欧拉定理

$$(x,m)=1\to x^{\varphi(m)}\equiv 1\pmod m$$

证明

记模 m 的既约剩余系为 $A=\{a_1,a_2,\cdots,a_{\varphi(m)}\}$，设集合 $B=xA=\{xa_1,xa_2,\cdots,xa_{\varphi(m)}\}$。则有 $B=A$：

- 对任意元素 $xa_k\in B$，因为 $(x,m)=1$，$(a_k,m)=1$，所以 $(xa_k,m)=1$。
- 任取 $1\le p\ne q\le\varphi(m)$，$xa_p\not\equiv xa_q\pmod m$。反证，因为 $(x,m)=1$，消去 x 得 $a_p\equiv a_q\pmod m$，与已知矛盾。

所以

$$a_1a_2\cdots a_{\varphi(m)}\equiv xa_1xa_2\cdots xa_{\varphi(m)}\pmod m$$

因为 $(a,m)=1$，消去得

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

扩展欧拉定理

$$x^{\varphi(m)}\equiv x^{2\varphi(m)}\pmod m$$

引理　若 p 是 n 的质因子，p 的次数为 k，则 $\varphi(n)\ge k$。

设 $n=p^k\cdot s$。$\varphi(n)=\varphi(p^k)\cdot\varphi(s)\ge\varphi(p^k)\ge p^k-p^{k-1}=2^{k-1}$。因为 $k\ge 1$，所以 $\varphi(n)\ge 2^{k-1}\ge k$。当且仅当 $n=2$ 或 $n=2^2$ 时取到等号。

证明

设 $m=s\cdot t$，s 的质因子集合含于 x 的质因子集合，$(s,t)=1$。显然 $(x,t)=1$。

对任意 s 的质因子 p，次数为 k，由引理，$\varphi(s)\ge k$。又因为 x 中 p 的次数至少为 1，所以 $x^{\varphi(s)}$ 中 p 的次数大于 k。所以 $s\mid x^{\varphi(s)}$，$s\mid x^{\varphi(m)}$。所以 $x^{\varphi(m)}\equiv x^{2\varphi(m)}\equiv 0\pmod s$。

对 t。因为 $(x,t)=1$，所以 $x^{\varphi(m)}\equiv x^{\varphi(t)}\equiv 1\pmod t$，$x^{\varphi(m)}\equiv x^{2\varphi(m)}\equiv 1\pmod t$。

由 $(s,t)=1$，中国剩余定理合并得

$$x^{\varphi(m)}\equiv x^{2\varphi(m)}\equiv \mathrm{inv}_t(s)s\pmod m$$

推论：降幂公式

$$x^a\equiv\begin{cases} x^{a \bmod \varphi(m)} & (x,m)=1\\ x^a & (x,m)\ne 1\land a\le\varphi(m)\\ x^{a \bmod \varphi(m)+\varphi(m)} & (x,m)\ne 1\land a\ge\varphi(m)\end{cases}$$