv x_{i_1j_1}\equiv x_{i_2j_2}\equiv m_2x_{i_2}^{(1)}+m_1x_{j_2}^{(2)}(\bmod m_1m_2)\quad,$$

则

$$x_{i_1j_1}\equiv x_{i_2j_2}(\bmod m_1)，\ x_{i_1j_1}\equiv x_{i_2j_2}(\bmod m_2)\,.$$

从而

$$m_2x_{i_1}^{(1)}\equiv m_2x_{i_2}^{(1)}(\bmod m_1),\qquad m_1x_{j_1}^{(2)}\equiv m_1x_{j_2}^{(2)}(\bmod m_2).$$

由 $(m_1,m_2)=1$ 知，

$$x_{i_1}^{(1)}\equiv x_{i_2}^{(1)}(\bmod m_1)，\ x_{j_1}^{(2)}\equiv x_{j_2}^{(2)}(\bmod m_2)\,.$$

这就证明了 m_1m_2 个 x_{ij} 两两不同余，是模 m 的完全剩余系．

下面证明 $x_i^{(1)}$，$x_j^{(2)}$ 分别遍历 m_1，m_2 的既约剩余系时，x_{ij} 是模 m 的既约剩余系．由以上证明知 x_{ij} 两两不同余．只要证明 $(x_{ij},m)=1$ 当且仅当 $(x^{(1)},m_1)=(x^{(2)},m_2)=1$．由于

$$(m_1,m_2)=1，\ (x^{(1)},m_1)=(x^{(2)},m_2)=1\,,$$

所以 $(x_{ij},m)=1$ 当且仅当

$$(m_2x^{(1)}+m_1x^{(2)},m_1)=1，\ (m_2x^{(1)}+m_1x^{(2)},m_2)=1$$

当且仅当

$$(x^{(1)},m_1)=(x^{(2)},m_2)=1\,.$$

定理得证．

容易证明，定理 2、3 的条件为充要条件．

定理 4 设 $m=m_1\cdots m_k$， $m_1,\cdots,m_k$ 两两既约．再设 $m=m_jM_j$，$1\le j\le k$，及

$$x=M_1x^{(1)}+\cdots+M_kx^{(k)}\,,\qquad（1）$$

那么 x 遍历模 m 的完全（既约）剩余系的充要条件是 $x^{(1)}$，…，$x^{(k)}$ 分别遍历 m_1，…，m_k 的

完全（既约）剩余系.

证明 当 $k=2$ 时，由定理 3 知结论成立．设 $k=n(n\ge 2)$ 时，定理成立，当 $k=n+1$ 时，

$m=m_1\cdots m_n m_{n+1}$，设 x 由式（1）给出，

$$\bar{x}^{(n)}=\frac{m}{m_1 m_{n+1}}x^{(1)}+\cdots+\frac{m}{m_n m_{n+1}}x^{(n)},$$

由定理 3 得

$$x=m_{n+1}\bar{x}^{(n)}+\frac{m}{m_{n+1}}x^{(n+1)}.$$

由以上两式就推出所要结论.

下面我们描述构造完全剩余系与既约剩余系的另外一种特别的方法.

定理 5 设 $m=m_1 m_2$，$x_i^{(1)}$，$1\le i\le m_1$ 遍历模 m_1 的完全剩余系，$x_j^{(2)}$，$1\le j\le m_2$ 遍历模 m_2 的完全剩余系，那么

$$x_{ij}=x_i^{(1)}+m_1 x_j^{(2)}$$

遍历模 m 的完全剩余系.

一般地，若 $m=m_1\cdots m_k$，

$$x=x^{(1)}+m_1 x^{(2)}+\cdots+m_1 m_2\cdots m_{k-1}x^{(k)},$$

那么 $x^{(1)}$，…，$x^{(k)}$ 分别遍历 m_1，…，m_k 的完全剩余系时，x 遍历模 m 的完全剩余系.

