# 现代密码学

## 第三十四讲 欧拉定理

信息与软件工程学院

# 欧拉定理

**推论 1** 设$m$，$n$是两个互素的整数，则$\varphi(mn)=\varphi(m)\varphi(n)$

**定理 1** 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 1，有

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

# 欧拉定理

**例**　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

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

# 欧拉定理

例　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！

# 欧拉定理

**定理 2 （欧拉定理）**设$m$是正整数，$r \in Z_m$，若$\gcd(r,m)=1$，则 $r^{\varphi(m)} \equiv 1(\mathrm{mod}\ m)$。

**证明：**取模$m$的一组既约剩余系$r_1, r_2, \cdots, r_{\varphi(m)}$，由简化剩余系结论知 $rr_1, rr_2, \cdots, rr_{\varphi(m)}$ 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

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

也即

$$(\prod_{i=1}^{\varphi(m)} r_i,$$

欧拉定理在密码技术中具有重要应用，如RSA

故有

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

感 谢 聆 听!

xionghu.uestc@gmail.com