第二章 同余
2015 年03月24 日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

访问主页
标题页
目录页
第 1 页 共 22 页
返回
全屏显示
关闭
退出

2.2 剩余类及完全剩余系

2.2.1 剩余类与剩余

因为同余是一种等价关系, 所以可借助于同余对全体整数进行分类, 并将每类作为一个数来看待, 进而得到整数的一些新性质.

设m是一个正整数. 对任意整数a, 令

$$C_a = \{c \mid c \in \mathbf{Z},\ c \equiv a \pmod{m}\}. \tag{1}$$

C_a 是非空集合, 因为$a \in C_a$.

定理2.2.1 设m是一个正整数. 则

i) 任一整数必包含在一个C_r 中, $0 \le r \le m-1$;

ii) $C_a = C_b$ 的充分必要条件是

$$a \equiv b \pmod{m}. \tag{2}$$

iii) C_a 与C_b 的交集为空集的充分必要条件是

$$a \not\equiv b \pmod{m}. \tag{3}$$

证 i) 设a 为任一整数. 由欧几里得除法, 存在惟一的整数q, r 使得

$$a = q \cdot m + r, \quad 0 \le r < m.$$

因此, 我们有$a \equiv r \pmod{m}$, a 包含在C_r 中.

ii) 因为$a \in C_a = C_b$, 所以必要性成立.

我们来证明充分性. 设整数a, b 满足关系式(2), 即

$$a \equiv b \pmod{m}.$$

要证明: $C_a = C_b$. 对任意的整数$c \in C_a$, 我们有 $c \equiv a \pmod{m}$.

由(2) 式及同余的传递性, 我们得到 $c \equiv b \pmod{m}$.

这说明, $c \in C_b$ 以及$C_a \subset C_b$.

同样, 对任意的整数$c \in C_b$, 我们有 $c \equiv b \pmod{m}$.

由(2) 式及同余的对称性, 我们得到 $b \equiv a \pmod{m}$.

再由同余的传递性, 得到 $c \equiv a \pmod{m}$.

这说明, $c \in C_a$ 以及$C_b \subset C_a$.

故$C_a = C_b$.

iii) 由ii) 立即得到必要性. 我们来证明充分性.

反证法. 假设C_a 与C_b 的交集非空, 即存在整数c 满足$c \in C_a$ 及$c \in C_b$, 则我们有

$$c \equiv a \pmod{m} \quad \text{及} \quad c \equiv b \pmod{m}.$$

对前一个同余式, 应用同余的对称性, 我们有

$$a \equiv c \pmod{m}.$$

再应用同余的传递性, 我们得到

$$a \equiv b \pmod{m}.$$

这与假设矛盾. 故C_a 与C_b 的交集为空集. 证毕

定义2.2.1 C_a 叫做**模m的a 的剩余类**. 一个剩余类中的任一数叫做该类的**剩余**或**代表元**. 若$r_0,\ r_1,\ \ldots,\ r_{m-1}$ 是m 个整数, 并且其中任何两个数都不在同一个剩余类里, 则$r_0,\ \ldots,\ r_{m-1}$ 叫做**模m 的一个完全剩余系**.

模m 的剩余类有m 个

$$C_0,\ C_1,\ \ldots,\ C_{m-1}. \tag{4}$$

它们作为新的元素的组成一个新集合, 通常写成

$$\mathbf{Z}/m\mathbf{Z} = \{C_0,\ C_1,\ \ldots,\ C_{m-1}\} = \{C_a \mid 0 \le a \le m-1\}. \tag{5}$$

特别地, 当$m = p$ 为素数时, 我们也写成

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \{C_0,\ C_1,\ \ldots,\ C_{p-1}\} = \{C_a \mid 0 \le a \le p-1\}. \tag{6}$$

注1 剩余类实际上就是一个等价分类中的等价类, 其对应于等价关系"模同余".

注2 $\mathbf{Z}/m\mathbf{Z}$ 中元素间的运算往往通过剩余类中的剩余或代表元来给出, 这时需要特别关注该运算不依赖于剩余或代表元的选取.

注3 $\mathbf{Z}/m\mathbf{Z}$ 中元素间的加法运算定义为:

$$C_a \oplus C_b := C_{a+b}. \tag{7}$$

此定义是合理的, 它不依赖于剩余或代表元的选取.

注4 $\mathbf{Z}/m\mathbf{Z}$ 中元素间的乘法运算定义为:

$$C_a \otimes C_b := C_{a\cdot b}. \tag{8}$$

此定义是合理的, 它不依赖于剩余或代表元的选取.