证明 我们先证明 $k=2$ 时，定理成立．此时，x_{ij} 共有 $m=m_1 m_2$ 个，因此只需证明他们两两不同余．若

$$x_{i_1}^{(1)}+m_1 x_{j_1}^{(2)}\equiv x_{i_1 j_1}\equiv x_{i_2 j_2}\equiv x_{i_2}^{(1)}+m_1 x_{j_2}^{(2)}\pmod{m_1 m_2} \qquad （3）$$

则必有

$$x_{i_1}^{(1)}\equiv x_{i_2}^{(1)}\pmod{m_1},$$

因为 $x_{i_1}^{(1)},x_{i_2}^{(1)}$ 在同一个模的完全剩余系中取值，即 $x_{i_1}^{(1)}=x_{i_2}^{(1)}$，再由（3）式得

$$m_1 x_{j_1}^{(2)}\equiv m_1 x_{j_2}^{(2)}\pmod{m_1 m_2},$$

即 $x_{j_1}^{(2)} \equiv x_{j_2}^{(2)} (\bmod m_2)$，同理有 $x_{j_1}^{(2)} = x_{j_2}^{(2)}$，这就证明了定理前半部分.

假设设 $k = n(n \geq 2)$ 时，定理成立，当 $k = n+1$ 时，$m = m_1 \cdots m_n m_{n+1}$，

$$\overline{x}^{(n)} = x^{(1)} + m_1 x^{(2)} + \cdots + m_1 \cdots m_{n-1} x^{(n)}.$$

由前半部分证明知

$$x = \overline{x}^{(n)} + m_1 \cdots m_{n-1} m_n x^{(n+1)}.$$

由以上两式就得到所要结论.

注 定理 5 仅是一个充分条件，不一定是必要条件.

定理 3、4、5 表明大模的完全（简化）剩余系，可以某种形式表为两个较小的模的完全剩余系的组合. 实际上，大模 m 的完全（简化）剩余系的构造可进一步通过 m 的素分解及模 m 的素数幂的原根来构造. 另外，定理 5 所描述的完全（既约）剩余系可以应用于某类公钥加密算法.

最后，我们讨论以下模 m 的剩余系与其因子的剩余系之间的关系.

定理 6 设 $m_1 \mid m$. 那么对任意的 r 有

$$r \bmod m \subseteq r \bmod m_1,$$

等号仅当 $m_1 = m$ 时成立.

若 $l_{0,} \cdots, l_{d-1}$ 是模 $d = m/m_1$ 的一组完全剩余系，则

$$r \bmod m_1 = \bigcup_{0 \leq j \leq d-1} (r + l_j m_1) \bmod m, \tag{1}$$

右边和式中的 d 个模 m 的同余类两两不同. 特别的有

$$r \bmod m_1 = \bigcup_{0 \leq j < d} (r + j m_1) \bmod m. \tag{2}$$

证明 我们把剩余类 $r \bmod m_1$ 中的数按模 m 来分类. 对 $r \bmod m_1$ 中任意两个数 $r + k_1 m_1, r + k_2 m_1$， 同余式

$$r + k_1 m_1 \equiv r + k_2 m_1 (\bmod m)$$

成立的充要条件是

$$k_1 \equiv k_2 (\bmod d).$$

由此就推出式（1）右边和式中的 d 个模 m 的同余类是两两不相交的，且 $r \bmod m_1$ 中的任一数

$r+km_1$ 必属于其中的一个同余类．另一方面，对任意的 j 必有

$$(r+l_j m_1) \bmod m \subseteq (r+l_j m_1) \bmod m_1 = r \bmod m_1 .$$

定理得证．

例 1 模 $m=5\times 7$，构造 m 的既约剩余系和完全剩余系．

解 令 $m_1=5$，$m_2=7$，$(5,7)=1$，则 $M_1=7$，$M_2=5$，当 $x^{(1)}$，$x^{(2)}$ 分别遍历 5 和 7 的完全（既约）剩余系时，

$$x=M_1x^{(1)}+M_2x^{(2)}=7x^{(1)}+5x^{(2)}$$

遍历 35 的完全（既约）剩余系．

	-3	-2	-1	0	1	2	3
-2	-29	-24	-19	-14	-9	-4	1
-1	-22	-17	-12	-7	-2	3	8
0	-15	-10	-5	0	5	10	15
1	-8	-3	2	7	12	17	22
2	-1	4	9	14	19	24	29

