初等数论
第二章 同余

中山大学　数据科学与计算机学院

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$r_i \not\equiv r_j \bmod m$.

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.

完全剩余系的写法

模m的剩余类有m个: $C_0, C_1, \ldots, C_{m-1}$. 作为新的元素组成一个新集合，通常写成

$$\mathbb{Z}/m\mathbb{Z} = \{C_0, C_1, C_2, \ldots, C_{m-1}\},$$

甚至

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

特别地，当$m = p$是素数时, 还可以写成

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p = \mathbb{F}_p = \{C_0, C_1, C_2, \ldots, C_{p-1}\} = \{0, 1, 2, \ldots, p-1\}.$$

特别重要的是，在$\mathbb{Z}/m\mathbb{Z}$中，元素间可以定义加法$\oplus$和乘法$\odot$，即

$$C_a \oplus C_b := C_{a+b} \quad C_a \odot C_b := C_{ab}.$$

这等价于0到$m-1$之间整数的模m运算，即

$$a(\mathrm{mod}\, m) + b(\mathrm{mod}\, m) = (a+b)(\mathrm{mod}\, m) \quad a(\mathrm{mod}\, m) \cdot b(\mathrm{mod}\, m) = (ab)(\mathrm{mod}\, m).$$

(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, 只需要说明这m_1m_2个值两两不同余即可. 或者说, 如果$m_2a + m_1b$和$m_2a' + m_1b'$模m_1m_2同余, 那么一定有$a \equiv a' \bmod m$和$b \equiv b' \bmod m$.

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

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

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

同理可以证明$b \equiv b' \bmod m$. ◇

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:
例如, 简化剩余类中与m互素的那个元素为a, 即$(a, m) = 1$, 对这个剩余类中的任一个元素c满足$c \equiv a \bmod m$, 都有

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

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

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 $aa' = a'a \equiv 1 \bmod m$

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.

定理

m_1与m_2互素, 如果x_1取遍模m_1的简化剩余系, x_2取遍模m_2的简化剩余系时, 则$m_2x_1+m_1x_2$遍历模m_1m_2的一个简化剩余系.

证明: 由

$$a=bq+c \Longrightarrow (a,b)=(b,c)$$

知

$$(m_2x_1+m_1x_2,m_1)=(m_2x_1,m_1)$$

又因为

$$(x_1,m_1)=1$$

我们有

$$(m_2x_1+m_1x_2,m_1)=(m_2x_1,m_1)=(m_2,m_1)=1$$

即$m_2x_1+m_1x_2$与m_1互素, 类似可得$m_2x_1+m_1x_2$与m_2互素, 从而$m_2x_1+m_1x_2$与m_1m_2互素.

为说明$m_2x_1+m_1x_2$遍历模m_1m_2的一个简化剩余系, 还需要说明任意一个模m_1m_2的简化剩余都具有形式:

$$m_2x_1+m_1x_2,\ \text{其中}\ (x_1,m_1)=1,(x_2,m_2)=1$$

事实上我们知道任意一个模m_1m_2的剩余都具有$m_2x_1+m_1x_2$形式. 一个剩余$m_2x_1+m_1x_2$要称为简化剩余必须满足$(m_2x_1+m_1x_2,m_1m_2)=1$.
由于$(m_1,m_2)=1$, 所以

$$(m_2x_1+m_1x_2,m_1)=(m_1x_2+m_2x_1,m_2)=1.$$

从而有

$$(x_1,m_1)=(m_2x_1,m_1)=(m_2x_1+m_1x_2,m_1)=1.$$

类似地推出

$$(x_2,m_2)=(m_1x_2,m_2)=(m_1x_2+m_2x_1,m_2)=1.$$

这就说明了任意一个模m_1m_2的简化剩余都具有:

$$m_2x_1+m_1x_2,\ \text{其中}\ (x_1,m_1)=1,(x_2,m_2)=1$$

这样的形式.

