定义 1.3.1 设 $a_1, \cdots, a_n$ 是 n $(n \geqslant 2)$ 个整数. 若整数 d 是它们中每一个数的因数, 则 d 就叫做 $a_1, \cdots, a_n$ 的一个**公因数**.

d 是 $a_1, \cdots, a_n$ 的一个公因数的数学表达式为

$$d \mid a_1, \ \ldots, \ d \mid a_n.$$

如果整数 $a_1, \ldots, a_n$ 不全为零, 那么整数 $a_1, \ldots, a_n$ 的所有公因数中最大的一个公因数就叫做**最大公因数**, 记作 $(a_1, \ldots, a_n)$.

特别地, 当 $(a_1, \ldots, a_n) = 1$ 时, 称 $a_1, \ldots, a_n$ **互素或互质**.

注 1 $d > 0$ 是 $a_1, \cdots, a_n$ 的最大公因数的数学表达式可叙述为

(i) $d \mid a_1, \cdots, d \mid a_n$.

(ii) 若 $e \mid a_1, \cdots, e \mid a_n$, 则 $e \mid d$.

详见定理 1.3.9 中的说明.

注 2 a, b 的最大公因数 $d = (a, b)$ 是集合

$$\{s \cdot a + t \cdot b \mid s, t \in \mathbf{Z}\}$$

中的最小正整数. 事实上, 由注 1 (i) 及定理 1.1.3 可说明上述集合中的所有元素都是 d 的

例 1.3.6 设 p 是一个素数, a 为整数. 如果 $p \nmid a$, 则 a 与 p 互素.

证 设 $(a, p) = d$. 则有 $d \mid p$ 及 $d \mid a$. 因为 p 是素数, 所以由 $d \mid p$, 有 $d = 1$ 或 $d = p$.

对于 $d = p$, 由 $d \mid a$, 有 $p \mid a$, 这与假设 $p \nmid a$ 矛盾, 因此, $d = 1$, 即 $(a, p) = 1$. 结论成立. 证毕.

定理 1.3.3 设 a, b, c 是三个不全为零的整数. 如果

$$a = q \cdot b + c \tag{1.10}$$

其中 q 是整数, 则 $(a, b) = (b, c)$.

证 设 $d = (a, b)$, $d' = (b, c)$, 则 $d \mid a$, $d \mid b$. 由定理 1.1.3, 得

$$d \mid a + (-q) \cdot b = c,$$

因而, d 是 b, c 的公因数. 从而, $d \leqslant d'$.

同理, 由 $d' \mid b$, $d' \mid c$, 得到

$$d' \mid q \cdot b + c = a,$$

以及 d' 是 a, b 的公因数, $d' \leqslant d$.

因此, $d = d'$. 于是, 定理 1.3.3 成立. 证毕.

定理 1.3.4 设 a, b 是任意两个正整数, 则 $(a, b) = r_n$, 其中 r_n 是广义欧几里得除法式 (1.11) 中最后一个非零余数, 并且, 当 $a > b$ 时, 计算 (a, b) 的时间为 $O(\log a \log^2 b)$.

证 根据广义欧几里得除法式 (1.11)、定理 1.3.3 以及定理 1.3.2, 有

$$\begin{aligned}
r_{-2} &= q_0 \cdot r_{-1} + r_0, && (a, b) = (r_{-2}, r_{-1}) = (r_{-1}, r_0), \\
r_{-1} &= q_1 \cdot r_0 + r_1, && (r_{-1}, r_0) = (r_0, r_1), \\
r_0 &= q_2 \cdot r_1 + r_2, && (r_0, r_1) = (r_1, r_2), \\
&\vdots \\
r_{n-3} &= q_{n-1} \cdot r_{n-2} + r_{n-1}, && (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}), \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, && (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n), \\
r_{n-1} &= q_{n+1} \cdot r_n + r_{n+1}, && (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n.
\end{aligned}$$

因此, 由性质 1.3.1 , 计算 (a, b) 的时间为

$$O(\log r_{-2} \log r_{-1} + \cdots + \log r_{n-1} \log r_n) = O(n \log a \log b) = O(\log a \log^2 b)$$

定理 1.3.4 成立. 证毕.

例 1.3.12 设 $a=-1859$, $b=1573$, 计算 (a,b).

解 由定理 1.3.1, $(-1859,1573)=(1859,1573)$.

运用广义欧几里得除法, 有

$$\begin{aligned} 1859 &= 1\cdot 1573 + 286,\\ 1573 &= 5\cdot 286 + 143,\\ 286 &= 2\cdot 143 + 0. \end{aligned}$$

根据定理 1.3.4, 得 $(-1859,1573)=143$.

定理 1.3.8 整数 a, b 互素的充分必要条件是存在整数 s, t 使得

$$sa+tb=1.$$

证 根据定理 1.3.7 可立即得到命题的必要性.

反过来, 设 $d=(a,b)$, 则有 $d\mid a$, $d\mid b$. 根据假设, 存在整数 s, t 使得

$$sa+tb=1.$$

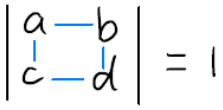
则有

$$d\mid sa+tb=1.$$

因此, $d=1$, 即整数 a, b 互素. 证毕.

例 1.3.21 设 4 个整数 a, b, c, d 满足关系式

$$ad-bc=1.$$



则 $(a,b)=1$, $(a,c)=1$, $(d,b)=1$, $(d,c)=1$.

定理 1.3.9 设 a, b 是任意两个不全为零的整数, d 是正整数, 则 d 是整数 a, b 的最大公因数的充要条件是:

(i) $d\mid a$, $d\mid b$;

(ii) 若 $e\mid a$, $e\mid b$, 则 $e\mid d$.

证 必要性. 若 d 是整数 a, b 的最大公因数, 则显然有 (i) 成立.

再由广义欧几里得除法 (定理 1.3.7) 知, 存在整数 s, t 使得

$$sa+tb=d.$$

因此, 当 $e\mid a$, $e\mid b$ 时, 有

$$e\mid sa+tb=d.$$

故 (ii) 成立.

反过来, 假设 (i) 和 (ii) 成立, 那么

(i) 说明 d 是整数 a, b 的公因数;

(ii) 说明 d 是整数 a, b 的公因数中的最大数, 因为 $e\mid d$ 时, 有 $|e|\leqslant d$.

因此, d 是整数 a, b 的最大公因数. 证毕.

注 定理 1.3.9(ii) 是说: 整数的最大公因数是所有公因数的倍数.

其次, 讨论互素整数的构造 $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$.

定理 1.3.10 设 a, b 是任意两个不全为零的整数,

(i) 若 m 是任一正整数, 则 $(m\cdot a,m\cdot b)=m\cdot(a,b)$.

