初等数论
第二章 同余

中山大学 数据科学与计算机学院

1. 同余

给定一个正整数m，设a, b是任意两个整数，如果m整除$a-b$:

$$m \mid (a-b)$$

即存在$k \in \mathbb{Z}$使得$a-b=km\,(a=km+b)$，则称a与b模m同余，记作$a \equiv b(\bmod m)$.

否则，称a与b模m不同余，记作$a \not\equiv b(\bmod m)$

例如，7|(27 − 6)，1是29被7除的余数，
所以：$27 \equiv 6(\bmod 7), 29 \equiv 1(\bmod 7)$

同余的基本性质

1. 任意整数与它自身模m同余: $a \equiv a \bmod m$; 此即自反性.
2. 如果a与b模m同余, 则b与a模m同余: 即

$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$$

   这是因为

$$a \equiv b \bmod m \Rightarrow \exists k \in \mathbb{Z}, s.t.\ a = km + b$$

$$\Rightarrow \exists(-k) \in \mathbb{Z}, s.t.\ b = (-k)m + a \Rightarrow b \equiv a \bmod m$$

   此即对称性.
3. 如果a与b模m同余, b与c模m同余, 则称a与c模m同余:

$$a \equiv b \bmod m, b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$$

   事实上,

$$a \equiv b \bmod m \Rightarrow \exists k_1 \in \mathbb{Z}, s.t.\ a = k_1 m + b$$

$$b \equiv c \bmod m \Rightarrow \exists k_2 \in \mathbb{Z}, s.t.\ b = k_2 m + c$$

   从而 $a = k_1 m + (k_2 m + c) = (k_1 + k_2)m + c$
   即a与c模m同余, 此即传递性.

示例: $m \in \mathbb{Z}^+, a \in \mathbb{Z}, C_a \triangleq \{c | a \equiv c \bmod m, c \in \mathbb{Z}\}$, 则

- C_a必非空;
  显然, 因为$a \in C_a$.
- 任意整数必包含在$C_0, C_1, \ldots, C_{m-1}$中的一个;
  $\forall c \in \mathbb{Z}, \exists q \in \mathbb{Z}, 0 \leq r < m, s.t.\ c = qm + r$, 从而$c \equiv r \bmod m$.
  根据上述集合的定义, $c \in C_r$.
- $C_a = C_b \iff a \equiv b \bmod m$;
  "$\Rightarrow$"比较简单: $b \in C_b = C_a \Rightarrow b \equiv a \bmod m$
  "$\Leftarrow$": 给定$a \equiv b \bmod m$, 要证明$C_a = C_b$, 需要说明$\forall c \in C_a \Rightarrow c \in C_b$和$\forall c \in C_b \Rightarrow c \in C_a$.

$$\forall c \in C_a \Rightarrow c \equiv a \bmod m \Rightarrow c \equiv b \bmod m \Rightarrow c \in C_b$$

  对$\forall c \in C_b \Rightarrow c \in C_a$ 类似可证.
- $C_a \cap C_b = \phi \iff a \not\equiv b \bmod m$
  "$\Rightarrow$": 如果$a \equiv b \bmod m$的话, 则有$C_a \cap C_b = C_a$而不是空集;
  "$\Leftarrow$": 如果$C_a \cap C_b \neq \phi$的话, 比如$c \in C_a \cap C_b$, 则有$c \equiv a \bmod m, c \equiv b \bmod m$, 从而应该有$a \equiv b \bmod m$, 这与已知条件矛盾.

- 设m除a的余数为r, m除b的余数为r', (这里r和r'是最小非负余数)则

$$a \equiv b \bmod m \iff r = r'$$

已知: $a = km + r, b = k'm + r'(0 \le r, r' < m)$
"$\Longleftarrow$":

$$r = r' \Rightarrow a - b = (k - k')m \Rightarrow a \equiv b \bmod m$$

"$\Longrightarrow$":

$$a - b = (k - k')m + (r - r')$$

而a与b模m同余, 即m整除$(a - b)$, 故$r - r' = 0$.

