第2章 同余

2.1同余的基本性质

【定义2.1.1】 给定一个正整数m和两个整数a, b, 如果$a-b$被m整除, 或$m|a-b$, 叫做a和b模m同余, 记作$a \equiv b(\mathrm{mod}\, m)$；否则叫做模$m$不同余, 记作$a \not\equiv b(\mathrm{mod}\, m)$.

【例2.1.1】 7|28=29−1, 故29≡1(mod 7).

7|21=27−6, 故27≡6(mod 7).

7|28=23− (−5), 故23≡−5(mod 7).

7∤20=25−5, 故25≢ 5(mod 7).

同余

简言之, 设模数m为大于1的整数, 可以把$a \pmod{m}$看成是欧几里德除法一般表示式中的余数.

如果$a = mq_1 + r_1, b = mq_2 + r_2$, 所谓$a$和$b$模$m$同余, 即是说限制$0 \leq r_1, r_2 \leq m$时，$r_1 = r_2$.

同余的性质

【定理2.1.1】 设m是一个正整数, a, b是两个整数, 则$a \equiv b \pmod{m}$当且仅当存在整数k, 使得$a = b + km$.

证明: 先证必要性. $a \equiv b \pmod{m}$ 也即 $m|a-b$, 故存在整数k, 使得$a-b=km$, 即$a=b+km$.

充分性. 若$a=b+km$, 则$a-b=km$, 故$m|a-b$, 也即$a \equiv b \pmod{m}$.

例如: 27≡6(mod 7), 因为27=6+3×7.

23≡2(mod 7), 因为23=2+3×7.

同余的性质

【定理2.1.2】 设m是一个正整数, 则模m同余是等价关系, 即满足下述性质:

（1）（自反性）对整数a有$a \equiv a \pmod m$.

（2）（对称性）对整数a和b, 若$a \equiv b \pmod m$, 则 $b \equiv a \pmod m$.

（3）（传递性）对整数a, b和c, 若$a \equiv b \pmod m$且$b \equiv c \pmod m$, 则$a \equiv c \pmod m$.

证明：性质（1）（2）容易证明，下面证明性质（3）.

（3）$a \equiv b \pmod m$, 则$m|a-b$; $b \equiv c \pmod m$, 则$m|b-c$. 故

$m|(a-b)+(b-c)=a-c$.

即$m|a-c$

同余的性质

【定理2.1.3】 设m为正整数, a, b, c, d为整数, 如果 $a \equiv b \pmod m$, $c \equiv d \pmod m$, 则

(i) $a + c \equiv b + d \pmod m$;

(ii) $ac \equiv bd \pmod m$.

证明: 已知$a \equiv b \pmod m$且$c \equiv d \pmod m$, 则存在整数h和k, 使等式$a = b + hm$且$c = d + km$成立.

故$a + c = (b + hm) + (d + km) = b + d + (h + k)m$.

$ac = (b + hm)(d + km) = bd + (hd + kb + hkm)m$.

由【定理2.1.1】即得结论.

特别地, 设m为正整数, a, b, k为整数. 如果 $a \equiv b \pmod{m}$, 则

(i) $a + k \equiv b + k \pmod{m}$;

(ii) $ak \equiv bk \pmod{m}$.

推论

由【定理2.1.3】可以得到如下结论.

【推论1】 若$a \equiv b \pmod m$, 则$\mathrm{n}a \equiv nb \pmod m$, 其中$n$为正整数.

【推论2】 若$a \equiv b \pmod m$, 则$a^n \equiv b^n \pmod m$, 其中n为正整数.

【推论3】 若$x \equiv y \pmod m$, $a_i \equiv b_i \pmod m$,$(i = 1,2, \dots, k)$, 则

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \equiv b_0 + b_1 y + b_2 y^2 + \cdots + b_k y^k \pmod m.$$

同余的性质

在进行同余运算时, 注意使用下面的规则:

（1）$a+b \pmod m \equiv (a \pmod m + b \pmod m) \pmod m$.

（2）$ab \pmod m \equiv (a \pmod m \times b \pmod m) \pmod m$.