(ii) 若非零整数 d 满足 $d\mid a$, $d\mid b$, 则 $\left(\dfrac{a}{d},\dfrac{b}{d}\right)=\dfrac{(a,b)}{|d|}$. 特别地,

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1.$$

证 设 $d=(a,b)$, $d'=(m\cdot a,m\cdot b)$. 由广义欧几里得除法 (定理 1.3.7), 存在整数 s, t 使得

$$sa+tb=d.$$

两端同乘以 m, 得到

$$s(m\cdot a)+t(m\cdot b)=m\cdot d.$$

因此 $d'\mid m\cdot d$.

又显然有 $m\cdot d\mid m\cdot a$, $m\cdot d\mid m\cdot b$. 根据定理 1.3.9 (ii), 有 $m\cdot d\mid d'$.

故 $d'=m\cdot d$, 即 (i) 成立.

再根据 (i), 当 $d\mid a$, $d\mid b$ 时, 有

$$\begin{aligned}(a,\ b) &= \left(|d|\cdot\frac{a}{|d|},\ |d|\cdot\frac{b}{|d|}\right)\\ &= |d|\cdot\left(\frac{a}{|d|},\ \frac{b}{|d|}\right)\\ &= |d|\cdot\left(\frac{a}{d},\ \frac{b}{d}\right).\end{aligned}$$

因此, $\left(\dfrac{a}{d},\ \dfrac{b}{d}\right)=\dfrac{(a,b)}{|d|}$. 特别地, 取 $d=(a,\ b)$, 有

$$\left(\frac{a}{(a,b)},\ \frac{b}{(a,b)}\right)=1.$$

故 (ii) 成立. 证毕.

例 1.3.22 设 $a=11\cdot 200\,306$, $b=23\cdot 200\,306$, 计算 $(a,\ b)$.

解 因为

$$(11,\ 23)=(11,\ 23-11\cdot 2)=(11,1)=1,$$

所以

$$(a,\ b)=(11\cdot 200\,306,\ 23\cdot 200\,306)=200\,306.$$

引理 1.3.1 设 a, b 是两个正整数. 则 2^a-1 被 2^b-1 除的最小非负余数是 2^r-1, 其中 r 是 a 被 b 除的最小非负余数. $2^a-1=(2^b-1)q_1+(2^r-1)$, $a=bq+r$

证 当 $a<b$ 时, $r=a$, 结论显然成立. 当 $a\geqslant b$. 对 a, b 用欧几里得除法, 存在不完全商 q 及最小非负余数 r 使得

$$a=q\cdot b+r,\quad 0\leqslant r\leqslant b,$$

进而,

$$2^a-1=2^r((2^b)^q-1)+2^r-1=q_1(2^b-1)+2^r-1,$$

其中 $q_1=2^r((2^b)^{q-1}+\cdots+2^b+1)$ 为整数, 结论成立. 证毕.

引理 1.3.2 设 a, b 是两个正整数, 则 2^a-1 和 2^b-1 的最大公因数是 $2^{(a,b)}-1$.

证 运用广义欧几里得除法及引理 1.3.1 立即得到结论. 证毕.

定理 1.3.10 设 a, b 是两个正整数, 则正整数 2^a-1 和 2^b-1 互素的充要条件是 a 和 b 互素.

证 因为

$$(2^a-1,2^b-1)=2^{(a,b)}-1,$$

而 $2^{(a,b)}-1=1$ 的充要条件是 $(a,b)=1$. 因此, 定理成立. 证毕.

定理 1.4.1 设 a, b, c 是三个整数, 且 $c\neq 0$. 如果 $c\mid ab$, $(a,c)=1$, 则 $c\mid b$.

证一 根据假设条件和定理 1.3.11 有

$$c\mid(ab,c)=(b,c).$$

从而 $c \mid b$.

证二 (直接证明) 因为 $(a,c)=1$. 根据定理 1.3.8 , 存在整数 s,t 使得

$$s\cdot a+t\cdot c=1.$$

两端同乘以 b, 得到

$$s\cdot(a\,b)+(t\,b)\cdot c=b.$$

根据定理 1.1.3, 由 $c \mid a\,b$, $c \mid c$ 可得

$$c \mid s\cdot(a\,b)+(t\,b)\cdot c=b,$$

即 $c \mid b$. 证毕.

例 1.4.1 因为 $15 \mid 2\cdot 75$, 又 $(2,15)=1$, 所以 $15 \mid 75$.

定理 1.4.4 设 a, b 是两个互素正整数, 则

(ⅰ) 若 $a \mid D$, $b \mid D$, 则 $a\cdot b \mid D$;

(ⅱ) $[a,b]=a\cdot b$.

(ⅰ) 设 $b \mid D$, 则存在整数 q, 使得 $D=q\cdot b$. 又 $a \mid D$, 即 $a \mid q\cdot b$, 以及 $(a,b)=1$, 根据定理 1.3.11 的推论, 得到 $a \mid q$. 因此存在整数 q', 使得 $q=q'\cdot a$, 进而, $D=q'\cdot(a\cdot b)$. 故 $a\cdot b \mid D$. (ⅰ) 得证.

(ⅱ) 显然 $a\cdot b$ 是 a, b 的公倍数. 又由 (ⅰ) 知, $a\cdot b$ 是 a, b 的公倍数中的最小正整数, 故 $[a,b]=a\cdot b$.

(ⅰ) **的直接证明** 由 $a \mid D$, $b \mid D$, 知存在 q_1, q_2 使得 $D=q_1\cdot a$, $D=q_2\cdot b$. 从而, $b\cdot D=q_1\cdot(a\cdot b)$, $a\cdot D=q_2\,(a\cdot b)$. 因为 $(a,b)=1$, 所以由广义欧几里得除法, 可找到整数 s,t , 使得 $s\cdot a+t\cdot b=(a,b)=1$, 进而 $D=(s\cdot a+t\cdot b)D=s\cdot(a\cdot D)+t\cdot(b\cdot D)=s\cdot q_2\cdot(a\cdot b)+t\cdot q_1\cdot(a\cdot b)=(s\cdot q_2+t\cdot q_1)(a\cdot b)$, 故 $a\cdot b \mid D$. 证毕.

例 1.4.4 设 p, q 是两个不同的素数, 则 $[p,q]=p\cdot q$.

定理 1.4.5 设 a, b 是两个正整数. 则

(ⅰ) 若 $a \mid D$, $b \mid D$, 则 $[a,b] \mid D$;

(ⅱ) $[a,b]=\dfrac{a\cdot b}{(a,b)}$.

证 令 $d=(a,b)$. 根据定理 1.3.10, 有

$$\left(\frac{a}{d},\frac{b}{d}\right)=1.$$

又根据定理 1.4.4,

$$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{a}{d}\cdot\frac{b}{d},$$

进而 $[a,b]=\dfrac{a\cdot b}{d}$, 即 (ⅱ) 成立.