注5 记

$$(\mathbf{Z}/m\mathbf{Z})^* = \{C_a \mid C_a \in \mathbf{Z}/m\mathbf{Z}, (a,m)=1\}. \tag{9}$$

对于$C_a, C_b \in (\mathbf{Z}/m\mathbf{Z})^*$, 有$C_{a\cdot b} \in (\mathbf{Z}/m\mathbf{Z})^*$.

例2.2.1 对任意整数 a, $C_a = \{a + k \cdot 10 \mid k \in \mathbf{Z}\}$ 是模 $m = 10$ 的剩余类.

0, 1, 2, 3, 4, 5, 6, 7, 8, 9 为模 10 的一个完全剩余系.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10 为模 10 的一个完全剩余系.

0, −1, −2, −3, −4, −5, −6, −7, −8, −9 为模 10 的一个完全剩余系.

0, 3, 6, 9, 12, 15, 18, 21, 24, 27 为模 10 的一个完全剩余系.

10, 11, 22, 33, 44, 55, 66, 77, 88, 99 为模 10 的一个完全剩余系.

2.2.2 完全剩余系

定理2.2.2 m 个整数 $r_0, r_1, \ldots, r_{m-1}$ 为模 m 的一个完全剩余系的充分必要条件是它们模 m 两两不同余.

证 设 $r_0, r_1, \ldots, r_{m-1}$ 是模 m 的一个完全剩余系. 根据定理 1 ii), 它们模 m 两两不同余.

反过来, 设 $r_0, r_1, \ldots, r_{m-1}$ 模 m 两两不同余. 根据定理 1 iii), 这 m 个整数中的任何两个整数都不在同一个剩余类里. 因此, 它们成为模 m 的一个完全剩余系.

例2.2.2 设 m 是一个正整数. 则

i) $0,\ 1,\ \ldots,\ m-1$ 是模 m 的一个完全剩余系, 叫做模 m 的最小非负完全剩余系;

ii) $1,\ \ldots,\ m-1,\ m$ 是模 m 的一个完全剩余系, 叫做模 m 的最小正完全剩余系;

iii) $-(m-1),\ \ldots,\ -1,\ 0$ 是模 m 的一个完全剩余系, 叫做模 m 的最大非正完全剩余系;

iv) $-m,\ -(m-1),\ \ldots,\ -1$ 是模 m 的一个完全剩余系, 叫做模 m 的最大负完全剩余系;

v) 当 m 分别为偶数时, $-\frac{m}{2},\ -\frac{m-2}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-2}{2},$ 或 $-\frac{m-2}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-2}{2},\ \frac{m}{2},$ 是模 m 的一个完全剩余系;

当 m 分别为奇数时, $-\frac{m-1}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-1}{2}$ 是模 m 的一个完全剩余系, 上述两个完全剩余系统称为模 m 的一个绝对值最小完全剩余系.

定理2.2.3 设m 是正整数, a 是满足$(a, m) = 1$ 的整数, b是任意整数. 若k 遍历模m 的一个完全剩余系, 则

$$a \cdot k + b \tag{10}$$

也遍历模m 的一个完全剩余系.

证 根据定理2.2.2, 我们只需证明: 当

$$k_0,\ k_1,\ \ldots,\ k_{m-1}$$

是模m 的一个完全剩余系时, m 个整数

$$a \cdot k_0 + b,\ a \cdot k_1 + b,\ \ldots,\ a \cdot k_{m-1} + b$$

模m两两不同余. 事实上,若存在k_i 和k_j $(i \neq j)$ 使得

$$a \cdot k_i + b \equiv a \cdot k_j + b \pmod{m},$$

则$m \mid a \cdot (k_i - k_j)$. 因为$(a, m) = 1$, 根据定理1.3.11 之推论, 我们有$m \mid k_i - k_j$. 这说明$k_i$ 与k_j 模m 同余, 与假设矛盾. 因此, $a \cdot k + b$ 也遍历模m 的一个完全剩余系. 证毕

注 定理2.2.3是说，$C_{a\cdot k_0+b},\ldots,C_{a\cdot k_{m-1}+b}$ 是$\mathbf{Z}/m\mathbf{Z}$ 中全部元素$C_{k_0},\ldots,C_{k_{m-1}}$ 的一个置换.

例2.2.3设$m=10,\ a=7,\ b=5$. 则形为$a\cdot k+b$ 的10 个数

$$5,\ 12,\ 19,\ 26,\ 33,\ 40,\ 47,\ 54,\ 61,\ 68$$

构成模 10 的一个完全剩余系.

2.2.3 两个模的完全剩余系

定理2.2.4 设m_1, m_2 是两个互素的正整数. 若k_1, k_2 分别遍历模m_1, m_2 的完全剩余系, 则 $m_2 \cdot k_1 + m_1 \cdot k_2$ 遍历模$m_1 \cdot m_2$的完全剩余系.