（3）$na \pmod m \equiv n(a \pmod m) \pmod m$.

（4）设$n = n_1 + n_2$, 则

$$a^n \pmod m \equiv \left(a \pmod m\right)^n \pmod m$$
$$\equiv (\left(a \pmod m\right)^{n_1} \times \left(a \pmod m\right)^{n_2}) \pmod m \, .$$

同余的性质-例题

【例2.1.2】 2003年5月9日是星期五，问此后的第2^{2003}是星期几？

解: $2^{2003}+5 \equiv (2^3)^{667} \times 2^2+5 \pmod 7$

$\equiv 1^{667} \times 2^2+5 \pmod 7$

$\equiv 9 \pmod 7 \equiv 2 \pmod 7$.

同余的性质-例题

【例2.1.3】 设十进制整数n=$a_k a_{k-1} \ldots a_1 a_0$, 若3|n, 则 $3 | a_k + a_{k-1} + \cdots + a_1 + a_0$.

证明: $n = a_k a_{k-1} \ldots a_1 a_0$

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

$n \pmod 3$

$\equiv a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_1 \times 10 + a_0 \pmod 3$

$\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3$.

故得证.

同余的性质-例题

【例2.1.4】 计算$15^7 \pmod{55}$.

解: $15^7 \pmod{55}$

$\equiv (15^2)^3 \times 15$

$\equiv 5^3 \times 15$

$\equiv 15 \times 15 \equiv 5 \pmod{55}$.

同余的性质

【定理2.1.4】 设m为正整数, a,b为整数, $ad \equiv bd \pmod m$. 若$(d,m)=1$, 则$a \equiv b \pmod m$.

证明: 由 $ad \equiv bd \pmod m$可得

$m \mid ad - bd = (a-b)d.$

而$(d,m)=1$, 故$m \mid (a-b)$, 即 $a \equiv b \pmod m$.

同余的性质-例题

【例2.1.5】 $95\equiv 25 \pmod 7$, 即$19\times 5\equiv 5\times 5 \pmod 7$ 且$(5, 7)=1$, 故$19\equiv 5 \pmod 7$.

【例2.1.6】 (反例)$115\equiv 25 \pmod{15}$, 即
$23\times 5\equiv 5\times 5 \pmod{15}$,
但 $23 \not\equiv 5 \pmod{15}$, 因为$(5, 15)=5$.

同余的性质

【定理2.1.5】 设m为正整数, a, b为整数, 若 $a \equiv b \pmod{m}$且k>0, 则$ak \equiv bk \pmod{mk}$.

证明: $a \equiv b \pmod{m}$, 则存在整数t, 使$a - b = mt$.

等式两边乘以k得$ak - bk = mkt$.

故$mk \mid ak - bk$, 即$ak \equiv bk \pmod{mk}$.

【例2.1.7】 因19≡5(mod 7), k=4>0, 所以 76≡20(mod 28).

同余的性质

【定理2.1.6】 设m为正整数, a, b为整数, $a \equiv b \pmod{m}$且$d \mid (a, b, m)$, 则 $\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right)$.

证明: 因$d \mid (a, b, m)$, 故存在整数a', b', m', 使得
$\mathrm{a} = da', b = db', m = dm'$.

又$a \equiv b \pmod{m}$, 故存在整数k, 使得$a = b + mk$, 即
$da' = db' + dm'k$.

等式两边消去d得$a' = b' + m'k$.

等式两端模m'得$a' \equiv \mathrm{b}' \pmod{m'}$.

即$\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right)$

同余的性质-例题

【例2.1.8】 $190 \equiv 50 \pmod{70}$, 取$d = 10$, 则 $19 \equiv 5 \pmod{7}$.

同余的性质

【定理2.1.7】 设m为正整数, a, b为整数, $a \equiv b \pmod{m}$且$d \mid m$, 则$a \equiv b \pmod{d}$.

证明: 因$a \equiv b \pmod{m}$故$m \mid a - b$.

又$d \mid m$ 得$d \mid a - b$, 即$a \equiv b \pmod{d}$.

【例2.1.9】 190≡50(mod 70), 取d=7|70, 则190≡50(mod 7).

