信息安全数学基础

第二章 同余

熊虎

电子科技大学

第二章 同余

2.2 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。

2.2 同余类与剩余系

定理2.2.1 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

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

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。 $\square$

2.2 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2.2.2 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。

2.2 同余类与剩余系

例2.2.1 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。

2.2 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2.2.2 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 $aa_i+b\equiv aa_j+b\pmod{m}$

2.2 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$a_i\equiv a_j(\mathrm{mod}\ m)$。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。

2.2 同余类与剩余系

定理2.2.3 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！

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。

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

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$p|m_1y+m_2x$，$p|m_1m_2$。

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，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。

2.2 同余类与剩余系

推论2.2.1 设m，n是两个互素的整数，则$\varphi(mn)=\varphi(m)(n)$。

定理2.2.6 若 $m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ ，则

$$\varphi(m)=m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

证明： 当$m=p^e$为单个素数的方幂时，在模m的完全剩余系$\{0,1,2,\cdots,p^e-1\}$的p^e整数中与p不互素的只有p的倍数，共有 p^{e-1}，因此与p^e互素的数共有p^e-p^{e-1}，即

$$\varphi(p^e)=p^e-p^{e-1}=p^e(1-\frac{1}{p})$$

根据推论2.2.1，有

$$\varphi(m)=\varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_k^{e_k})=\prod_{i=1}^{k}p_i^{e_i}(1-\frac{1}{p_i})=m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

2.2 同余类与剩余系

例2.2.3 计算11，121，143和120的欧拉函数。

解： $\varphi(11)=11-1=10$

$121=11^2$ 因此 $\varphi(121)=11^2-11=110$

$143=11\times 13$ 因此

$\varphi(143)=\varphi(11)\cdot\varphi(13)=(11-1)\times(13-1)=120$

$120=2^3\times 3\times 5$ 因此

$$\varphi(120)=120\cdot(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=32$$

2.2 同余类与剩余系

定理2.2.7 设m是正整数,$r \in \mathbf{Z}_m$，若 $\gcd(r, m) = 1$，则存在整数$s \in \mathbf{Z}_m$，使得

$$rs \equiv 1 \pmod{m}$$

整数s也称为r模整数m下的乘法逆元。

证明： 因为$\gcd(r, m) = 1$，根据定理1.2.2存在整数s_1，t_1，使得

$$s_1 r + t_1 m = 1$$

因此有$s_1 r \equiv 1 \pmod{m}$。取s为s_1模去m后的最小正整数，即可得证。

2.2 同余类与剩余系

例2.2.4 求15 (mod 26)的乘法逆元。

解： 15与26互素，存在乘法逆元。做辗转相除法，可得

$$26 = 1 \times 15 + 11$$
$$15 = 1 \times 11 + 4$$
$$11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$

因此有

$$\begin{aligned}1 &= 4 - 3 = 4 - (11 - 2 \times 4) \\ &= 3 \times 4 - 11 = 3 \times (15 - 11) - 11 \\ &= 3 \times 15 - 4 \times 11 = 3 \times 15 - 4 \times (26 - 15) \\ &= 7 \times 15 - 4 \times 26\end{aligned}$$

所以 15 (mod 26) 的乘法逆元为7。

例2.2.5 求11 (mod 26) 的乘法逆元。

解： 11与26互素，存在乘法逆元。做辗转相除法

$$26 = 2 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

因此有

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \times 4) \\ &= 3 \times 4 - 11 \\ &= 3 \times (26 - 2 \times 11) - 11 \\ &= 3 \times 26 - 7 \times 11 \end{aligned}$$

又因为 $-7 \equiv 19 (\mathrm{mod}\ 26)$，所以 11 (mod 26)的乘法逆元为19。

2.2 同余类与剩余系

例2.2.6 设 $m=12$,$\varphi(12)=4$ ， 1， 5， 7， 11构成模12既约剩余系, $\gcd(5,12)=1$， 因此有$5\times1, 5\times5, 5\times7, 5\times11$也构成模12的简化剩余系， 经过计算可知

$$5\times1\equiv5(\bmod\ 12),\quad 5\times5\equiv1(\bmod\ 12),$$

$$5\times7\equiv11(\bmod\ 12),\quad 5\times11\equiv7(\bmod\ 12)$$

将上面四个式子左右对应相乘可得

$$(5\times1)(5\times5)(5\times7)(5\times11)\equiv5\times1\times11\times7(\bmod\ 12)$$