证 因为k_1, k_2 分别遍历m_1, m_2 个数时, $m_2 \cdot k_1 + m_1 \cdot k_2$ 遍历$m_1 \cdot m_2$ 个整数, 所以只需证明这$m_1 \cdot m_2$ 个整数模$m_1 \cdot m_2$ 两两不同余. 事实上, 若整数k_1, k_2 和k_1', k_2' 满足

$$m_2 \cdot k_1 + m_1 \cdot k_2 \equiv m_2 \cdot k_1' + m_1 \cdot k_2' \pmod{m_1 \cdot m_2}, \qquad (11)$$

则我们有 $m_2 \cdot k_1 + m_1 \cdot k_2 \equiv m_2 \cdot k_1' + m_1 \cdot k_2' \pmod{m_1}$,

或者 $m_2 \cdot k_1 \equiv m_2 \cdot k_1' \pmod{m_1}$,

进而, $m_1 \mid m_2(k_1 - k_1')$. 因为$(m_1, m_2) = 1$, 所以$m_1 \mid k_1 - k_1'$. 故k_1与k_1'模m_1同余.

同理, k_2与k_2'模m_2同余.

因此, 定理是成立的. 证毕

例2.2.4 设$m_1 = 14$, $m_2 = 15$. 则当k_1, k_2 分别遍历模m_1, m_2 的完全剩余系, $k_3 = m_2 \cdot k_1 + m_1 \cdot k_2$ 遍历模$m_1 \cdot m_2$的完全剩余系.

$k_1 \setminus k_3 \setminus k_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	14	28	42	56	70	84	98	112	126	140	154	168	182	196
1	15	29	43	57	71	85	99	113	127	141	155	169	183	197	1
2	30	44	58	72	86	100	114	128	142	156	170	184	198	2	16
3	45	59	73	87	101	115	129	143	157	171	185	199	3	17	31
4	60	74	88	102	116	130	144	158	172	186	200	4	18	32	46
5	75	89	103	117	131	145	159	173	187	201	5	19	33	47	61
6	90	104	118	132	146	160	174	188	202	6	20	34	48	62	76
7	105	119	133	147	161	175	189	203	7	21	35	49	63	77	91
8	120	134	148	162	176	190	204	8	22	36	50	64	78	92	106
9	135	149	163	177	191	205	9	23	37	51	65	79	93	107	121
10	150	164	178	192	206	10	24	38	52	66	80	94	108	122	136
11	165	179	193	207	11	25	39	53	67	81	95	109	123	137	151
12	180	194	208	12	26	40	54	68	82	96	110	124	138	152	166
13	195	209	13	27	41	55	69	83	97	111	125	139	153	167	181

例2.2.5 设 $p,\ q$ 是不同的素数, $n = pq$. 则对任意整数 c, 存在惟一的一对整数 $x,\ y$ 满足 $qx + py \equiv c \pmod n$,
$0 \le x < p,\ 0 \le y < q$.

证 因为 $p,\ q$ 是两个不同的素数, 所以 $p,\ q$ 是互素的. 根据定理 4 及其证明, 知 $x,\ y$ 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. 因此, 存在惟一的一对整数 $x,\ y$ 满足

$$qx + py \equiv c \pmod n, \qquad 0 \le x < p,\ 0 \le y < q.$$

例2.2.6 设$m_1 = 2,\ m_2 = 5$. 则形为$5k_1 + 2k_2$ 的10 个数

$$0,\ 2,\ 4,\ 6,\ 8,\ 5,\ 7,\ 9,\ 11,\ 13$$

构成模10 的一个完全剩余系.

例 5 设$m_1 = 14,\ m_2 = 15$. 则当$k_1,\ k_2$ 分别遍历模$m_1,\ m_2$ 的完全剩余系, $k_3 = m_2 \cdot k_1 + m_1 \cdot k_2$ 遍历模$m_1 \cdot m_2$的完全剩余系.

$k_1 \setminus k_3 \setminus k_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	14	28	42	56	70	84	98	112	126	140	154	168	182	196
1	15	29	43	57	71	85	99	113	127	141	155	169	183	197	1
2	30	44	58	72	86	100	114	128	142	156	170	184	198	2	16
3	45	59	73	87	101	115	129	143	157	171	185	199	3	17	31
4	60	74	88	102	116	130	144	158	172	186	200	4	18	32	46
5	75	89	103	117	131	145	159	173	187	201	5	19	33	47	61
6	90	104	118	132	146	160	174	188	202	6	20	34	48	62	76
7	105	119	133	147	161	175	189	203	7	21	35	49	63	77	91
8	120	134	148	162	176	190	204	8	22	36	50	64	78	92	106
9	135	149	163	177	191	205	9	23	37	51	65	79	93	107	121
10	150	164	178	192	206	10	24	38	52	66	80	94	108	122	136
11	165	179	193	207	11	25	39	53	67	81	95	109	123	137	151
12	180	194	208	12	26	40	54	68	82	96	110	124	138	152	166
13	195	209	13	27	41	55	69	83	97	111	125	139	153	167	181