- 给定正整数m, 且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$, 则$(a_1 \pm a_2) \equiv (b_1 \pm b_2) \bmod m$
事实上,

$$a_1 \equiv b_1 \bmod m \Rightarrow a_1 = k_1 m + b_1$$

$$a_2 \equiv b_2 \bmod m \Rightarrow a_2 = k_2 m + b_2$$

$$\therefore (a_1 + a_2) = (k_1 + k_2)m + (b_1 + b_2)$$

$$\therefore (a_1 + a_2) \equiv (b_1 + b_2) \bmod m$$

同样地, $(a_1 - a_2) \equiv (b_1 - b_2) \bmod m$

- 给定正整数m，且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$，则$(a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod m$
  事实上，

$$a_1 \equiv b_1 \bmod m \Longrightarrow a_1 = k_1 m + b_1$$

$$a_2 \equiv b_2 \bmod m \Longrightarrow a_2 = k_2 m + b_2$$

$$\begin{aligned}\therefore (a_1 \cdot a_2) &= (k_1 m + b_1)(k_2 m + b_2) = k_1 k_2 m^2 + k_1 b_2 m + k_2 b_1 m + b_1 b_2 \\ &= (k_1 k_2 m + k_1 b_2 + k_2 b_1) m + b_1 b_2\end{aligned}$$

$$\therefore (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod m$$

- 特殊地,我们有 $\forall 0 \leq i \in \mathbb{Z}, a \equiv b \bmod m \Longrightarrow a^i \equiv b^i \bmod m$
- $x \equiv y \bmod m, a_0 \equiv b_0 \bmod m, a_1 \equiv b_1 \bmod m, \ldots, a_k \equiv b_k \bmod m$

$$\Longrightarrow (a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k) \equiv (b_0 + b_1 y + b_2 y^2 + \ldots + b_k y^k) \bmod m$$

- 对于大整数k和小整数m，在计算$b^k (\mathrm{mod} m)$时，可以先尝试寻找整数$0 < k' < k$使得$b^{k'} (\mathrm{mod} m) = \pm 1 (\mathrm{mod} m)$.

示例:
给定十进制数$n = (a_k a_{k-1} \dots a_2 a_1 a_0)_{10} (0 \le a_i \le 9)$, 则

$$3 | n \iff 3 | (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)$$

$$9 | n \iff 9 | (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)$$

事实上,

$$\left.\begin{array}{c} n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ 10 \equiv 1 \bmod 3 \end{array}\right\} \Longrightarrow$$

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_k \cdot 1^k + a_{k-1} \cdot 1^{k-1} + \dots a_2 \cdot 1^2 + a_1 \cdot 1 + a_0$$

$$\therefore n \equiv (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0) \bmod 3$$

根据同余的性质, 3除n余数与3除$(a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)$的余数相同, 所以3除$n$的余数为0当且仅当3除$(a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)$的余数为0, 即

$$3 \,|\, n \iff 3 \,|\, (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)$$

对9的情况证明完全类似.

示例:

给定1000进制数$n=(a_ka_{k-1}\dots a_2a_1a_0)_{1000}(0\le a_i\le 999)$，则

$$7|n \iff 7|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

$$11|n \iff 11|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

$$13|n \iff 13|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

事实上，$1000=7\times 11\times 13-1 \Longrightarrow 1000\equiv -1 \bmod 7$

$$\therefore 1000^{2k}\equiv 1 \bmod 7, 1000^{2k+1}\equiv -1 \bmod 7$$

$$a_0+a_1\cdot 1000+a_2\cdot 1000^2+a_3\cdot 1000^3+\dots a_k\cdot 1000^k$$

$\equiv a_0+a_1\cdot(-1)+a_2\cdot(-1)^2+a_3\cdot(-1)^3+a_4\cdot(-1)^4\dots a_k\cdot(-1)^k \bmod 7$

即

$$n\equiv(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots) \bmod 7$$

$$\therefore 7|n \iff 7|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

对于11和13的情况证明完全类似.

示例: $m,n,a\in\mathbb{Z}^+$, 如果$n^a\not\equiv 0 \bmod m, n^a\not\equiv 1 \bmod m$, 则存在$n$的一个素因子$p$使得$p^a\not\equiv 0 \bmod m, p^a\not\equiv 1 \bmod m$.