同余的性质

【定理2.1.8】 设a, b为整数, $a \equiv b(\mathrm{mod}\, m_i), (i = 1,2, \ldots, k)$的充分必要条件是

$a \equiv b(\mathrm{mod}[m_1, m_2, \ldots, m_k])$.

证明: $a \equiv b(\mathrm{mod}\, m_i)$当且仅当 $m_i \mid a-b$, 则

$[m_1, m_2, \ldots, m_k] \mid a - b$.

即$a \equiv b(\mathrm{mod}[m_1, m_2, \ldots, m_k])$.

【例2.1.10】 已知190≡50(mod 28), 190≡50(mod 35)以及[28, 35]=140, 则190≡50(mod 140).

同余的性质

【定理2.1.9】 设m为正整数, a,b为整数, $a \equiv b \pmod m$, 则$(a,m)=(b,m)$.

证明: 由$a \equiv b \pmod m$, 故存在整数k, 使得$a = mk + b$. 故$(a,m)=(b,m)$.

2.2完全剩余系

设m为正整数, 记$C_a = \{c | c \in Z,\ a \equiv c \pmod m\}$.
C_a非空, 因为至少$a \in C_a$.

例如, 设$m = 5, a = 1$, 则C_1={…, -4, 1, 6, … }, 也就是和1模5同余的整数的集合.

剩余类

【定理2.2.1】 设m是一个正整数, 则

(1) 任一整数必包含在某个C_r中, $0 \le r \le m-1$;

(2) $C_a = C_b$ 当且仅当 $a \equiv b \pmod m$;

(3) $C_a \cap C_b = \emptyset$当且仅当$a \not\equiv b \pmod m$.

证明：（1）设a是一个整数, 由带余除法, 有

$a = mq + r, 0 \le r < m$

因此$r \equiv a \pmod m$, 于是a属于C_r.

（2）必要性. 设$C_a = C_b$，则$a \in C_a = C_b$，故
$a \equiv b \pmod m$.

充分性. 因$a \equiv b \pmod m$, 对任意$c \in C_a$, $a \equiv c \pmod m$, 故$b \equiv c \pmod m$,故$c \in C_b$, 故$C_a \subseteq C_b$.

同理, $C_b \subseteq C_a$, 从而$C_a = C_b$.

(3) 必要性. 由（2）即得.

充分性. 用反证法证明. 若$a \not\equiv b \pmod m$时
$C_a \cap C_b \neq \emptyset$, 则可设$c \in C_a$, $c \in C_b$. 则$a \equiv c \pmod m$, $b \equiv c \pmod m$, 可得$a \equiv b \pmod m$. 矛盾.

剩余类

【例2.2.1】 设$m=5$, 则r的取值为0, 1, 2, 3, 4.

$C_0=\{\dots,-5,0,5,10,15,\dots\}$;

$C_1=\{\dots,-4,1,6,11,\dots\}$;

$C_2=\{\dots,-3,2,7,12,\dots\}$;

$C_3=\{\dots,-2,3,8,13,\dots\}$;

$C_4=\{\dots,-1,4,9,14,\dots\}$.

对于【定理2.2.1】的性质(1), 因为$C_0\cup C_1\cup C_2\cup C_3\cup C_4=Z$, 故任一整数必包含在某个$C_r$中.

对于性质(2)，例如$1\equiv 6 \pmod 5$, 故$C_1=C_6$. 反之亦然.

对于性质(3)，例如$1\not\equiv 2 \pmod 5$, 故$C_1\cap C_2=\emptyset$. 反之亦然.

剩余类

【定义2.2.1】 集合C_a叫做模m的a的**剩余类**. 模m的剩余类共有m个, 例如$C_0, C_1, C_2, \ldots, C_{m-1}$. 一个剩余类中的任一个数叫做该类的**剩余**.

若$r_0, r_1, \ldots, r_{m-1}$是$m$个整数, 且其中任何两个都不在同一个剩余类中, 则称$r_0, r_1, \ldots, r_{m-1}$为模$m$的一个完全剩余系.

