现代密码学

第三十二讲 完全剩余系

信息与软件工程学院

同余类与剩余系

集合根据等价关系可分为两两互不相交的集合。

整数的同余关系是一个等价关系。

给定正整数m，全体整数可按照模m是否同余分为若干两两不相交的集合，使得每一个集合中的任意两个正整数对模m一定同余，而属于不同集合的任意两个整数对模m不同余，每一个这样的集合称为模m的同余类或剩余类。

同余类与剩余系

定理 1 对于给定的正整数m，有且恰有m个不同的模m的剩余类。

证明：根据带余除法，对于任意整数a，都有

$$a = qm + r, \quad 0 \leq r < m$$

也就是说任何一个整数模m必然与$\{0, 1, 2, \cdots, m-1\}$中的一个同余，而且这m个整数模m互不同余。所以模m的剩余类有且恰有m个。

同余类与剩余系

模m的m个剩余类可分别记为$[i]$，i为该剩余类中整数除m所得的余数，可分别如下表示：

$$[0]=\{\cdots,-2m,-m,0,m,2m,\cdots\}$$
$$[1]=\{\cdots,-2m+1,-m+1,1,m+1,2m+1,\cdots\}$$
$$[2]=\{\cdots,-2m+2,-m+2,2,m+2,2m+2,\cdots\}$$
$$\vdots$$
$$[m-1]=\{\cdots,-2m+(m-1),-m+(m-1),m-1,m+(m-1),2m+(m-1),\cdots\}$$

定义 在整数模m的所有剩余类中各取一个代表元 $a_1,a_2,\cdots,a_m,(a_i\in[i-1],\ i=1,2,\cdots,m)$，则称$a_1,a_2,\cdots,a_m$为模$m$的完全剩余系。完全剩余系$0,1,2,\cdots,m-1$称为最小非负完全剩余系。

同余类与剩余系

例 取$m=7$，则模m的剩余类为

$$
\begin{aligned}
[0] &= \{\cdots, -14, -7, 0, 7, 14, \cdots\} \\
[1] &= \{\cdots, 13, -6, 1, 8, 15, \cdots\} \\
[2] &= \{\cdots, -12, -5, 2, 9, 16, \cdots\} \\
[3] &= \{\cdots, -11, -4, 3, 10, \cdots\} \\
[4] &= \{\cdots, -10, -5, 4, 11, \cdots\} \\
[5] &= \{\cdots, -9, -2, 5, 12, \cdots\} \\
[6] &= \{\cdots, -8, -1, 6, 13, \cdots\}
\end{aligned}
$$

7，15，16，-4，-10，5，-1为模7的一组完全剩余系。

0，1，2，3，4，5，6为模7的最小非负完全剩余系。

同余类与剩余系

通常情况下，以$\mathbf{Z}_m$表示由m的最小非负完全剩余系集合$\mathbf{Z}_m=\{0,1,2,\cdots,m-1\}$。$\mathbf{Z}_m$中的加法、减法、乘法都是模$m$意义下的运算。

定理 2 设m是正整数，整数a满足$\gcd(a,m)=1$，b是任意整数。若x遍历模m的一个完全剩余系，则$ax+b$也遍历模m的一个完全剩余系。

证明： 设$a_1,a_2,\cdots,a_m$为模m的完全剩余系。根据完全剩余系的定义，这组整数模m两两不同余。

要证明$aa_1+b,aa_2+b,\cdots,aa_m+b$也是模$m$的一组完全剩余系。只需要证明这$m$个数模$m$两两不同余即可。若存在$a_i$和$a_j$，$i\neq j$，使得

$$aa_i+b\equiv aa_j+b(\bmod\ m)$$

同余类与剩余系

则有 $m|a(a_i-a_j)$，由于 $\gcd(a,m)=1$，所以 $m|(a_i-a_j)$，即有 $a_i\equiv a_j \pmod m$。这与 $a_1,a_2,\cdots,a_m$ 模 m 两两不同余矛盾。因此 $aa_1+b,aa_2+b,\cdots,aa_m+b$ 模 m 两两不同余。定理得证。

同余类与剩余系

例 当$m=12$时，则$\{0,1,2,3,4,5,6,7,8,9,10,11\}$ 构成模12 完全剩余系。

$\gcd(5,12)=1$

$a=5, b=0$

$\{0,5,10,3,8,1,6,11,4,9,2,7\}$

同余类与剩余系

定理 3 设 m_1，m_2 是两个互素的正整数。如果 x 遍历模 m_1 的一个完全剩余系，y 遍历模 m_2 的一个完全剩余系，则 m_1y+m_2x 遍历模 m_1m_2 的一个完全剩余系。

证明： 只需要证明所有的 m_1y+m_2x 模 m_1m_2 两两互不同余即可。事实上，若整数 x_1，x_2 属于模 m_1 的一个完全剩余系，y_1，y_2 属于模 m_2 的一个完全剩余系，满足：

$$m_1y_1+m_2x_1\equiv m_1y_2+m_2x_2 \pmod{m_1m_2}$$

根据定理2.1.3同余的性质（5），有

$$m_1y_1+m_2x_1\equiv m_1y_2+m_2x_2 \pmod{m_1}$$

即

$$m_2x_1\equiv m_2x_2 \pmod{m_1}$$

故 $m_1|m_2(x_1-x_2)$，又 m_1，m_2 互素，所以 $m_1|(x_1-x_2)$，即 x_1，x_2 模 m_1 同余。同理可证 y_1，y_2 模 m_2 同余。 矛盾！

同余类与剩余系

例　当 $m=3$ 时，$\{0,1,2\}$ 构成模3 完全剩余系，当 $n=2$ 时，$\{0,1\}$ 构成模2 完全剩余系。

$$0\times 2+0\times 3=0$$
$$0\times 2+1\times 3=3$$
$$1\times 2+0\times 3=2$$
$$1\times 2+1\times 3=5$$
$$2\times 2+0\times 3=4$$
$$2\times 2+1\times 3=7=1$$

$\{0,1,2,3,4,5\}$构成模6完全剩余系。

感 谢 聆 听!

xionghu.uestc@gmail.com