再由

$$\frac{a}{d} \mid \frac{D}{d},\qquad \frac{b}{d} \mid \frac{D}{d},$$

得到

$$\frac{a}{d}\cdot\frac{b}{d} \mid \frac{D}{d}.$$

从而 $\dfrac{a\cdot b}{d} \mid D$, 即 (ⅰ) 成立. 证毕.

定理 1.6.1 (算术基本定理) 任一整数 $n>1$ 都可以表示成素数的乘积, 且在不考虑乘积顺序的情况下, 该表达式是唯一的, 即

$$n=p_1\cdots p_s, \qquad p_1\leqslant\cdots\leqslant p_s, \tag{1.21}$$

其中 p_i 是素数, 并且若

$$n=q_1\cdots q_t, \qquad q_1\leqslant\cdots\leqslant q_t,$$

其中 q_j 是素数, 则 $s=t$, $p_i=q_i$, $1\leqslant i\leqslant s$.

例 1.6.3 设正整数 n 有因数分解式

$$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}, \quad \alpha_i>0,\ i=1,\cdots,s.$$

则 n 的因数个数

$$d(n)=(1+\alpha_1)\cdots(1+\alpha_s).$$

例 1.6.6 设 n 是合数, p 是 n 的素因数. 设 $p^\alpha \,||\, n$ (即 $p^\alpha \mid n$, 但 $p^{\alpha+1}\nmid n$), 则 $p^\alpha \nmid \binom{n}{p}$, 其中 $\binom{n}{p}=\dfrac{n(n-1)\cdots(n-p+1)}{p!}$.

证 因为 $p^\alpha \,||\, n$, 设 $n=n'\cdot p^\alpha$, $(n',p)=1$, 则对于 $1\leqslant k\leqslant p-1$, 有 $(n-k,p)=1$. 否则, $p|n-(n-k)=k$, 矛盾. 根据定理 1.3.12, 有 $((n-1)\cdots(n-p+1),p)=1$. 从而,

$$\binom{n}{p}=\frac{n}{p}\frac{(n-1)\cdots(n-p+1)}{(p-1)!}=n'\cdot\frac{(n-1)\cdots(n-p+1)}{(p-1)!}\cdot p^{\alpha-1}.$$

但

$$\left(n'\cdot\frac{(n-1)\cdots(n-p+1)}{(p-1)!},\ p\right)=1,$$

故 $p^\alpha \nmid \binom{n}{p}$. 证毕.

注 例 1.6.6 将应用于 AKS 的证明.

定义 2.1.1 给定一个正整数 m. 两个整数 a, b 叫做模 m **同余**[1], 如果 $a-b$ 被 m 整除, 或 $m \mid a-b$, 就记作 $a \equiv b \pmod{m}$. 否则, 叫做模 m **不同余**, 记作 $a \not\equiv b \pmod{m}$.

定理 2.1.2 设 m 是一个正整数, 则模 m 同余是等价关系, 即

(1) (自反性) 对任一整数 a, 有 $a \equiv a \pmod{m}$.

(2) (对称性) 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$.

(3) (传递性) 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$.

证 可运用定理 2.1.1 来给出证明.

(1) (自反性) 对任一整数 a, $a = a + 0 \cdot m$, 所以

$$a \equiv a \pmod{m}.$$

(2) (对称性) 若 $a \equiv b \pmod{m}$, 则存在整数 k 使得

$$a = b + q \cdot m,$$

从而有

$$b = a + (-q) \cdot m.$$

因此,

$$b \equiv a \pmod{m}.$$

(3) (传递性) 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则分别存在整数 q_1, q_2 使得

$$a = b + q_1 \cdot m, \qquad b = c + q_2 \cdot m,$$

从而

$$a = c + (q_1 + q_2) \cdot m.$$

因为 $q_1 + q_2$ 是整数, 所以

$$a \equiv c \pmod{m}.$$

证毕.

例 2.1.3 因为 $39 \equiv 32 \pmod{7}$, $32 \equiv 25 \pmod{7}$, 所以

$$39 \equiv 25 \pmod{7}. \qquad \text{传递性}$$

同时有

$$39 \equiv 39 \pmod{7}, \qquad 25 \equiv 25 \pmod{7}, \qquad \text{自反性}$$

以及

$$32 \equiv 39 \pmod{7}, \qquad 25 \equiv 32 \pmod{7}. \qquad \text{对称性}$$

定理 2.1.4 设 m 是一个正整数, 设 a_1, a_2, b_1, b_2 是 4 个整数. 如果

$$a_1 \equiv b_1 \pmod{m}, \qquad a_2 \equiv b_2 \pmod{m},$$

则

(i) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$. (2.3)

(ii) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$. (2.4)

证 依题设, 根据定理 2.1.1 , 分别存在整数 q_1, q_2 使得

$$a_1 = b_1 + q_1 \cdot m, \quad a_2 = b_2 + q_2 \cdot m,$$

从而

$$\begin{aligned} a_1 + a_2 &= b_1 + b_2 + (q_1 + q_2) \cdot m, \\ a_1 \cdot a_2 &= b_1 \cdot b_2 + (q_1 \cdot m) \cdot b_2 + b_1 \cdot (q_2 \cdot m) + (q_1 \cdot m)(q_2 \cdot m) \\ &= b_1 \cdot b_2 + (q_1 + q_2 + q_1 \cdot q_2 \cdot m) \cdot m. \qquad \text{(交换性)} \end{aligned}$$

因为 $q_1 + q_2$, $q_1 + q_2 + q_1 \cdot q_2 \cdot m$ 都是整数, 所以根据定理 2.1.1, 可知式 (2.3) 和式 (2.4) 成立, 即定理成立. 证毕.

例 2.1.5 2003 年 5 月 9 日是星期五, 问第 2^{2003} 天是星期几?

解 因为

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 = 8 \equiv 1 \pmod{7},$$

又 $2003 = 667 \cdot 3 + 2$, 所以

$$2^{2003} = (2^3)^{667} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{7}.$$

故第 2^{2003} 天是星期二.

定理 2.1.6 设整数 n 有十进制表示式

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0, \quad 0 \leqslant a_i < 10.$$

则 (i) $3 \mid n$ 的充分必要条件是

$$3 \mid a_k + \cdots + a_0. \tag{2.6}$$

(ii) $9 \mid n$ 的充分必要条件是

$$9 \mid a_k + \cdots + a_0. \tag{2.7}$$

定理 2.1.7 设整数 n 有一千进制表示式:

$$n = a_k 1000^k + \cdots + a_1 1000 + a_0, \qquad 0 \leqslant a_i < 1000.$$

则 7(或 11, 或 13) 整除 n 的充分必要条件是 7 (或 11, 或 13) 能整除整数

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

例 2.1.16 设 p, q 是不同的素数. 如果整数 a, b 满足

$$a \equiv b \pmod{p}, \quad a \equiv b \pmod{q},$$

则有

$$a \equiv b \pmod{p \cdot q}.$$

证 设 $a \equiv b \pmod{p}$, $a \equiv b \pmod{p}$, 则

$$p \mid a-b, \quad q \mid a-b.$$

因为 p, q 是不同的素数, 所以根据定理 1.4.4, 有

$$p \cdot q \mid a-b.$$

即

$$a \equiv b \pmod{p \cdot q}.$$

证毕.