简化剩余系的写法

模m的简化剩余系可以写成

$$(\mathbb{Z}/m\mathbb{Z})^* = \{C_a \,|\, 0 \le a \le m, (a,m) = 1\},$$

甚至

$$\mathbb{Z}_m^* = \{a \,|\, 0 \le a \le m, (a,m) = 1\}.$$

简化剩余系的元素个数$\varphi(m)$, 因此

$$|\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m).$$

特别地，当$m = p$是素数时, 还可以写成

$$\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = \{C_1, C_2, C_3, \ldots, C_{p-1}\} = \mathbb{F}_p \setminus \{C_0\}.$$

在$\mathbb{F}_p^*$中，元素间还可以定义除法$\div$，即

$$C_a \div C_b := C_{ac}$$

其中，c是1到$p-1$之间的整数，使得$bc \equiv cb \equiv 1 \bmod p$.

3. 欧拉函数的性质

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

事实上, 在大于等于0, 小于p^α的数中:

$$\begin{array}{cccc}
0 & 1 & \dots & p-1 \\
p & p+1 & \dots & 2p-1 \\
2p & 2p+1 & \dots & 3p-1 \\
3p & 3p+1 & \dots & 4p-1 \\
\dots & \dots & \dots & \dots \\
(p^{\alpha-1}-1)p & (p^{\alpha-1}-1)p+1 & \dots & (p^{\alpha-1}-1)p+(p-1)
\end{array}$$

与p^α有公因子(大于1)的只是第一列, 其他列的数均与p^α互素.
例如, $3p+1$与p^α互素, 因为否则有公因子p的话,

$$p \,|\, 3p, p \,|\, (3p+1) \Longrightarrow p|1$$

矛盾. 再如$(p^{\alpha-1}-1)p+1$与p^α互素, 因为否则有公因子$p^i(i<\alpha)$的话, 则有公因子p,

$$p \,|\, (p^{\alpha-1}-1)p, p \,|\, ((p^{\alpha-1}-1)p+1) \Longrightarrow p \,|\, 1$$

矛盾. 其他情况类似.

这样与p^α互素的数的个数就是

$$p^\alpha - p^{\alpha-1}$$

即

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

◇

(2) $(m,n)=1 \Longrightarrow \varphi(mn)=\varphi(m)\varphi(n)$

这是因为, 我们已经知道: x遍历模m的简化剩余系, y遍历模n的简化剩余系时, 会有$xn+ym$遍历模mn的一个简化剩余系,

一方面, 模mn的一个简化剩余系所含元素个数是

$$\varphi(mn)$$

另一方面, x遍历模m的简化剩余系, y遍历模n的简化剩余系时, 得到$xn+ym$的个数是

$$\varphi(m)\varphi(n)$$

从而

$$\varphi(mn)=\varphi(m)\varphi(n)$$

$\diamond$

示例: 计算

$$\varphi(77)=\varphi(7)\varphi(11)=6\cdot 10=60$$

$$\varphi(30)=\varphi(2)\varphi(3)\varphi(5)=1\cdot 2\cdot 4=8$$

特殊地, p,q是素数时,

$$\varphi(pq)=\varphi(p)\varphi(q)=(p-1)(q-1)=pq-p-q+1$$

对任意正整数n, 其标准分解式为

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

有

$$\begin{aligned} \varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_s^{\alpha_s}) \\ p_1^{\alpha_1}(1 - \frac{1}{p_1}) \cdot p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdot \ldots \cdot p_s^{\alpha_s}(1 - \frac{1}{p_s}) \\ = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_s}) \end{aligned}$$

如果不知道n的分解式的话, 求其欧拉函数值是困难的.
相反地, 如果n是两个素数p和q的乘积, 已知欧拉函数$\varphi(n)$的值, 那么容易分解n, 即找到p和q.

