现代密码学

第三十三讲 简化剩余系

信息与软件工程学院

同余类与剩余系

在模m的一个剩余类当中，如果有一个数与m互素，则该剩余类中所有的数均与m互素，这时称该剩余类与m互素。

定义 1 与m互素的剩余类的个数称为欧拉函数，记为$\varphi(m)$

$\varphi(m)$ 等于 $\mathbf{Z}_m$ 当中与m互素的数的个数。对于任意一个素数 p， $\varphi(p)=p-1$

定义 2 在与m互素的 $\varphi(m)$个模 m 的剩余类中各取一个代表元 $a_1,a_2,\cdots,a_{\varphi(m)}$，它们组合成的集合称为模$m$ 的一个既约剩余系或简化剩余系。$\mathbf{Z}_m$中与m互素的数构成模 m 的一个既约剩余系，称为最小非负既约剩余系。

例 设$m=12$，则1，5，7，11构成模12 既约剩余系。

同余类与剩余系

定理 1 设m是正整数。整数a满足$\gcd(a,m)=1$ 。若x 遍历模m的一个既约剩余系，则 ax也遍历模 m的一个既约剩余系。

证明： 因为 $\gcd(a,m)=1$ $\gcd(x,m)=1$ 所以 $\gcd(ax,m)=1$。又若 $ax_i \equiv ax_j (\mathrm{mod}\ m)$，则由 $\gcd(a,m)=1$ 可得 $x_i \equiv x_j (\mathrm{mod}\ m)$。因此，若 x遍历模 m的一个既约剩余系，则 ax遍历$\varphi(m)$个数，这些数均属于某个模 m既约剩余类的剩余，而且两两互不同余。故而有 ax也遍历模 m的一个既约剩余系。

同余类与剩余系

例 设$m=12$，则$\{1,5,7,11\}$构成模12 简化剩余系。

$$\gcd(5,12)=1$$

$$\{5,1,11,7\}$$

同余类与剩余系

定理 2 设m_1，m_2是两个互素的正整数。如果x 遍历模m_1的一个既约剩余系，y遍历模 m_2的一个既约剩余系，则m_1y+m_2x 遍历模m_1m_2的一个既约剩余系。

证明思路：首先证明m_1y+m_2x与 m_1m_2互素，其次证明的任何一个既约剩余都可以表示成为 m_1y+m_2x的形式，其中 x与m_1互素，y与 m_2互素。：

证明：由定理2.2.3可知 m_1y+m_2x模 m_1m_2两两互不同余。首先证明当$\gcd(x,m_1)=1$，$\gcd(y,m_2)=1$ 时，m_1y+m_2x与 m_1m_2互素。用反证法。假设m_1y+m_2x与 m_1m_2不互素，则必有一个素数 p 满足 $p|m_1y+m_2x$，$p|m_1m_2$

同余类与剩余系

例　当 $m=3$ 时，$\{1,2\}$ 构成模3 简化剩余系。

$$5\times1+3\times1=8$$
$$5\times1+3\times2=11$$
$$5\times1+3\times3=14$$
$$5\times1+3\times4=2$$

例　当 $n=5$ 时，则 $\{1,2,3,4\}$构成模5简化剩余系。

$$5\times2+3\times1=13$$
$$5\times2+3\times2=1$$
$$5\times2+3\times3=4$$
$$5\times2+3\times4=7$$

$\{1,2,4,7,8,11,13,14\}$ 构成模15简化剩余系。

感 谢 聆 听!

xionghu.uestc@gmail.com