完全剩余系

例如, 0, 1, 2, 3, 4是5个数, 且任何两个都不在模5的某一个剩余类中, 故称{0, 1, 2, 3, 4}为模5的一个完全剩余系. 由定义知, 集合{0, 6, 2, 8, 4}也是模5的一个完全剩余系, {5, 6, 2, 8, 9}也是模5的一个完全剩余系.

【注】每个剩余类中都包含了无穷多个整数, 而完全剩余系则恰好由m个数组成.

完全剩余系

【例2.2.2】 设$m = 10$, 则$C_a = \{a + 10k | k \in Z\}$是模$m = 10$的剩余类. 下面是模10的完全剩余系的举例:

（1）0, 1, 2, ..., 9

（2）1, 2, 3, ..., 10

（3）0, －1, －2, ..., －9

（4）0, 3, 6, 9, ..., 27

（5）10, 11, 22, 33, 44, ..., 99

【定理2.2.2】 设r_0，r_1，…，r_{m-1}为整数，这m个整数为模m的一个完全剩余系当且仅当它们模m两两不同余.

该定理给出了判断一个集合是否为模m的一个完全剩余系的方法. (1)该集合要有m个整数；(2)集合中任意两个整数模m两两不同余.

完全剩余系

【例2.2.3】 模m的完全剩余系中,

（i）最小非负完全剩余系是: $0, 1, \ldots, m-1$.

（ii）最小正完全剩余系是: $1, 2, \ldots, m$.

（iii）绝对值最小完全剩余系是:

m为偶数: $-\frac{m}{2}, -(m-2)/2, \ldots, (m-2)/2$ 或

$-(m-2)/2, \ldots, (m-2)/2, m/2$;

m为奇数: $-\frac{m-1}{2}, -(m-3)/2, \ldots, (m-1)/2$.

完全剩余系-性质

【定理2.2.3】 设a是满足$(a,m)=1$的整数, b为任意整数. 若$r_0,r_1,\dots,r_{m-1}$为模m的一个完全剩余系, 则$ar_0+b,ar_1+b,\dots,ar_{m-1}+b$也是模$m$的一个完全剩余系.

证明: 由【定理2.2.2】, 先证明: （1）$ar_0+b,ar_1+b,\dots,ar_{m-1}+b$是$m$个整数, 然后证明: （2）这$m$个整数模$m$两两不同余.

（1）易知$ar_0+b,ar_1+b,\dots,ar_{m-1}+b$是$m$个整数.

（2）用反证法证明. 若$ar_i+b\equiv ar_j+b \pmod m$, 其中$(0\le i<j\le m-1)$,则$ar_i\equiv ar_j \pmod m$. 又$(a,m)=1$, 故$r_i\equiv r_j \pmod m$. 由题设知, $r_0,r_1,\dots,r_{m-1}$为m的一个完全剩余系. 由【定理2.2.2】知, $r_i\not\equiv r_j \pmod m$. 矛盾.

故$ar_0+b,ar_1+b,\dots,ar_{m-1}+b$是模$m$的一个完全剩余系.

反证法的思路

反证法的思路可以描述为: 设条件为A, 结论为B. 欲证明A=>B, 改为通过已知A∧~B, 推导出与现有结论相矛盾的结果, 从而判断结论为B.

在【定理2.2.3】中, 反证法用来证明: 已知$r_0, r_1, \ldots, r_{m-1}$为模$m$的一个完全剩余系, $(a, m) = 1$, 推出$ar_i + b \not\equiv ar_j + b \pmod{m}$, 其中 $(0 \leq i < j \leq m-1)$. 改为通过已知$r_0, r_1, \ldots, r_{m-1}$为模$m$的一个完全剩余系, $(a, m) = 1$, $ar_i + b \equiv ar_j + b \pmod{m}$, 其中 $(0 \leq i < j \leq m-1)$. 利用已知结论推导出$r_i \equiv r_j \pmod{m}$. 这与已知$r_0, r_1, \ldots, r_{m-1}$为模$m$的一个完全剩余系矛盾. 故$ar_i + b \not\equiv ar_j + b \pmod{m}$.