即

$$5^4\times(1\times5\times7\times11)\equiv1\times5\times7\times11(\bmod\ 12)$$

由于$\gcd(1\times5\times7\times11,12)=1$， 根据同余性质（3）可得 $5^4\equiv1(\bmod\ 12)$， 即

$$5^{\varphi(12)}\equiv1(\bmod\ 12)$$

并非巧合！

2.2 同余类与剩余系

定理2.2.8（欧拉定理） 设m是正整数，$r \in Z_m$，若$\gcd(r,m)=1$，则 $r^{\varphi(m)} \equiv 1 (\bmod\ m)$。

证明： 取模m的一组既约剩余系$r_1, r_2, \cdots, r_{\varphi(m)}$，由定理2.2.4知$rr_1, rr_2, \cdots, rr_{\varphi(m)}$也是模$m$的一组既约剩余系，从而有

$$\forall 1 \le i \le \varphi(m),\ \gcd(r,m)=1$$

因为

$$\prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{i=1}^{\varphi(m)} (rr_i) \equiv r^{\varphi(m)} \prod_{i=1}^{\varphi(m)} r_i (\bmod\ m)$$

也即

$$\Big(\prod_{i=1}^{\varphi(m)} r$$

欧拉定理在密码技术中具有重要应用，如RSA

故有

$$r^{\varphi(m)} \equiv 1 (\bmod\ m)$$

2.2 同余类与剩余系

推论2.2.2 （费马小定理）设p是一个素数，则对于任意整数a，均有

$$a^p \equiv a(\mathrm{mod}\ p)$$

定理2.2.9 （Wilson定理）设p是素数，$r_1, \cdots, r_{p-1}$是模p的既约剩余系，则有

$$r_1 r_2 \cdots r_{p-1} \equiv -1(\mathrm{mod}\ p)$$

证明：当$p=2$时，结论显然成立。当$p \geq 3$时，根据定理2.2.7，对取定的既约剩余系$r_1, \cdots, r_{p-1}$中的每一个r_i，必有唯一的r_j是其在模运算下的乘法逆元，即

$$r_i r_j \equiv 1(\mathrm{mod}\ p)$$

使$r_i = r_j$的充要条件是

$$r_i^2 \equiv 1(\mathrm{mod}\ p)$$

即
$$(r_i - 1)(r_i + 1) \equiv 0(\mathrm{mod}\ p)$$

2.2 同余类与剩余系

由于p是素数且$p\geq 3$，所以上式成立的充要条件是

$$r_i-1\equiv 0(\bmod\ p)\text{或}\ r_i+1\equiv 0(\bmod\ p)$$

由于$p\geq 3$，所以这两式不能同时成立。因此，在$\{r_1,\cdots,r_{p-1}\}$中，除了$r_i\equiv 1,-1(\bmod\ p)$这两个整数外，对其他的r_i必有$r_i\neq r_j$使得$r_ir_j\equiv 1(\bmod\ p)$成立。不妨设$r_1\equiv 1(\bmod\ p)$，$r_{p-1}\equiv -1(\bmod\ p)$。这样，在$\{r_1,\cdots,r_{p-1}\}$中除了$r_1,r_{p-1}$外，其他的数恰好可按关系式$r_ir_j\equiv 1(\bmod\ p)$两两分完，即有

$$r_2\cdots r_{p-2}\equiv 1(\bmod\ p)$$

由此可得$r_1r_2\cdots r_{p-1}\equiv -1(\bmod\ p)$。

$1,2,\cdots,p-1$是模p的既约剩余系，所以有

$$(p-1)!\equiv -1(\bmod\ p)$$

谢谢！