信息安全数学基础

简化剩余系

熊虎

信息与软件工程学院

xionghu.uestc@gmail.com

2.2 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2.2.3 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2.2.4 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2.2.2 设$m=12$，则1，5，7，11构成模12 既约剩余系。

2.2 同余类与剩余系

定理2.2.4 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$ax_i\equiv ax_j \pmod{m}$，则由$\gcd(a,m)=1$，可得$x_i\equiv x_j \pmod{m}$。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。

2.2 同余类与剩余系

定理2.2.5 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$p|m_1y+m_2x$，$p|m_1m_2$。

2.2 同余类与剩余系

由于$\gcd(m_1,m_2)=1$，所以$p|m_1$或$p|m_2$。不妨设$p|m_1$，则由m_1,m_2互素，可知$p\nmid m_2$。又$\gcd(x,m_1)=1$，所以p与x互素。由$p|m_1y+m_2x$可知$p|m_2x$，从而$p|x$，这与p，x互素矛盾。因此有m_1y+m_2x与m_1m_2互素。

接下来证明m_1m_2的任意一个既约剩余都可以表示为m_1y+m_2x，其中$\gcd(x,m_1)=1$，$\gcd(y,m_2)=1$。设整数a满足$\gcd(a,m_1m_2)=1$。根据定理2.2.3，可知存在x，y，使得

$$a\equiv m_1y+m_2x \pmod{m_1m_2}$$

因此，$\gcd(m_1y+m_2x,m_1m_2)=1$，根据最大公因数的性质，有

$$\gcd(x,m_1)=\gcd(m_2x,m_1)=\gcd(m_1y+m_2x,m_1m_2)=1$$

同理，$\gcd(y,m_2)=1$。定理得证。