例 2.1.17 设 m, n, a 都是正整数. 如果

$$n^a \not\equiv 0, 1 \pmod{m}, \tag{2.9}$$

则存在 n 的一个素因数 p 使得

$$p^a \not\equiv 0, 1 \pmod{m}. \tag{2.10}$$

证 反证法. 如果存在 n 的一个素因数 p, 使得 $p^a \equiv 0 \pmod{m}$, 则 $m \mid p^a$. 但 $p^a \mid n^a$, 故 $m \mid n^a$, 即 $n^a \equiv 0 \pmod{m}$. 这与假设式 (2.9) 矛盾.

如果对 n 的每个素因数 p, 都有

$$p^a \equiv 1 \pmod{m}.$$

根据定理 2.1.4 (ii), 有

$$n^a \equiv 1 \pmod{m}.$$

这也与假设式 (2.9) 矛盾. 因此, 结论式 (2.10) 成立. 证毕.

设 m 是一个正整数. 对任意整数 a, 令

$$C_a = \{c \mid c \in \mathbf{Z},\ c \equiv a \pmod{m}\}. \tag{2.11}$$

C_a 是非空集合, 因为 $a \in C_a$.

定理 2.2.1 设 m 是一个正整数, 则

(i) 任一整数必包含在一个 C_r 中, $0 \leqslant r \leqslant m-1$;

(ii) $C_a = C_b$ 的充分必要条件是

$$a \equiv b \pmod{m}. \tag{2.12}$$

(iii) C_a 与 C_b 的交集为空集的充分必要条件是

$$a \not\equiv b \pmod{m}. \tag{2.13}$$

定义 2.3.1 设 m 是一个正整数，则 m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数的个数，记作 $\varphi(m)$，通常叫做**欧拉 (Euler) 函数**.

例 2.3.1 设 $m=10$. 则 10 个整数 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 中与 10 互素的整数为 1, 3, 7, 9，所以 $\varphi(10)=4$.

例 2.3.2 设 $m=p$ 为素数，则 p 个整数 $1, 2, \ldots, p-1, p$ 中与 p 互素的整数为 $1, 2, \ldots, p-1$，所以 $\varphi(p)=p-1$.

定理 2.3.1 对于素数幂 $m=p^{\alpha}$，有

$$\varphi(m)=p^{\alpha}-p^{\alpha-1}=m\prod_{p\mid m}\left(1-\frac{1}{p}\right). \tag{2.26}$$

→ p|m时连乘

例 2.3.3 设 $m=7^2$，则 $\varphi(7^2)=7^2\left(1-\frac{1}{7}\right)=42$.

定理 2.3.5 设 m 是一个正整数，a 是满足 $(a,m)=1$ 的整数，则存在唯一的整数 a'，$1\leqslant a'<m$ 使得

$$a\cdot a'\equiv 1 \pmod{m}. \tag{2.31}$$

a'为a模m的一个逆元

证一 (存在性证明) 因为 $(a,m)=1$，根据定理 2.3.4，k 遍历模 m 的一个最小简化剩余系时，$a\cdot k$ 也遍历模 m 的一个简化剩余系. 因此，存在整数 $k=a'$，$1\leqslant a'<m$ 使得 $a\cdot a'$ 属于 1 的剩余类，即式 (2.31) 成立.

(唯一性证明) 若有整数 a'，a'' $1\leqslant a', a''<m$ 使得

$$a\cdot a'\equiv 1, \quad a\cdot a''\equiv 1 \pmod{m},$$

则 $a(a'-a'')\equiv 0 \pmod{m}$，从而，$a'-a''\equiv 0 \pmod{m}$. 故 $a'=a''$. 证毕.

因为在实际运用中，常常需要具体地求出整数，所以运用广义欧几里得除法给出定理 2.3.5 的构造性证明.

证二 (构造性证明) 因为 $(a,m)=1$，根据定理 1.3.7，运用广义欧几里得除法，可找到整数 s，t 使得

$$s\cdot a+t\cdot m=(a,m)=1.$$

因此，整数 $a'=s$ ~~$\pmod m$~~ 满足式 (2.31). 证毕.

定理 2.3.7 设 m，n 是互素的两个正整数，则

$$\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n). \tag{2.33}$$

证 根据定理 2.3.6，当 k_1 遍历模 m 的简化剩余系，共 $\varphi(m)$ 个整数，以及 k_2 遍历模 n 的简化剩余系，共 $\varphi(n)$ 个整数时，$n\cdot k_1+m\cdot k_2$ 遍历模 $m\cdot n$ 的简化剩余系，其整数个数为 $\varphi(m)\cdot\varphi(n)$. 但模 $m\cdot n$ 的简化剩余系的元素个数又为 $\varphi(m\cdot n)$，故式 (2.33) 成立. 证毕.

例 2.3.15 $\varphi(77)=\varphi(7)\varphi(11)=6\cdot 10=60$.

例 2.3.16 $\varphi(30)=\varphi(2)\varphi(3)\varphi(5)=1\cdot 2\cdot 4=8$.

下面再给出欧拉函数 $\varphi(m)$ 的计算.

定理 2.3.8 设正整数 m 的标准因数分解式为

$$m=\prod_{p\mid m}p^{\alpha}=p_1^{\alpha_1}\cdots p_k^{\alpha_s},$$

则

$$\varphi(m)=m\prod_{p\mid m}\left(1-\frac{1}{p}\right)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right). \tag{2.34}$$

证 由欧拉函数的可乘性 (定理 2.3.7 的式 (2.33)), 以及定理 2.3.1 的式 (2.26), 有

$$\begin{aligned}\varphi(m) &= \prod_{p|m}\varphi(p^\alpha) = \prod_{p|m}(p^\alpha - p^{\alpha-1}) \\ &= m\Big(1-\frac{1}{p_1}\Big)\cdots\Big(1-\frac{1}{p_k}\Big).\end{aligned}$$

证毕.

特别地, 当 m 是不同素数 p, q 的乘积时, 有

推论 设 p, q 是不同的素数, 则

$$\varphi(p\cdot q) = p\cdot q - p - q + 1. \tag{2.35}$$

定理 2.4.1 (Euler) 设 m 是大于 1 的整数. 如果 a 是满足 $(a,m)=1$ 的整数, 则

$$a^{\varphi(m)} \equiv 1 \pmod m. \tag{2.37}$$

定理 2.4.2 (Fermat) 设 p 是一个素数, 则对任意整数 a, 有

$$a^p \equiv a \pmod p. \tag{2.42}$$

逆定理: 设n是一个奇正整数, 若$(a,n)=1$, 且a^n 则n是合

证 分两种情形考虑.