例 2 设 $m>1$，$(m,a)=1$，证明：

（1） 对任意整数 b，$\sum_{x \bmod m}\{\frac{ax+b}{m}\}=\frac{1}{2}(m-1)$；

（2） $\sum_{\substack{x \bmod m\\(x,m)=1}}\{\frac{ax}{m}\}=\frac{1}{2}\phi(m)$．

证明（1）因为 $(m,a)=1$，所以当 x 遍历 m 的完全剩余系时，对任意的整数 b，$ax+b$ 遍历 m 的完全剩余系，所以

$$\sum_{x \bmod m}\{\frac{ax+b}{m}\}=\sum_{0\le i\le m-1}\frac{i}{m}=\frac{1}{2}(m-1).$$

（2）因为 $(m,a)=1$，当 x 遍历 m 的既约剩余系时，ax 遍历 m 的既约剩余系，所以

$$\sum_{\substack{x \bmod m\\(x,m)=1}}\{\frac{ax}{m}\}=\sum_{\substack{1\le i<m\\(i,m)=1}}\frac{i}{m}=\frac{1}{2}\phi(m).$$

§3　Euler 定理

Euler 函数 $\phi(m)$ 在数论中占有很重要的地位，下面我们利用同余理论给出它的一个性质及在已知 m 素分解的情况下的求值公式.

定理 1 （1） 设 p 是素数，$k \ge 1$．那么

$$\phi(p^k) = p^{k-1}(p-1),$$

（2）$\phi(m) = \phi(m_1)\phi(m_2)$，其中 $m = m_1 m_2$，$(m_1, m_2) = 1$.

（3）$\phi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)\cdots p_r^{\alpha_r - 1}(p_r - 1) = m\prod\limits_{p|m}(1-\frac{1}{p})$，

其中 $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$， $p_1,\cdots p_r$ 为不同的素因子.

证明 （1）$\phi(p^k)$等于满足以下条件的 r 的个数：

$$(r, p^k) = 1，1 \le r \le p^k .$$

p 是素数，所以

$$(r, p^k) = 1 \Leftrightarrow (r, p) = 1,$$

即 r 为 p^k 中不能被 p 整除的数，$1, 2, \cdots, p^k$ 中能被 p 整除的数可表示为 $kp, k = 1, 2, \cdots p^{k-1}$，

共 p^{k-1} 个，故

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

（2）由上节定理 3 即得（2）.

（3）由（2）进一步推出若 $m = m_1 m_2 \cdots m_r$， $m_1, m_2, \cdots, m_r$ 两两既约，则

$$\phi(m) = \phi(m_1)\phi(m_2\cdots m_r) = \phi(m_1)\phi(m_2)\cdots\phi(m_r) .$$

特别地，若 $m > 1, m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}, \alpha_j \ge 1$，则

$$\phi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)\cdots p_r^{\alpha_r - 1}(p_r - 1) = m\prod_{p|m}(1-\frac{1}{p}).$$

注 由定理 3. 1 可知，除了 $\phi(1)=\phi(2)=1$，对 $m\geq 3$ 必有 $2\mid\phi(m)$.

推论 给定模 p^k， $a+bp, 1\leq a\leq p-1, 0\leq b\leq p^{k-1}-1$ 为模 p^k 的既约剩余系.

证明 由上节定理 6 知

$$r=a+bp,\quad 1\leq a\leq p-1,\quad 0\leq b\leq p^{k-1}-1 \qquad (1)$$

遍历模 p^k 的既约剩余系．再由定理 1（1）知（1）式恰好构成模 p^k 的既约剩余系.

模 m 的既约剩余系可以取种种不同的形式，但每个既约剩余系中所有数的乘积对模 m 是不变的，即若 $\{r_0,\cdots,r_{\phi(m)-1}\}$，$\{r_0',\cdots,r_{\phi(m)-1}'\}$ 是模 m 的两个既约剩余系，那么必有

$$\prod_{j=1}^{\phi(m)} r_j\equiv\prod_{j=1}^{\phi(m)} r_j' (\operatorname{mod} m) .$$

由此就可推出著名的 Euler 定理.