2.2.4 多个模的完全剩余系

定理2.2.5 设 $m_1,\ m_2,\ \ldots, m_k$ 是 k 个互素的正整数. 若 $x_1,\ x_2,\ \ldots,\ x_k$ 分别遍历模 $m_1,\ m_2,\ \ldots,\ m_k$ 的完全剩余系, 则

$$m_2\cdots m_k x_1 + m_1 m_3\cdots m_k x_2 + \cdots + m_1\cdots m_{k-1}x_k$$

遍历模 $m_1 m_2\cdots m_k$ 的完全剩余系.

证一 (直接证明) 因为 $x_1,\ x_2,\ \ldots,\ x_k$ 分别遍历 $m_1,\ m_2,\ \ldots, m_k$ 个数时,

$$m_2\cdots m_k x_1 + m_1 m_3\cdots m_k x_2 + \cdots + m_1\cdots m_{k-1}x_k$$

遍历 $m_1 m_2\cdots m_k$ 个整数, 所以只需证明这 $m_1 m_2\cdots m_k$ 个整数模 $m_1 m_2\cdots m_k$ 两两不同余.

事实上, 若整数 $x_1,\ x_2,\ \ldots,\ x_k$ 和 $y_1,\ y_2,\ \ldots,\ y_k$ 满足

$$\begin{aligned} & m_2\cdots m_kx_1+m_1m_3\cdots m_kx_2+\cdots+m_1\cdots m_{k-1}x_k \\ \equiv\ & m_2\cdots m_ky_1+m_1m_3\cdots m_ky_2+\cdots+m_1\cdots m_{k-1}y_k \\ & (\mathrm{mod}\ m_1m_2\cdots m_k), \end{aligned}$$

则对于 m_1, 根据定理2.1.11, 我们有

$$\begin{aligned} & m_2\cdots m_kx_1+m_1m_3\cdots m_kx_2+\cdots+m_1\cdots m_{k-1}x_k \\ \equiv\ & m_2\cdots m_ky_1+m_1m_3\cdots m_ky_2+\cdots+m_1\cdots m_{k-1}y_k\ (\mathrm{mod}\ m_1), \end{aligned}$$

或者 $m_2\cdots m_kx_1\equiv m_2\cdots m_ky_1\ (\mathrm{mod}\ m_1)$,
进而, $m_1\mid m_2\cdots m_k(x_1-y_1)$. 因为

$$(m_1,m_2)=1,\ldots,(m_1,m_k)=1,$$

所以 $(m_1,m_2\cdots m_k)=1$, 从而 $m_1\mid x_1-y_1$. 故 x_1 与 y_1 模 m_1 同余.
同理, x_2 与 y_2 模 m_2 同余,$\ldots$, x_k 与 y_k 模 m_k 同余.
因此, 定理是成立的. 证毕.

证二 (归纳证明) 对 k 运用数学归纳法. $k=2$ 时, 命题就是定理 4, 命题成立.

假设 $k \geq 3$, 命题对 $k-1$ 成立, 即 $x_1,\ x_2,\ \ldots,\ x_{k-1}$ 分别遍历 $m_1,\ m_2,\ \ldots, m_{k-1}$ 个数时,

$$y_1 = m_2 \cdots m_{k-1} x_1 + m_1 m_3 \cdots m_{k-1} x_2 + \cdots + m_1 \cdots m_{k-2} x_{k-1}$$

遍历 $m_1 m_2 \cdots m_{k-1}$ 的完全剩余系.

对于 k, 我们有

$m_2 \cdots m_k x_1 + \cdots + m_1 \cdots m_{k-2} m_k x_{k-1} + m_1 \cdots m_{k-1} x_k$

$= m_k y_1 + m_1 \cdots m_{k-1} x_k$

其中 $y_1 = m_2 \cdots m_{k-1} x_1 + \cdots + m_1 \cdots m_{k-2} x_{k-1}$. 根据归纳假设, $x_1,\ x_2,\ \ldots,\ x_{k-1}$ 分别遍历 $m_1,\ m_2,\ \ldots, m_{k-1}$ 个数时, y_1 遍历模 $m_1 \cdots m_{k-1}$ 的完全剩余系. 因此, 根据定理2.2.4, $m_k y_1 + m_1 \cdots m_{k-1} x_k$ 遍历模 $m_1 \cdots m_{k-1} m_k$ 的完全剩余系. 这就是说, 命题对 k 成立. 证毕.