(4) $n \in \mathbb{Z}^+, \sum_{d|n} \varphi(d) = n$

证明: 设d是n的因数(比如$n=8$时, d可取$1,2,4$或是8), 对于$\{1,2,3,4,\ldots,n\}$的n个数进行分类,

$$\Phi_d = \{m|1 \le m \le n, (m,n) = d\}$$

比如, $n=8$的话, 有$\Phi_1 = \{1,3,5,7\}$, $\Phi_2 = \{2,6\}$, $\Phi_4 = \{4\}$, $\Phi_8 = \{8\}$

可以看到, 按照这个分类, $\{1,2,3,4,\ldots,n\}$中的每个数属于且仅属于一个Φ的集合中. 这样, n就等于这些集合所含的元素个数之和.
我们知道

$$(m,n) = d \iff (\frac{m}{d}, \frac{n}{d}) = 1$$

所以集合Φ_d等价于下面的说法

$$\Phi_d = \{m \,|\, 1 \le m \le n, (\frac{m}{d}, \frac{n}{d}) = 1\}$$

即

$$\Phi_d = \{m = dk \,|\, 1 \le k \le \frac{n}{d}, (k, \frac{n}{d}) = 1\}$$

这样Φ_d的元素个数就是满足条件

$$1 \le k \le \frac{n}{d}, (k, \frac{n}{d}) = 1$$

的k的个数, 即$\varphi(\frac{n}{d})$. 从而$n = \sum_{d\,|\,n} \varphi(\frac{n}{d})$

事实上，当d遍历整数n的所有正因数时，$\frac{n}{d}$遍历整数n的所有正因数，所以有

$$\sum_{d\,|\,n} \varphi(\frac{n}{d}) = \sum_{d\,|\,n} \varphi(n/\frac{n}{d}) = \sum_{d\,|\,n} \varphi(d)$$

例如，$n = 8$时，

$$\sum_{d} \varphi(\frac{n}{d}) = \varphi(\frac{8}{1}) + \varphi(\frac{8}{2}) + \varphi(\frac{8}{4}) + \varphi(\frac{8}{8})$$

$$= \varphi(8) + \varphi(4) + \varphi(2) + \varphi(1) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8)$$

$$= \sum_{d} \varphi(d)$$

基于上述这一性质，可以对整数集合$\{1, 2, \ldots, m\}$按照与m的最大公因数进行划分.

(5) $1 < m \in \mathbb{Z}, (a,m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \bmod m$

证明: 设$r_1, r_2, r_3, \ldots, r_{\varphi(m)}$是$1, 2, 3, \ldots, m-1, m$中与$m$互素的整数全体, 它们构成模$m$的一个简化剩余系(最小简化剩余系),

因为$(a,m) = 1$
所以$ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$也构成模$m$的一个简化剩余系,
这样,

$$\{ar_1(\bmod m), ar_2(\bmod m), \ldots, ar_{\varphi(m)}(\bmod m)\} = \{r_1, r_2, r_3, \ldots, r_{\varphi(m)}\}$$

换句话说, 即

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv r_1 r_2 r_3 \ldots r_{\varphi(m)} \bmod m$$

整理得

$$(r_1 r_2 r_3 \ldots r_{\varphi(m)})(a^{\varphi(m)} - 1) \equiv 0 \bmod m$$

但

$$(r_1, m) = 1, (r_2, m) = 1, \ldots, (r_{\varphi(m)}, m) = 1 \Longrightarrow (r_1 r_2 r_3 \ldots r_{\varphi(m)}, m) = 1$$

从而

$$a^{\varphi(m)} - 1 \equiv 0 \bmod m \qquad \diamond$$

这个结论被称为著名的Euler定理

示例:

$$2^{10} \equiv 1 \bmod 11$$

这是因为:

$$(2, 11) = 1, \varphi(11) = 10$$

$$23 \nmid a \Longrightarrow a^{22} \equiv 1 \bmod 23$$

这是因为

$$23 \nmid a \Longrightarrow (a, 23) = 1$$

$$\varphi(23) = 22$$

(6) p是素数, $a \in \mathbb{Z}$, 则$a^p \equiv a \bmod p$

证明:

- 如果$p \mid a$的话, 有
$$p \mid a, p \mid a^p$$
从而
$$p \mid (a^p - a)$$
即
$$a^p \equiv a \bmod p$$
- 如果$p \nmid a$的话, 则
$$(a, p) = 1$$
从而
$$a^{\varphi(p)} \equiv 1 \bmod p$$
即
$$a^{p-1} \equiv 1 \bmod p$$
从而
$$a^p \equiv a \bmod p \qquad \diamond$$

这就是著名的Fermat小定理