定理 2 （Euler 定理） 设 $(a,m)=1$， 则有

$$a^{\phi(m)}\equiv 1(\operatorname{mod} m). \qquad (2)$$

证明 取 $r_0,\cdots,r_{\phi(m)-1}$ 是模 m 的一组既约剩余系，由 § 2 定理 2 知，当 $(a,m)=1$ 时，$ar_0,\cdots,ar_{\phi(m)-1}$ 也是模 m 的既约剩余系，因此，

$$\prod_{j=0}^{\phi(m)-1} r_j\equiv\prod_{j=0}^{\phi(m)-1}(ar_j)=a^{\phi(m)}\prod_{j=0}^{\phi(m)-1} r_j (\operatorname{mod} m),$$

由于 $(r_j, m)=1,\ \ j=0,\dots,\phi(m)-1$，所以

$$a^{\phi(m)}\equiv 1(\operatorname{mod} m) .$$

特别当 p 为素数时，$\phi(p)=p-1$，对任意的 a，$(a,\ p)=1$ 有

$$a^{p-1}\equiv 1(\operatorname{mod} p) . \qquad (3)$$

通常把式（3）称为 **Fermat 小定理.**

注 1 在式（2）中取 $a=-1$，得 $(-1)^{\phi(m)}-1\equiv 0(\operatorname{mod} m)$，同样可推出当 $m\geq 3$ 时，必有 $2|\phi(m)$.

2 　定理 2 给出了一种理论上计算 a 对模 m 的逆 a^{-1} 的很方便的方法，即当 $(a,m)=1$ 时，

$$a^{-1} \equiv a^{\phi(m)-1} (\bmod m) . \tag{4}$$

但从计算复杂性的角度来看，上述方法对于多数的模 m 是不有效的，因为在实际计算中，由（4）的计算需要首先计算 $\phi(m)$，而 $\phi(m)$ 的计算往往涉及到分解因子问题.

例 1 设 k 是给定的正整数，证明：一定存在正整数 n 使得

$$\phi(n) = \phi(n+k) .$$

证明 　若 $2 \nmid k$，则 $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，令 $n = k$，则

$$\phi(n+k) = \phi(2k) = \prod_{i-1}^{s} p_i^{\alpha_i - 1}(p_i - 1) = \phi(k) = \phi(n) .$$

若 $2 \mid k$，则 $k = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，令 $n = (p-1)k$， p 为最小的不能整除 k 的素数，设 $p - 1 = 2^{t_0} p_1^{t_1} p_2^{t_2} \cdots p_l^{t_l}$， 　则

$$n + k = pk = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l} p p_{l+1}^{\alpha_{l+1}} \cdots p_s^{\alpha_s} ,$$

$$\phi(n+k) = 2^{\alpha_0 - 1} \prod_{i=1}^{l} p_i^{\alpha_i - 1}(p_i - 1)(p-1) \prod_{j=l+1}^{s} p_j^{\alpha_j - 1}(p_j - 1)$$

$$= 2^{\alpha_0 + t_0 - 1} \prod_{i-1}^{l} p_i^{\alpha_i + t_i - 1}(p_i - 1) \prod_{j=l+1}^{s} p_j^{\alpha_j - 1}(p_j - 1) = \phi(n) \cdot$$

§4 　Wilson 定理

上节我们已经利用模 m 的既约剩余系的性质得到了 Euler 函数 $\phi(m)$ 的特性及 Euler 定理，下面我们再来引入一个关于模 m 的既约剩余系乘积的重要定理.