(i) 若 a 被 p ~~整数~~ 整除, 则同时有

$$a \equiv 0 \pmod p \quad 和 \quad a^p \equiv 0 \pmod p.$$

因此式 (2.42) 成立.

(ii) 若 a 不被 p 整数, 则 $(a,p)=1$ (见例 1.3.4). 根据定理 2.4.1 式 (2.37),

$$a^{p-1} \equiv 1 \pmod p.$$

两端同乘 a, 得到式 (2.42). 证毕.

定理 2.4.3 (Wilson) 设 p 是一个素数. 则

$$(p-1)! \equiv -1 \pmod p. \tag{2.44}$$

证 若 $p=2$, 结论显然成立.

现设 $p \geqslant 3$. 根据定理 2.3.5, 对于每个整数 a, $1 \leqslant a \leqslant p-1$, 存在唯一的整数 a', $1 \leqslant a' \leqslant p-1$, 使得

$$a\cdot a' \equiv 1 \pmod p.$$

而 $a' = a$ 的充要条件是 a 满足

$$a^2 \equiv 1 \pmod p. \Rightarrow a^2-1 \equiv 0 \pmod p$$

这时, $a=1$ 或 $a=p-1$. $\Rightarrow (a+1)(a-1) \equiv 0 \pmod p$

$\Rightarrow a+1 \equiv 0 \pmod p \Rightarrow a = p-1$

或 $a-1 \equiv 0 \pmod p \Rightarrow a=1$

将 $2,\cdots,p-2$ 中的 a 与 a' 配对, 得到

$$\begin{aligned}1\cdot 2\cdot\cdots\cdot(p-2)(p-1) &\equiv 1\cdot(p-1)\prod_a a\cdot a' \\ &\equiv 1\cdot(p-1) \\ &\equiv -1 \pmod p.\end{aligned}$$

因此, 定理 2.4.3 成立. 证毕.

定义 3.1.1 设 m 是一个正整数，$f(x)$ 为多项式

$$f(x)=a_nx^n+\cdots+a_1x+a_0,$$

其中 a_i 是整数，则

$$f(x)\equiv 0\ (\mathrm{mod}\ m) \tag{3.1}$$

叫做模 m **同余式**. 若 $a_n\not\equiv 0\ (\mathrm{mod}\ m)$，则 n 叫做 $f(x)$ 的**次数**，记为 $\deg f$. 此时，式 (3.1) 又叫做模 m 的n **次同余式**.

如果整数 $x=a$ 使得式 (3.1) 成立，即

$$f(a)\equiv 0\ (\mathrm{mod}\ m)$$

则 a 叫做该同余式 (3.1) 的 **解**. 事实上，满足 $x\equiv a\ (\mathrm{mod}\ m)$ 的所有整数都使得同余式 (3.1) 成立，即 a 所在剩余类

$$C_a=\{c\mid c\in\mathbf{Z},\ c\equiv a\ (\mathrm{mod}\ m)\}$$

中的每个剩余都使得同余式 (3.1) 成立，因此，同余式 (3.1) 的解 a 通常写成

$$x\equiv a\ (\mathrm{mod}\ m).$$

在模 m 的完全剩余系中，使得同余式 (3.1) 成立的剩余个数叫做同余式 (3.1) 的**解数**.

定理 3.1.3 设 m 是一个正整数，a 是满足 $m\nmid a$ 的整数，则一次同余式

$$ax\equiv b\ (\mathrm{mod}\ m) \tag{3.3}$$

有解的充分必要条件是 $(a,m)\mid b$. 而且，当同余式 (3.3) 有解时，其解为

$$x\equiv\frac{b}{(a,m)}\cdot\left(\left(\frac{a}{(a,m)}\right)^{-1}\left(\mathrm{mod}\ \frac{m}{(a,m)}\right)\right)+t\cdot\frac{m}{(a,m)}\ (\mathrm{mod}\ m),$$

$t=0,\ 1,\cdots,\ (a,m)-1.$ 共 (a,m) 个解

定理 3.2.1 (**中国剩余定理**) 设 $m_1,\cdots,m_k$ 是 k 个两两互素 的正整数，则对任意的整数 $b_1,\cdots,b_k$，同余式组

$$\begin{cases} x\equiv b_1 & (\mathrm{mod}\ m_1)\\ \quad\vdots & \\ x\equiv b_k & (\mathrm{mod}\ m_k)\end{cases} \tag{3.8}$$

一定有解，且解是唯一的. 事实上，

(i) 若令

$$m=m_1\cdots m_k,\quad m=m_i\cdot M_i,\quad i=1,\cdots,k,$$

则同余式组 (3.8) 的解可表示为

$$x\equiv b_1\cdot M_1'\cdot M_1+b_2\cdot M_2'\cdot M_2+\cdots+b_k\cdot M_k'\cdot M_k\ (\mathrm{mod}\ m), \tag{3.9}$$

其中

$$M_i'\cdot M_i\equiv 1\ (\mathrm{mod}\ m_i),\ i=1,2,\cdots,k.$$

(ii) 若令

$$N_i=m_1\cdots m_i,\quad i=1,\cdots,k-1,$$

则同余式组 (3.8) 的解可表示为

$$x\equiv x_k\ (\mathrm{mod}\ m_1\cdots m_k),$$

其中 $N_i' \cdot N_i \equiv 1 \pmod{m_{i+1}}$, $i = 1, 2, \cdots, k-1$, 而 x_i 是同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv b_i \pmod{m_i} \end{cases}$$

的解, $i = 1, \cdots, k$, 并满足递归关系式

$$x_i \equiv x_{i-1} + ((b_i - x_{i-1})N_{i-1}' \pmod{m_i}) \cdot N_{i-1} \pmod{m_1 \cdots m_i}, \quad i = 2, \cdots, k. \tag{3.10}$$

定理 3.4.4 同余式 (3.26) 的解数不超过它的次数.

证 反证法. 设 n 次同余式 (3.26) 的解数超过 n 个, 则式 (3.26) 至少有 $n+1$ 个解. 设它们为

$$x \equiv a_i \pmod{p}, \quad i = 1, \cdots, n, n+1.$$

根据定理 3.4.2, 对于 n 个解 $a_1, \cdots, a_n$, 可得到

$$f(x) \equiv f_n(x)(x - a_1) \cdots (x - a_n) \pmod{p}.$$

因为 $f(a_{n+1}) \equiv 0 \pmod{p}$, 所以

定理 3.4.4 同余式 (3.26) 的解数不超过它的次数.
证 反证法. 设 n 次同余式 (3.26) 的解数超过 n 个, 则式 (3.26) 至少有 $n+1$ 个解. 设
它们为
$x \equiv a_i \pmod{p}, \quad i = 1, \cdots, n, n+1.$

因为 $a_i \not\equiv$ 它们为 $f_n(x)$ 是首项系数为 a 证毕.

