信息安全数学基础

完全剩余系

熊虎

信息与软件工程学院

xionghu.uestc@gmail.com

2.2 同余类与剩余系

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

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

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。

例2.2.4 求 $15 \pmod{26}$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 $15 \pmod{26}$ 的乘法逆元为7。

2.2 同余类与剩余系

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

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$5\times 1, 5\times 5, 5\times 7, 5\times 11$也构成模12的简化剩余系，经过计算可知

$$5\times 1\equiv 5 \pmod{12},\quad 5\times 5\equiv 1 \pmod{12},$$

$$5\times 7\equiv 11 \pmod{12},\quad 5\times 11\equiv 7 \pmod{12}$$

将上面四个式子左右对应相乘可得

$$(5\times 1)(5\times 5)(5\times 7)(5\times 11)\equiv 5\times 1\times 11\times 7 \pmod{12}$$

即

$$5^4\times(1\times 5\times 7\times 11)\equiv 1\times 5\times 7\times 11 \pmod{12}$$

由于$\gcd(1\times 5\times 7\times 11, 12)=1$，根据同余性质（3）可得 $5^4\equiv 1 \pmod{12}$，即

$$5^{\varphi(12)}\equiv 1 \pmod{12}$$

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 $r^{\varphi(m)} \equiv 1 \pmod{m}$。

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

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

也即

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

欧拉定理在密码技术中具有重要应用，如RSA

故有

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