定理 1（**Wilson 定理**）设 p 是素数， $r_1, \cdots, r_{p-1}$ 是模 p 的既约剩余系，则

$$\prod_{r \bmod p}{}' r \equiv r_1 \cdots r_{p-1} \equiv -1 (\bmod p) \tag{1}$$

特别地有

$$(p-1)! \equiv -1 (\bmod p). \qquad (2)$$

证明　当 $p=2$ 时结论显然成立．设 $p \ge 3$，对于每个 $r_i, 0<i<p$，必有唯一的一个 r_j 使得

$$r_i r_j \equiv 1 (\bmod p) . \qquad (3)$$

使 $r_i = r_j$ 的充要条件是 $r_i^2 \equiv 1(\bmod p).$ 即

$$(r_i - 1)(r_i + 1) \equiv 0 (\bmod p) .$$

由于 p 是素数且 $p \ge 3$，所以上式成立当且仅当

$$r_i - 1 \equiv 0(\bmod p) \text{ 或 } r_i + 1 \equiv 0(\bmod p) .$$

由于素数 $p \ge 3$，所以这两式不能同时成立．因此，在这组模 p 的既约剩余系中，除了

$$r_i \equiv 1,\ -1(\bmod p) \qquad (4)$$

对其它的 r_i 必有 $r_j \ne r_i$ 使式（3）成立．不妨设

$$r_1 \equiv 1(\bmod p)，\ r_{p-1} \equiv -1(\bmod p) .$$

这样，在这组模 p 的既约剩余系中除去满足式（4）的两个数之外，其它的数恰好可按关系式（3）两两分完，即有

$$r_2 \cdots r_{p-2} \equiv 1(\bmod p) .$$

由此就推出式（1）．$1, 2, \cdots, p-1$ 是模 p 的既约剩余系，所以式（2）成立．

对于模 p^l 的剩余系有下面相同的结果

定理 2 设素数 $p \ge 3$，$c = \phi(p^l), l \ge 1$，以及 $r_1, r_2, \cdots, r_c$ 是模 p^l 的一组既约剩余系．我们有

$$r_1 r_2 \cdots r_c \equiv -1(\bmod p^l) . \qquad (5)$$

特别的有

$$\prod_{r=1}^{p-1} \prod_{s=0}^{p^{l-1}-1} (r+ps) \equiv -1(\bmod p^l). \qquad (6)$$

在定理 2 的符号和条件下，我们有 $c=\phi(p^l)=\phi(2p^l)$. 取

$$r_j{}'=\begin{cases} r_j, & \text{当} r_j \text{不是偶数}, \\ r_j+p^l, & \text{当} 2 \mid r_j. \end{cases}$$

显见，$r_j{}'(1\le j\le c)$ 仍是模 p^l 的一组既约剩余系，且都是奇数．因此它也是模 $2p^l$ 的一组既约剩余系．且有

$$r_1'\cdots r_c'\equiv -1(\bmod 2p^l).$$

所以我们有

定理 3 设素数 $p\ge 3$, $l\ge 1$, $c=\phi(2p^l)$, 以及 $r_1, r_2, \cdots, r_c$ 是模 $2p^l$ 的一组既约剩余系．我们有

$$r_1 r_2\cdots r_c\equiv -1(\bmod 2p^l)\,. \tag{7}$$

定理 4 设 $c=\phi(2^l)=2^{l-1}$, $l\ge 1$, $r_1,\cdots,r_c$ 是模 2^l 的既约剩余系．我们有

$$r_1\cdots r_c\equiv\begin{cases} -1(\bmod 2^l), & l=1, 2, \\ 1(\bmod 2^l), & l\ge 3. \end{cases} \tag{8}$$

证明 $l=1$, 2 时结论可直接验证．现设 $l\ge 3$. 对每个 r_i 必有唯一的 r_j 使

$$r_i\, r_j\equiv 1(\bmod 2^l)\,. \tag{9}$$

使 $r_i=r_j$ 的充要条件是 $r_i^{\,2}\equiv 1(\bmod 2^l)$. 即

$$(r_i-1)(r_i+1)\equiv 0(\bmod 2^l).$$

注意到 $(r_i, 2)=1$, 上式即

$$\frac{r_i-1}{2}\cdot\frac{r_i+1}{2}\equiv 0(\bmod 2^{l-2}).$$

注意到 $(\frac{r_i-1}{2},\frac{r_i+1}{2})=1$, 就推出 $r_i=r_j$ 的充要条件是

$$\frac{r_i-1}{2}\equiv 0(\bmod 2^{l-2})\text{ 或 }\frac{r_i+1}{2}\equiv 0(\bmod 2^{l-2}),$$

即

$$r_i \equiv 1 (\bmod 2^{l-1}) \text{ 或 } r_i \equiv -1 (\bmod 2^{l-1}) .$$

因此，在这个模 2^l 的既约剩余系中仅当

$$r_i \equiv 1，2^{l-1}+1，2^{l-1}-1，2^l-1 (\bmod 2^l) \tag{10}$$

时，有 $r_i = r_j$．这样，对模 2^l 的既约剩余系中的每个 r_i 除去这四数（这四个数两两对模 2^l 不同余）外必有 $r_j \ne r_i$．所以除了这四个数外，既约剩余系中的 $c-4$ 个数可按关系式（9）两两分对分完，即这 $c-4$ 个数的乘积对模 2^l 同余于 1．由此及式（10）就证明了式（8）对 $l \ge 3$ 成立．