$f_n(a_{n+1}) \equiv a_n \Leftarrow$ $\Rightarrow a_n \equiv 0 \pmod{p}$ 但是 p 不能整除 a_n ∴矛盾

推论 次数 $< p$ 的整系数多项式对所有整数取值模 p 为零的充要条件是其系数被 p 整除.

证 充分性显然. 下面证必要性. 若不然, 多项式 $f(x)$ 有系数不被 p 整除, 这说明模 p 多项式 $f(x) \pmod{p}$ 次数 $< p$. 根据定理 3.4.4, 多项式的解数 $< p$, 与假设条件矛盾, 故推论成立. 证毕.

再给出同余式解数的判断.

定理 3.4.5 设 p 是一个素数, n 是一个正整数, $n \leqslant p$. 那么同余式

$$f(x) = x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p} \tag{3.29}$$

有 n 个解的充分必要条件是 $x^p - x$ 被 $f(x)$ 除所得余式的所有系数都是 p 的倍数.

定义 4.1.1 设 m 是正整数. 若同余式

$$x^2 \equiv a \pmod{m}, \qquad (a, m) = 1 \tag{4.3}$$

有解, 则 a 叫做模 m 的**平方剩余**(或**二次剩余**); 否则, a 叫做模 m 的**平方非剩余**(或**二次非剩余**).

定理 4.2.1 (欧拉判别条件) 设 p 是奇素数, $(a, p) = 1$, 则

(i) a 是模 p 的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

(ii) a 是模 p 的平方非剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

并且当 a 是模 p 的平方剩余时, 同余式 (4.4) 恰有二解.

定义 4.3.1 设 p 是素数. 定义**勒让得 (Legendre) 符号** 如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 是模 } p \text{ 的平方剩余;}\\ -1, & \text{若 } a \text{ 是模 } p \text{ 的平方非剩余;}\\ 0, & \text{若 } p \mid a.\end{cases}$$

由此, 对于 $(a,p)=1$, 有

$$\left(\frac{a}{p}\right)=1 \quad \Longleftrightarrow \quad x^2\equiv a \pmod p \text{ 有解}$$

$$\left(\frac{a}{p}\right)=-1 \quad \Longleftrightarrow \quad x^2\equiv a \pmod p \text{ 无解}$$

定理 4.3.2 设 p 是奇素数, 则

$$(1)\ \left(\frac{1}{p}\right)=1; \tag{4.11}$$

$$(2)\ \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}. \tag{4.12}$$

证 根据欧拉判别法则 (定理 4.3.1), 对于 $a=1$ 时, 有 $a^{\frac{p-1}{2}}=1$, 所以式 (4.11) 成立; 而对于 $a=-1$ 时, 有 $a^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}$, 又因为 p 是奇数, 所以式 (4.12) 成立. 证毕.

进一步, 可以给出 p 的表达式.

推论 设 p 是奇素数, 那么

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{若 } p\equiv 1 \pmod 4;\\ -1, & \text{若 } p\equiv 3 \pmod 4.\end{cases} \tag{4.13}$$

证 根据欧拉判别法则 (定理 4.3.1), 有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

若 $p\equiv 1 \pmod 4$, 则存在正整数 k 使得 $p=4k+1$, 从而

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1.$$

若 $p\equiv 3 \pmod 4$, 则存在正整数 k 使得 $p=4k+3$, 从而

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k+1}=-1.$$

定理 4.3.3 设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$;

(ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) 设 $(a,p)=1$, 则 $\left(\frac{a^2}{p}\right)=1$.

引理 4.3.1 (Gauss) 设 p 是奇素数. a 是整数, $(a,p)=1$. 如果整数

$$a\cdot 1,\ a\cdot 2,\ \cdots,\ a\cdot\frac{p-1}{2}$$

中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m, 则

$$\left(\frac{a}{p}\right)=(-1)^m.$$

定理 4.4.1 (二次互反律) 若 p, q 是互素奇素数, 则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

定义 4.5.1 设 $m=p_1\cdots p_r$ 是奇素数 p_i 的乘积. 对任意整数 a, 定义**雅可比 (Jacobi) 符号** 为

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right). \tag{4.23}$$

雅可比符号形式上是勒让得符号的推广, 但所蕴涵的意义已经不同. 与式 (4.10) 作比较, 对于 $(a,m)=1$, 有

$$\begin{aligned}&\left(\frac{a}{m}\right)=1 \quad \Longleftarrow \quad x^2\equiv a \pmod m \text{ 有解}\\ &\left(\frac{a}{m}\right)=-1 \quad \Longrightarrow \quad x^2\equiv a \pmod m \text{ 无解}\end{aligned} \tag{4.24}$$

雅可比符号为 -1, 可判断 a 是模 m 平方非剩余; 但雅可比符号为 1, 却不能判断 a 是模 m 平方剩余. 例如, 3 是模 119 平方非剩余, 但

$$\left(\frac{3}{119}\right)=\left(\frac{3}{7}\right)\left(\frac{3}{17}\right)=(-1)(-1)=1.$$

定义 5.1.1 设 $m>1$ 是整数, a 是与 m 互素的正整数, 则使得

$$a^e\equiv 1 \pmod m$$

成立的最小正整数 e 叫做 a 对模 m 的 **指数**, 记作 $\mathrm{ord}_m(a)$.

如果 a 对模 m 的指数是 $\varphi(m)$, 则 a 叫做模 m 的 **原根**.

例 5.1.1 设整数 $m=7$, 这时 $\varphi(7)=6$. 有

$$\begin{aligned}&1^1\equiv 1, && 2^3=8\equiv 1, && 3^3=27\equiv -1,\\ &4^3\equiv(-3)^3\equiv 1, && 5^3\equiv(-2)^3\equiv -1, && 6^2\equiv(-1)^2\equiv 1 \pmod 7.\end{aligned}$$

列成表为

a	1	2	3	4	5	6
$\mathrm{ord}_m(a)$	1	3	6	3	6	2

因此, 3, 5 是模 7 的原根. 但 2, 4, 6 不是模 7 的原根.

例 5.1.2 设整数 $m=14=2\cdot 7$, 这时 $\varphi(14)=6$. 有

$$\begin{aligned}&1^1\equiv 1, && 3^3=27\equiv -1, && 5^3=125\equiv -1,\\ &9^3=(\ 5)^3=1, && 11^3=(\ 3)^3=1, && 13^2=(\ 1)^2=1 \pmod{14}.\end{aligned}$$

列成表为

a	1	3	5	9	11	13
$\mathrm{ord}_m(a)$	1	6	6	3	3	2

因此, 3, 5 是模 14 的原根. 但 9, 11, 13 不是模 14 的原根.