对于0的情况, 如果不存在素因子p使得$p^a\not\equiv 0 \bmod m$的式子成立, 即表明对n的任意素因子p都有$p^a\equiv 0 \bmod m$的式子成立. 例如, 对n的一个素因子p_1有$p_1^a\equiv 0 \bmod m$, 则

$$m\,|\,p_1^a \Longrightarrow m\,|\,n^a$$

这与条件$n^a\not\equiv 0 \bmod m$矛盾.

对于1的情况, 如果不存在素因子p使得$p^a\not\equiv 1 \bmod m$的式子成立, 即表明对n的任意素因子p都有$p^a\equiv 1 \bmod m$的式子成立, 考虑n的标准分解式,$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots p_s^{\alpha_s}$.

$$\begin{gathered}
p_1^a\equiv 1 \bmod m \Longrightarrow [p_1^a]^{\alpha_1}\equiv 1 \bmod m\\
p_2^a\equiv 1 \bmod m \Longrightarrow [p_2^a]^{\alpha_2}\equiv 1 \bmod m\\
\cdots\cdots\\
p_s^a\equiv 1 \bmod m \Longrightarrow [p_s^a]^{\alpha_s}\equiv 1 \bmod m\\
\therefore [p_1^a]^{\alpha_1}\cdot[p_2^a]^{\alpha_2}\cdot[p_3^a]^{\alpha_3}\ldots[p_s^a]^{\alpha_s}\equiv 1 \bmod m\\
\therefore [p_1^{\alpha_1}]^a\cdot[p_2^{\alpha_2}]^a\cdot[p_3^{\alpha_3}]^a\ldots[p_s^{\alpha_s}]^a\equiv 1 \bmod m\\
\therefore n^a\equiv 1 \bmod 1
\end{gathered}$$

与已知条件矛盾.

$$ad \equiv bd(\bmod m) \overset{?}{\Longrightarrow} a \equiv b \bmod m$$

反例: $5 \times 2 \equiv 3 \times 2 \bmod 4$, 但$5 \not\equiv 3 \bmod 4$.

$$ad \equiv bd(\bmod m) \overset{?}{\Longrightarrow} a \equiv b \bmod m$$

反例: $5 \times 2 \equiv 3 \times 2 \bmod 4$, 但$5 \not\equiv 3 \bmod 4$.

- $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d,m)=1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m$

  事实上,
  $$ad \equiv bd \bmod m \Longrightarrow m|(ad-bd) \Longrightarrow m|[d(a-b)]$$
  又因为$(d,m)=1$ (根据第一章$(a,c)=1, c|ab \Rightarrow c|b$), 故有$m|(a-b)$.

- $\left.\begin{array}{c} a \equiv b \bmod m \\ d|m \end{array}\right\} \Longrightarrow a \equiv b \bmod d$

  事实上, $a \equiv b \bmod m \Longrightarrow m|(a-b) \Longrightarrow d|(a-b) \Longrightarrow a \equiv b \bmod d$.

- $\left.\begin{array}{c} a \equiv b \bmod m \\ k>0 \end{array}\right\} \Longrightarrow (ak) \equiv (bk) \bmod (mk) \Longrightarrow (ak) \equiv (bk) \bmod m$

  事实上,
  $$a \equiv b \bmod m \Rightarrow m|(a-b) \Rightarrow (mk)|[k(a-b)]$$
  $$\Rightarrow (mk)|(ka-kb) \Rightarrow (ak) \equiv (bk) \bmod (mk)$$

- $\left.\begin{array}{c} a \equiv b \bmod m \\ d|a,b,m \end{array}\right\} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$

  事实上, $a \equiv b \bmod m \Longrightarrow (a-b) = km \Longrightarrow \dfrac{a-b}{d} = \dfrac{km}{d}$

  $\Longrightarrow \dfrac{a}{d} - \dfrac{b}{d} = k \cdot \dfrac{m}{d} \Longrightarrow \dfrac{a}{d} \equiv \dfrac{b}{d} \bmod \dfrac{m}{d}$

- $\left.\begin{array}{c} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \\ \cdots \\ a \equiv b \bmod m_k \end{array}\right\} \Longrightarrow a \equiv b \bmod [m_1, m_2, \ldots, m_k]$