总结以上讨论，我们证明了当 $m = 2, 4, p^l, 2p^l$（ p 为奇素数）时，模 m 的一组既约剩余系的乘积同余 -1 模 m．可以证明在其它情形必同余于 1 模 m．Wilson 定理是很有用的，下面举例给予说明．

例 1 设 p 是奇素数，证明：

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} (\bmod p) .$$

证明 注意到当 p 为奇素数时

$$(p-1)! = (1\cdot(p-1))(3\cdot(p-3))......((p-4)\cdot(p-(p-4))((p-2)\cdot(p-(p-2)))$$

$$\equiv (-1)^{(p-1)/2} 1^2 \cdot 3^2 .... (p-2)^2 ,$$

由此及定理 1 即得所要结论．

例 2 设 p 是奇素数，证明：

$$((p-1/2)!)^2 \equiv (-1)^{(p+1)/2} (\bmod p) .$$

证明 因为

$$((p-1/2)!)^2 \equiv 1^2 \times 2^2 \times \cdots \times [(p-1)/2]^2 (\bmod p)$$

$$\equiv [1\cdot(-p+1)]\cdot[2\cdot(-p+2)]\cdot\cdots\cdot\{[(p-1)/2]\}\cdot\{-p+[(p-1)/2]\} (\bmod p)$$

$$\equiv (-1)^{(p-1)/2} \cdot 1\cdot(p-1)\cdot 2\cdot(p-2)\cdot\cdots\cdot[(p-1)/2]\cdot[(p+1)/2]$$

$$\equiv (-1)^{(p-1)/2} \cdot (p-1)! .$$

根据 Wilson 定理知：

$$((p-1/2)!)^2 \equiv (-1)^{(p+1)/2} (\bmod p).$$

习题

1．求（1）$2^{143} \bmod 13$；（2）$3^{174} \bmod 17$；（3）$2^{133} \bmod 19$；

2．若同余式 $a \equiv b(\bmod m)$ 及 $c \equiv d(\bmod m)$ 同时成立，那么 m 应满足什么条件？

3．判断以下结论是否成立？若成立给出证明.

（1） 若 $a^2 \equiv b^2(\bmod m)$ 成立，则 $a \equiv b(\bmod m)$；

（2） 若 $a \equiv b(\bmod m)$ 成立，则 $a^2 \equiv b^2(\bmod m)$；

（3） 若 $a \equiv b(\bmod 2)$，则 $a^2 \equiv b^2(\bmod 2^2)$；

（4） 设 p 是奇素数，$p \nmid a$，那么，$a^2 \equiv b^2(\bmod p)$ 成立的充要条件是

$$a \equiv b(\bmod p) \text{ 或 } a \equiv -b(\bmod p),$$

有且仅有一式成立.

4．当 m 满足什么条件时，$1+2+\cdots+(m-1)+m \equiv 0(\bmod m)$.

5．（1）分别求模 $m=7,11,13$ 的所有元素的逆；

（2）求 5 对 9 的逆，7 对 10 的逆，11 对 8 的逆.

6．证明： $70! \equiv 61!(\bmod 71)$.

7．证明： 对任意整数 n，以下同余式中至少有一个成立.

$$n \equiv 0(\bmod 2), \quad n \equiv 0(\bmod 3), \quad n \equiv 1(\bmod 4),$$

$$n \equiv 3(\bmod 8), \quad n \equiv 7(\bmod 12), \quad n \equiv 23(\bmod 24).$$

8．证明： 当 $m>2$ 时，$0^2, 1^2, \cdots, (m-1)^2$ 一定不是模 m 的完全剩余系.