定理 5.1.1 设 $m>1$ 是整数, a 是与 m 互素的整数, 则整数 d 使得

$$a^d \equiv 1 \pmod{m} \tag{5.4}$$

的充分必要条件是

$$\mathrm{ord}_m(a) \mid d. \tag{5.5}$$

证 充分性. 设式 (5.5) 成立, 即 $\mathrm{ord}_m(a) \mid d$, 那么存在整数 q 使得 $d = q \cdot \mathrm{ord}_m(a)$. 因此, 有

$$a^d = \left[a^{\mathrm{ord}_m(a)}\right]^q \equiv 1 \pmod{m}.$$

必要性. 反证法. 如果式 (5.5) 不成立, 即 $\mathrm{ord}_m(a) \nmid d$, 则由欧几里得除法 (定理 1.1.9), 存在整数 q, r 使得

$$d = q \cdot \mathrm{ord}_m(a) + r, \qquad 0 < r < \mathrm{ord}_m(a).$$

从而,

$$a^r \equiv \left[a^{\mathrm{ord}_m(a)}\right]^q \cdot a^r = a^d \equiv 1 \pmod{m}.$$

这与 $\mathrm{ord}_m(a)$ 的最小性矛盾. 故式 (5.5) 成立. 证毕.

推论 1 设 $m>1$ 是整数, a 是与 m 互素的整数, 则

$$\mathrm{ord}_m(a) \mid \varphi(m). \tag{5.6}$$

证 根据欧拉定理 (定理 2.4.1), 有

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

由定理 5.1.1, 有式 (5.6). 证毕.

例 5.1.1 求整数 5 模 17 的指数 $\mathrm{ord}_{17}(5)$.

解 因为 $\varphi(17) = 16$, 所以只需对 16 的因数 $d = 1,\ 2,\ 4,\ 8,\ 16$, 计算 $a^d \pmod{m}$. 因为

$$5^1 \equiv 5,\ 5^2 = 25 \equiv 8,\ 5^4 \equiv 64 \equiv 13 \equiv -4, 5^8 \equiv (-4)^2 \equiv 16 \equiv -1,\ 5^{16} \equiv (-1)^2 \equiv 1 \pmod{17},$$

所以 $\mathrm{ord}_{17}(5) = 16$. 这说明 5 是模 17 的原根.

推论 2 设 p 是奇素数, 且 $\dfrac{p-1}{2}$ 也是素数. 如果 a 是一个模 p 不为 $0,\ 1, -1$ 的整数, 则

$$\mathrm{ord}_p(a) = \frac{p-1}{2} \text{ 或 } p-1.$$

证 根据欧拉定理 (定理 2.4.1), 有

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

根据推论 1, 整数 a 模 p 的指数 $\mathrm{ord}_p(a)$ 是 $\varphi(p) = p-1 = 2 \cdot \dfrac{p-1}{2}$ 的因数, 但 $\mathrm{ord}_m(a) \neq 2$, 所以

$$\mathrm{ord}_p(a) = \frac{p-1}{2} \text{ 或 } p-1.$$

性质 5.1.1 设 $m>1$ 是整数, a 是与 m 互素的整数.

(ⅰ) 若 $b\equiv a \pmod m$, 则 $\operatorname{ord}_m(b)=\operatorname{ord}_m(a)$.

(ⅱ) 设 a^{-1} 使得 $a^{-1}\cdot a\equiv 1 \pmod m$, 则 $\operatorname{ord}_m(a^{-1})=\operatorname{ord}_m(a)$.

证 (ⅰ) 若 $b\equiv a \pmod m$, 则

$$b^{\operatorname{ord}_m(b)} \equiv b^{\operatorname{ord}_m(a)} \equiv a^{\operatorname{ord}_m(a)} \equiv 1 \pmod m,$$

根据定理 5.1.1 式 (5.5), 有 $\operatorname{ord}_m(b) \mid \operatorname{ord}_m(a)$.

同样, 有 $\operatorname{ord}_m(a) \mid \operatorname{ord}_m(b)$. 故 $\operatorname{ord}_m(b)=\operatorname{ord}_m(a)$.

(ⅱ) 因为

$$(a^{-1})^{\operatorname{ord}_m(a^{-1})} \equiv (a^{-1})^{\operatorname{ord}_m(a)} \equiv \left[a^{\operatorname{ord}_m(a)}\right]^{-1} \equiv 1 \pmod m,$$

根据定理 5.1.1 式 (5.5), 有 $\operatorname{ord}_m(a^{-1}) \mid \operatorname{ord}_m(a)$.

同样, 有 $\operatorname{ord}_m(a) \mid \operatorname{ord}_m(a^{-1})$. 故 $\operatorname{ord}_m(a^{-1})=\operatorname{ord}_m(a)$. 证毕.

例 5.1.8 整数 39 模 17 的指数为 $\operatorname{ord}_{17}(39)=\operatorname{ord}_{17}(5)=16$. 整数 7 模 17 的指数为 16. 因为 $5^{-1}\equiv 7 \pmod m$.

定理 5.1.2 设 $m>1$ 是整数, a 是与 m 互素的整数, 则

$$1=a^0,\ a,\ \cdots,\ a^{\operatorname{ord}_m(a)-1} \tag{5.7}$$

模 m 两两不同余. 特别地, 当 a 是模 m 的原根, 即 $\operatorname{ord}_m(a)=\varphi(m)$ 时, 这 $\varphi(m)$ 个数

$$1=a^0,\ a,\ \cdots,\ a^{\varphi(m)-1} \tag{5.8}$$

组成模 m 的简化剩余系.

证 反证法. 如果式 (5.7) 中有两个数模 m 同余, 则存在整数 $0\leqslant k,\ l<\operatorname{ord}_m(a)$ 使得

$$a^k\equiv a^l \pmod m.$$

不妨设 $k>l$. 则由 $(a,m)=1$ 和定理 2.1.8, 得

$$a^{k-l}\equiv 1 \pmod m.$$

但 $0<k-l<\operatorname{ord}_m(a)$. 这与 $\operatorname{ord}_m(a)$ 的最小性矛盾. 因此, 结论成立.

再设 a 是模 m 的原根, 即 $\operatorname{ord}_m(a)=\varphi(m)$, 则有 $\varphi(m)$ 个数即式 (5.8), 也即

$$1=a^0,\ a,\ \cdots,\ a^{\varphi(m)-1}$$

模 m 两两不同余. 根据定理 2.3.3, 这 $\varphi(m)$ 个数组成模 m 的简化剩余系. 证毕.