完全剩余系-举例

【例2.2.4】 设$m = 6$, 模m的最小非负完全剩余系为0, 1, 2, 3, 4, 5.

	$ar_i + b(a = 5, b = 3)$	$ar_i + b(a = 3, b = 2)$
$r_i = 0$	5×0+3=3	3×0+2=2
$r_i = 1$	5×1+3=8≡ $2 \pmod 6$	3×1+2=5
$r_i = 2$	5×2+3=13≡ $1 \pmod 6$	3×2+2=8≡ $2 \pmod 6$
$r_i = 3$	5×3+3=18≡ $0 \pmod 6$	3×3+2=11≡ $5 \pmod 6$
$r_i = 4$	5×4+3=23≡ $5 \pmod 6$	3×4+2=14≡ $2 \pmod 6$
$r_i = 5$	5×5+3=28≡ $4 \pmod 6$	3×5+2=17≡ $5 \pmod 6$

由此可见, 当$a = 5, b = 3$时, 则集合{3,8, 13, 18, 23,28}为模6的一个完全剩余系. 当$a = 3, b = 2$时, 因为$a = 3$与6不互素, 不满足定理的条件, 故集合{2, 5, 8, 11, 14, 17}不为模6的一个完全剩余系.

完全剩余系-性质

【定理2.2.4】 设m_1, m_2是两个互素的正整数, 若x_1, x_2分别遍历m_1, m_2的完全剩余系, 则$m_2x_1 + m_1x_2$遍历模m_1m_2的完全剩余系.

证明:（1）当x_1, x_2分别遍历m_1, m_2个整数时, $m_2x_1 + m_1x_2$则遍历模m_1m_2个整数.

（2）证明m_1m_2个整数$m_2x_1+m_1x_2$模m_1m_2两两不同余.

若存在x_1,x_2和y_1,y_2满足

$m_2x_1+m_1x_2\equiv m_2y_1+m_1y_2\pmod{m_1m_2}$.

则由2.1节同余的【定理2.1.7】知

$m_2x_1+m_1x_2\equiv m_2y_1+m_1y_2\pmod{m_1}$.

即 $\quad m_2x_1\equiv m_2y_1\pmod{m_1}$.

而$(m_1,m_2)=1$, 故由由2.1节同余的【定理2.1.4】知

$x_1\equiv y_1\pmod{m_1}$.

同理可证, $x_2\equiv y_2\pmod{m_2}$.

结论成立.

完全剩余系-举例

【例2.2.5】 设$m_1 = 3, m_2 = 4, (m_1, m_2)$=1, 模3的一个完全剩余系为0,1,2, 模4的一个完全剩余系为0,1, 2, 3, 则

4×0+3×0=0,　4×0+3×1=3,　4×0+3×2=6,
4×0+3×3=9,

4×1+3×0=4,　4×1+3×1=7,　4×1+3×2=10,
4×1+3×3=13≡ 1(mod 12),

4×2+3×0=8,　4×2+3×1=11,　4×2+3×2=14≡ 2(mod 12),
4×2+3×3=17≡ 5(mod 12).

0, 3, 6 ,9, 4, 7, 10, 13, 8, 11, 14, 17为模12的一个完全剩余系.

完全剩余系-举例

【例2.2.6】 设p, q是两个不同的素数, $n = pq$, 则对任意整数c, 存在唯一的一对数x和y, 满足

$$qx + py = c(mod\, n),\quad 0 \le x < p, 0 \le y < q.$$

证明: p, q是两个素数, 故互素.

再由【定理2.2.4】, 当x, y分别遍历模p, q的完全剩余系时, $qx + py$遍历模$n = pq$的完全剩余系. 故存在唯一的一对整数x, y, 满足$qx + py = c(\mathrm{mod}\, n)$.

2.3简化剩余系

【定义2.3.1】 如果一个模m的剩余类中存在一个与m互素的剩余, 则该剩余类叫做简化剩余类（或者既约剩余类）.

【例2.3.1】 设$n = 10$, 则模10的剩余类$C_1, C_2, \dots, C_{10}$中, C_1中任一个整数都与10互素, 故C_1是模10的简化剩余类. 同理, C_3, C_7, C_9也是模10的简化剩余类.