  事实上,

$$a \equiv b \bmod m_i \Longrightarrow m_i|(a-b)(i = 1, 2, \ldots, k)$$

$$\therefore [m_1, m_2, \ldots, m_k]|[a-b]$$

$$\therefore a \equiv b \bmod [m_1, m_2, \ldots, m_k]$$

  特别的,$a \equiv b \bmod p, a \equiv b \bmod q, (p \neq q) \Longrightarrow a \equiv b \bmod pq$

- $a \equiv b \bmod m \Longrightarrow (a, m) = (b, m)$

  事实上, $a \equiv b \bmod m \Longrightarrow a = mk + b \Longrightarrow (a, m) = (b, m)$.

2. 剩余类

- 剩余类: 称
$$C_a \triangleq \{c | c \equiv a \bmod m, c \in \mathbb{Z}\}$$
为模m的a的剩余类. 这个集合中有无数多个元素. C_a中的任意元素称为这个类的剩余或代表元.
- 模m的剩余类有m个:$C_0, C_1, \ldots, C_{m-1}$.
- 完全剩余系: 如果m个整数$r_0, r_1, \ldots, r_{m-1} \in \mathbb{Z}$, 且它们中的任意两个都不在同一个剩余类中. 例如,
$$r_0 \in C_0, r_1 \in C_1, \ldots, r_{m-1} \in C_{m-1},$$
则称
$$\{r_0, r_1, \ldots, r_{m-1}\}$$
为模m的一个完全剩余系.

定理

设m为正整数，m个整数$r_0, r_1, \ldots, r_{m-1}$是模$m$的一个完全剩余系的充要条件是它们模$m$两两不同余，即对于$i, j = 0, 1, \ldots, m-1$, 且$i \neq j$, 有$r_i \not\equiv r_j \bmod m$.

(i) 整数a与正整数m互素, b是任意一个整数, 则: 当x取遍模m的一个完全剩余系中的数时, 相应的数$ax+b$也构成模m的一个完全剩余系.

证明: 假设x取遍一个完全剩余系$r_0, r_1, \ldots, r_{m-1}$, 只需要说明得到的$m$个整数$ar_0+b, ar_1+b, ar_2+b, \ldots, ar_{m-1}+b$两两不同余即可.

如果说这些数中存在两个同余, 比如$ar_0+b \equiv ar_1+b \bmod m$, 此即

$$m|(ar_0+b-ar_1-b) \Longrightarrow m|[a(r_0-r_1)]$$

而a与m互素, 所以

$$m|(r_0-r_1)$$

即

$$r_0 \equiv r_1 \bmod m$$

不可能. $\diamond$

(ii) 设m_1与m_2互素, 如果x_1取遍模m_1的完全剩余系中的数, x_2取遍模m_2的完全剩余系中的数时, 则$m_2x_1 + m_1x_2$取遍模m_1m_2完全剩余系中的数.

证明: x_1有m_1种取法, x_2有m_2种取法, 所以$m_2x_1 + m_1x_2$有m_1m_2中取法, 我们只需要说明这m_1m_2个值两两不同余即可.
如果存在$m_2a + m_1b$和$m_2a' + m_1b'$模m_1m_2同余, 即x_1分别取a, a'满足$a \neq a' \bmod m$, x_2分别取b, b'满足$b \neq b' \bmod m$, 则

$$m_2a + m_1b \equiv m_2a' + m_1b' \bmod m_1m_2$$

从而

$$m_2a + m_1b \equiv m_2a' + m_1b' \bmod m_1$$

所以

$$m_2a \equiv m_2a' \bmod m_1$$

而m_1与m_2互素, 从而

$$a \equiv a' \bmod m_1$$

矛盾. ◇

简化剩余类

如果一个模m的完全剩余类中有元素与m互素，则这个剩余类被称为简化剩余类.