定理 5.1.3 设 $m>1$ 是整数, a 是与 m 互素的整数, 则

$$a^d\equiv a^k \pmod m$$

的充分必要条件是

$$d\equiv k \pmod{\operatorname{ord}_m(a)}.$$

证 根据欧几里得除法 (定理 1.1.9) , 存在整数 $q,\ r$ 和 $q',\ r'$ 使得

$$\begin{aligned} d&=\ q\cdot\operatorname{ord}_m(a)+r, \quad 0\leqslant r<\operatorname{ord}_m(a).\\ k&=q'\cdot\operatorname{ord}_m(a)+r', \quad 0\leqslant r'<\operatorname{ord}_m(a).\end{aligned}$$

又 $a^{\operatorname{ord}_m(a)}\equiv 1 \pmod m$, 故

$$a^d\equiv (a^{\operatorname{ord}_m(a)})^q\cdot a^r\equiv a^r, \quad a^k\equiv a^{r'} \pmod m.$$

必要性. 若 $a^d \equiv a^k$, 则

$$a^r \equiv a^{r'} \pmod{m}.$$

由定理 5.1.2, 得到 $r = r'$. 故 $d \equiv k \pmod{\operatorname{ord}_m(a)}$.

充分性. 若 $d \equiv k \pmod{\operatorname{ord}_m(a)}$, 则

$$r = r', \quad a^d \equiv a^k \pmod{m}.$$

因此, 定理成立. 证毕.

例 5.1.10 $2^{1\,000\,000} \equiv 2^{10} \equiv 100 \pmod{231}$.

因为整数 2 模 231 的指数为 $\operatorname{ord}_{231}(2) = 30$, $1\,000\,000 \equiv 10 \pmod{30}$.

例 5.1.11 $2^{2002} = 2^1 = 2 \pmod{7}$.

因为整数 2 模 7 的指数为 $\operatorname{ord}_7(2) = 3$, $2002 \equiv 1 \pmod{3}$.

定理 5.1.4 设 $m > 1$ 是整数, a 是与 m 互素的整数. 设 d 为非负整数, 则

$$\operatorname{ord}_m(a^d) = \frac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))}. \tag{5.9}$$

证 因为

$$a^{d \operatorname{ord}_m(a^d)} = \left(a^d\right)^{\operatorname{ord}_m(a^d)} \equiv 1 \pmod{m},$$

根据定理 5.1.1, $\operatorname{ord}_m(a) \mid d \operatorname{ord}_m\left(a^d\right)$. 从而

$$\frac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))} \mid \operatorname{ord}_m(a^d) \cdot \frac{d}{(d, \operatorname{ord}_m(a))}.$$

因为 $\left(\dfrac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))}, \dfrac{d}{(d, \operatorname{ord}_m(a))}\right) = 1$, 根据定理 1.3.11 之推论,

$$\frac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))} \mid \operatorname{ord}_m(a^d).$$

另一方面, 有

$$(a^d)^{\frac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))}} = \left(a^{\operatorname{ord}_m(a)}\right)^{\frac{d}{(d, \operatorname{ord}_m(a))}} \equiv 1 \pmod{m},$$

根据定理 5.1.1,

$$\operatorname{ord}_m\left(a^d\right) \mid \frac{\operatorname{ord}_m(a)}{(d, \operatorname{ord}_m(a))}.$$

因此, 有式 (5.9). 证毕.

例 5.1.12 整数 $5^2 \equiv 8 \pmod{17}$ 模 17 的指数为 $\operatorname{ord}_{17}\left(5^2\right) = \dfrac{\operatorname{ord}_{17}(5)}{(2, \operatorname{ord}_{17}(5))} = 8$.

推论 1 设 $m > 1$ 是整数, g 是模 m 的原根. 设 $d \geqslant 0$ 为整数, 则 g^d 是模的原根当且仅当 $(d, \varphi(m)) = 1$.

证 根据定理 5.1.4 式 (5.9), 有

$$\operatorname{ord}_m\left(g^d\right) = \frac{\operatorname{ord}_m(g)}{(d, \operatorname{ord}_m(g))} = \frac{\varphi(m)}{(d, \varphi(m))}.$$

因此, g^d 是模的原根, 即 $\operatorname{ord}_m\left(g^d\right) = \varphi(m)$ 当且仅当 $(d, \varphi(m)) = 1$. 证毕.

推论 2 设 $m > 1$ 是整数, a 是与 m 互素的整数. 设 $k \mid \operatorname{ord}_m(a)$ 为正整数, 则使得

$$\operatorname{ord}_m(a^d) = k, \quad 1 \leqslant d \leqslant \operatorname{ord}_m(a)$$

正整数 d 满足 $\dfrac{\operatorname{ord}_m(a)}{k} \mid d$, 且这样 d 的个数为 $\varphi(k)$.

定理 5.1.5 设 $m>1$ 是整数. 如果模 m 存在一个原根 g, 则模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

证 设 g 是模 m 的一个原根. 根据定理 5.1.2 式 (5.8), $\varphi(m)$ 个整数

$$g^0=1,\ g,\ \cdots,\ g^{\varphi(m)-1}$$

构成模m的一个简化剩余系. 又根据定理 5.1.4之推论, g^d 是模m的原根当且仅当 $(d,\varphi(m))=1$. 因为这样的 d 共有 $\varphi(\varphi(m))$ 个, 所以模 m 有 $\varphi(\varphi(m))$ 个不同的原根. 证毕.

推论 设 $m>1$ 是整数, 且模 m 存在一个原根. 设

$$\varphi(m)=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad \alpha_i>0,\ i=1,\cdots,s,$$

则整数 a, $(a,m)=1$ 是模 m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}=\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right). \tag{5.10}$$

定理 5.1.6 设 $m>1$ 是整数, a, b 都是与 m 互素的整数. 如果 $(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$, 则

$$\mathrm{ord}_m(a\cdot b)=\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b). \tag{5.11}$$

反之亦然.

定理 5.1.7 设 m, n 都是大于 1 的整数, a 是与 m 互素的整数, 则

(i) 若 $n\mid m$, 则 $\mathrm{ord}_n(a)\mid\mathrm{ord}_m(a)$.

(ii) 若 $(m,n)=1$, 则

$$\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)].$$

推论 1 设 p, q 是两个不同的奇素数, a 是与 $p\cdot q$ 互素的整数, 则

$$\mathrm{ord}_{p\cdot q}(a)=[\mathrm{ord}_p(a),\mathrm{ord}_q(a)]\mid[p-1,q-1].$$

推论 2 设 p, $q=2p-1$ 是两个不同的奇素数, a 是与 $p\cdot q$ 互素的整数, 则

$$\mathrm{ord}_{p\cdot q}(a)=[\mathrm{ord}_p(a),\mathrm{ord}_q(a)]\mid q-1.$$

定理 5.2.3 模 m 的原根存在的充要条件是 $m=2$, 4, p^α, $2p^\alpha$, 其中 p 是奇素数.