9．写出模 23 的一组完全剩余系 $r_1, r_2, \cdots, r_{23}$，且 $r_1, r_2, \cdots, r_{23}$ 满足以下两个条件：

$$r_j \equiv 0(\bmod 7), \quad r_j \equiv j(\bmod 5).$$

１０．设$m \ge 3$，$r_1, r_2, \cdots, r_s$是所有小于$m/2$且和m既约的正整数．证明：

$-r_s, \cdots, -r_1, r_1, r_2, \cdots, r_s$及$r_1, r_2, \cdots, r_s, (m-r_1), \cdots, (m-r_s)$都是模$m$的既约剩余系，并且当$m \ge 3$时，$2 \mid \phi(m)$．

１１．举例说明存在正整数，使得

（1）$\phi(n)=\phi(n+1)$；

（2）$\phi(n)=\phi(n+2)$；

（3）$\phi(n)=\phi(n+3)$．

１２．设n,h是正整数，证明：在不超过nh的正整数中，和n既约的数的个数等于$h\phi(n)$．

１３．构造$m=2\times 11$和$m=3\times 5\times 7$的完全剩余系和既约剩余系．

１４．设$m=m_1m_2\cdots m_k$，$m_1, m_2, \cdots, m_k$两两既约，$(m,a_i)=1$．证明：当$x^{(i)}$分别遍历m_i的完全（既约）剩余系时，

$$x=(M_1a_1x^{(1)}+M_2+\cdots+M_k)(M_1+M_2a_2x^{(2)}+\cdots+M_k)\cdots(M_1+M_2+\cdots+M_ka_kx^{(k)})$$

遍历$m=m_1m_2\cdots m_k$的既约剩余系．其中$M_im_i=m$，　$i=1, 2, \cdots, k.$

１５．对给定的正整数k，仅有有限多个n使得$\phi(n)=k$．

１６．证明：（1）$\phi(mn)=(m,n)\phi([m,n])$；

（2）$\phi(mn)\phi((m,n))=(m,n)\phi(m)\phi(n)$；

（３）当$(m,n)>1$时，则有$\phi(mn)>\phi(m)\phi(n)$．

１７．证明：（1）$\phi(n)>\sqrt{n}/2$，

（2）若n为合数，则$\phi(n)\le n-\sqrt{n}$．

１８．设$m=2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，$p_j$是不同的奇素数，$(m,a)=1$，$\lambda(m)=[\phi(2^{\alpha_0}), \cdots, \phi(p_r{}^{\alpha_r})]$．证明：$a^{\lambda(m)}\equiv 1 \pmod{m}$．

１９．设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$， p_j 是不同的奇素数． $\alpha=Max\{\alpha_1,\cdots,\alpha_r\}$， a 为任意整数．证明：（1） $a^{\alpha+\phi(m)}\equiv a^{\alpha}(\bmod m)$；

（2） $a^m\equiv a^{m-\phi(m)}(\bmod m)$．

２０．设素数 $p>2,a>1$．证明：

（1） a^p-1 的素因数 q 必是 $a-1$ 的因数，或是 $q-1\equiv 0(\bmod 2p)$；

（2） a^p+1 的素因数 q 必是 $a+1$ 的因数，或是 $q-1\equiv 0(\bmod 2p)$．

２１．设素数 $p>5$，证明：

（1） $(p-1)!+1$ 不可能是素数的方幂；

（2） $(p-2)!-1$ 不可能是素数的方幂．

２２．证明： $n,n+2$ 同时是素数的充要条件是

$$4((n-1)!+1)\equiv -n(\bmod n(n+2))．$$

２３．设素数 p 为奇数，证明：

（１） 当 $p=4m+3$ 时，对任意整数 a 均有 $a^2\not\equiv -1(\bmod p)$；

（２） 当 $p=4m+1$ 时，必有整数 a 满足 $a^2\equiv -1(\bmod p)$．

２４．设 $m\geq 3$， $r_1,r_2,\cdots,r_m$ 及 $r_1',r_2',\cdots,r_m'$ 是模 m 的两组完全剩余系．证明：$r_1r_1',r_2r_2',\cdots,r_mr_m'$ 一定不是模 m 的完全剩余系．

２５．设 $m\neq 1,2,4,p^{\alpha},2p^{\alpha}$， p 为奇素数．证明：$\prod\limits_{\substack{r\bmod m\\(r,m)=1}} r\equiv 1(\bmod m)$．