简化剩余类-性质

【定理2.3.1】 设r_1, r_2是同一剩余类中的两个剩余，则r_1与m互素的充分必要条件是r_2与m互素.

证明: 由题设知 $r_1 = r_2 + km$. 故$(r_1, m) = (r_2, m)$.

$\therefore$ $(r_1, m) = 1$ $(r_2, m) = 1$.

简化剩余系

【定义2.3.2】 设m为正整数, 在模m的所有不同简化剩余类中, 从每个类任取一个数组成的整数集合, 叫做模m的一个简化剩余系（或称为缩系、既约剩余系）.

【例2.3.2】 设$n = 10$, 由【例2.3.1】, 模10的简化剩余类有C_1, C_3, C_7, C_9. 从这 4 个剩余类中各取一个数, 比如{1, 3, 7, 9}, 则该集合为模10的一个简化剩余系. 当然, 也可以是{11, 3, 27, 39}等等.

简化剩余系-性质

【定义2.3.3】 设m为正整数, 则1,2,…,m中与m互素的整数的个数, 记作$\varphi(m)$, 叫做欧拉（Euler）函数.

由【定义2.3.2】和【定义2.3.3】知, 模m的简化剩余系的元素的个数为$\varphi(m)$.

【例2.3.3】 设n=10, 由【例2.3.2】, {1, 3, 7, 9}为模10的一个简化剩余系. 完全剩余系1,2,…,10中与10互素的整数为1, 3, 7, 9, 故$\varphi(10)$=4.

简化剩余系-例题

【例2.3.4】 模6的一个简化剩余系为1, 5.

模20的一个简化剩余系为1, 3, 7, 9, 11, 13, 17, 19.

简化剩余系-例题

【例2.3.5】 模m的简化剩余系:

（i）最小非负简化剩余系: 0, 1, ..., $m-1$中与m互素的所有整数.

（ii）最小正简化剩余系: 1, 2, ..., m中与m互素的所有整数.

（iii）绝对值最小简化剩余系,

当m为偶数时:

$$-m/2, -(m-2)/2, \ldots, (m-2)/2 \text{ 或}$$
$$-(m-2)/2, \ldots, (m-2)/2, \qquad m/2$$

中与m互素的所有整数;

m为奇数时:

$$-(m-1)/2, -(m-3)/2, \ldots, (m-1)/2$$

中与m互素的所有整数.

模m的最小非负简化剩余系与最小正简化剩余系相同.

简化剩余系-例题

【例2.3.6】 模15的简化剩余系为($\varphi(15)=8$):

（i）最小非负简化剩余系: 1, 2, 4, 7, 8, 11, 13, 14.

（ii）最小正简化剩余系: 1, 2, 4, 7, 8, 11, 13, 14.

（iii）绝对值最小简化剩余系: －7, －4,－2, －1, 1, 2, 4, 7.

【例2.3.7】 素数p的最小非负简化剩余系为{1, 2, ……, $p－1$}, $\varphi(p)=p-1$.

最小正简化剩余系也是这个集合.

简化剩余系-性质

【定理2.3.2】 设m为正整数, 整数$r_1, r_2, \ldots, r_{\varphi(m)}$均与$m$互素, 且这$\varphi(m)$个数两两模$m$不同余, 则它们构成模$m$的一个简化剩余系.

该定理给出了判断一个集合是否为模m的一个简化剩余系的方法. (1) 该集合有$\varphi(m)$个整数; (2) 集合中每个数都与m互素; (3) 集合中任意两个整数模m两两不同余.

简化剩余系-性质

【定理2.3.3】 设m为正整数, a是满足$(a,m)=1$的整数. 那么, 若$r_1,r_2,\ldots,r_{\varphi(m)}$为模$m$的一个简化剩余系, 则$ar_1,ar_2,\ldots,ar_{\varphi(m)}$也模$m$的一个简化剩余系.