事实上，这时候，这个类中所有元素均与m互素:
比如简化剩余类中与m互素的那个元素为$a, (a,m)=1$，对这个剩余类中的任一个元素$c, c \equiv a \bmod m$，即

$$c = mk + a \Longrightarrow (c,m) = (m,a)$$

$$\therefore (c,m) = 1 \iff (m,a) = 1$$

将小于m与m互素的正整数的个数记作$\varphi(m)$，称之为欧拉函数.
模m的简化剩余类的个数是$\varphi(m)$.

比如$\varphi(10) = 4$, $(1,3,7,9$与10互素$)$.

这样模10的简化剩余类就是C_1, C_3, C_7, C_9.

最小简化剩余系

在模m的所有简化剩余类中各取一个元素构成的集合叫做模m的简化剩余.

比如, $1, 2, 3, \ldots, m-1, m$中与m互素的整数全体构成模m的一个简化剩余系, 称之为模m的最小简化剩余系.

比如, $\{1, 3, 7, 9\}$是模10的一个简化剩余系和最小简化剩余系,
$\{1, 7, 11, 13, 17, 19, 23, 29\}$是模30的一个简化剩余系($\varphi(30) = 8$).

$\{1, 2, 3, \ldots, p-1\}$(p为素数)是模p的一个简化剩余系, 且有

$$\varphi(p) = p - 1$$

事实上,容易看到任意$\varphi(m)$个两两模m不同余, 并与m互素的整数一起都构成了一个模m的简化剩余系.

(i) $(a,m)=1$, 如果x取遍模m的一个简化剩余系中的元素, 则ax也取遍模m的一个简化剩余系中的元素.

证明: 对于x取的模m的一个简化剩余系中的任意元素, 总有

$$(x,m)=1$$

所以

$$(ax,m)=1$$

即相应的元素ax也与m互素.
还需要说明x取了这个剩余系中的不同的值m_1,m_2时, 相应的am_1,am_2不同余.
否则,

$$\left.\begin{array}{c} am_1 \equiv am_2 \bmod m \\ (a,m)=1 \end{array}\right\} \Longrightarrow m_1 \equiv m_2 \bmod m$$

矛盾. $\diamond$

(ii) $(a,m)=1, \exists a' \in \mathbb{Z}, 1 \le a' < m$ 使得 $aa' \equiv 1 \bmod m$

证明:

$$(a,m)=1 \Longrightarrow \exists s,t,\ \text{使得}\ sa+tm=1$$

$$\Longrightarrow sa+tm \equiv 1 \bmod m$$

$$\Longrightarrow sa \equiv 1 \bmod m$$

取

$$a' = s \bmod m)$$

即得所求. 从证明过程可以看到, a'在$1 \sim m$之间, 且a'是唯一的. $\diamond$
例如,

$$2 \cdot 4 \equiv 1 \bmod 7$$

$$3 \cdot 5 \equiv 1 \bmod 7$$

$$6 \cdot 6 \equiv 1 \bmod 7$$

这个结论在密码学中经常用到, 即乘法逆的概念.

定理（wilson定理）

p是素数，则$(p-1)! \equiv -1 \bmod p$

证明: 将p作为模数，a任意取$1,2,3,\ldots,p-1$都与p互素，所以存在唯一的整数数a'满足$1 \leq a' < p$使得$aa' \equiv 1 \bmod p$成立.
特别地，如果$a=a'$，则有$a^2 \equiv 1 \bmod p$，即$p \mid (a-1)(a+1)$，而a的可能的取值是$1,2,3,\ldots,p-1$，所以$a=1$或$a=p-1$.
这也表明，当a取值为1或$p-1$时，使得$aa' \equiv 1 \bmod p$成立的整数a'是1或$p-1$. 对于除此之外的a的可能取值，相应的使得$aa' \equiv 1 \bmod p$成立的整数a'不等于a.

于是，将$2,3,\ldots,p-2$中的满足$aa' \equiv 1 \bmod p$的a和a'两两配对，得到

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2) \equiv 1 \bmod p.$$

又因为

$$1 \cdot (p-1) \equiv -1 \bmod p$$

所以，

$$\begin{aligned}1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2) \cdot (p-1) &= 1 \cdot [2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2)] \cdot (p-1) \\ &\equiv 1 \cdot (p-1) \equiv -1 \bmod p \qquad \diamond\end{aligned}$$

这个结论也被称为Wilson定理.