证明: (1) 易知$ar_1,ar_2,\ldots,ar_{\varphi(m)}$表示了$\varphi(m)$个数;

(2) 由$(a,m)=1$及$(r_i,m)=1$知$(ar_i,m)=1$, 即ar_i是简化剩余类的剩余.

(3) 用反证法证明集合中任意两个整数模m两两不同余.

假设$ar_i \equiv ar_j \pmod{m}, 1 \le i,j \le \varphi(m)$且$i \ne j$. 因$(a,m)=1$, 故$r_i \equiv r_j \pmod{m}$. 又因$r_i$和$r_j$是模$m$的简化剩余系中的元素, 故必有$r_i \not\equiv r_j \pmod{m}$, 矛盾. 故$ar_i \not\equiv ar_j \pmod{m}$.

故$ar_1,ar_2,\ldots,ar_{\varphi(m)}$也模$m$的一个简化剩余系.

简化剩余系-例题

【例2.3.8】 已知1, 7, 11, 13, 17, 19, 23, 29是模30的简化剩余系, (7, 30)=1, 则

7, 7×7≡19, 7×11≡17, 7×13≡1, 7×17≡29, 7×19≡13, 7×23≡11, 7×29≡23(mod 30)

也是模30的简化剩余系.

简化剩余系-例题

【例2.3.9】 设$m = 6$, 模m的最小非负简化剩余系为1, 5.

	$ar_i(a = 5)$	$ar_i(a = 3)$
$r_i = 1$	5×1=5	3×1=3
$r_i = 5$	5×5=25≡ $1(\mathrm{mod}\,6)$	3×5=15≡ $3(\mathrm{mod}\,6)$

简化剩余系-性质

【定理2.3.4】 设m为正整数, a是满足$(a,m)=1$的整数. 则存在整数$a'(1 \le a' < m)$使得

$$aa' \equiv 1 \pmod m.$$

证明: 由$(a,m)=1$知存在整数s,t, 使得$sa+tm=(a,m)=1$, 等式两端模m得$sa \equiv 1 (\mathrm{mod}\, m)$, 故求得$a' \equiv s \pmod m$.

简化剩余系-例题

【例2.3.10】 设$m = 880, a = 17$, 求a', 满足$aa' \equiv 1 \pmod m$.

解: 由辗转相除法, 得

880=17×51+13,　17=13+4,　13=4×3+1

1=13−4×3

=13−(17−13)×3=13×4−17×3

=(880−17×51)×4−17×3

=880×4−17×207

等式两端模880得$a' \equiv -207 \pmod{880} \equiv 673$.

简化剩余系-性质

【定理2.3.5】 m_1, m_2是两个互素的正整数, 若x_1, x_2分别遍历模m_1, m_2的简化剩余系, 则$m_2x_1 + m_1x_2$遍历模m_1m_2的简化剩余系.

证明: (1) 易知, 若x_1, x_2分别遍历模m_1, m_2的简化剩余系, 则$m_2x_1 + m_1x_2$遍历m_1m_2个数.

(2) 证明$m_2x_1+m_1x_2$属于模m_1m_2的某个简化剩余类, 即证

$(m_2x_1+m_1x_2, m_1m_2)=1.$

事实上, 由$(m_1,m_2)=1$及$(m_1,x_1)=1$和$(m_2,x_2)=1$知

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

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

所以 $(m_2x_1+m_1x_2, m_1m_2)=1.$

(3) 证明: 当$x_1 \not\equiv y_1 \pmod{m_1}$, 或者$x_2 \not\equiv y_2 \pmod{m_2}$时, 由【定理2.2.4】有

$m_2x_1+m_1x_2 \not\equiv m_2y_1+m_1y_2 \pmod{m_1m_2}.$

简化剩余系-例题

【例2.3.11】 设$m_1 = 3$, , $m_2 = 4$, (m_1, m_2)=1, 模3的一个简化剩余系为1,2, 模4的一个简化剩余系为1,3, 则

4×1+3×1=7,

4×2+3×1=11,

4×1+3×3=13≡ 1(mod 12),

4×2+3×3=17≡ 5(mod 12).

由计算结果可知, 7, 11, 13, 17是模12的一个简化剩余系.