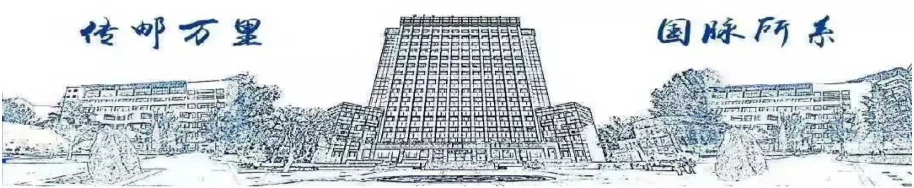
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

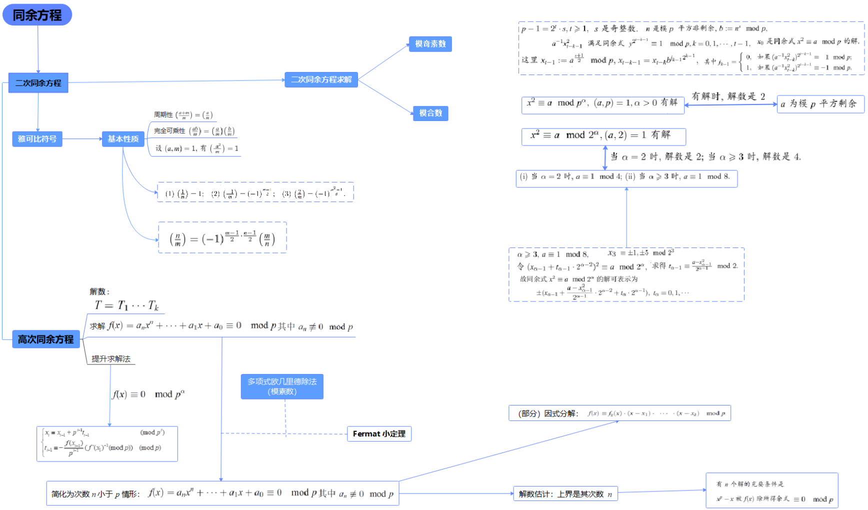
—— 阶与原根

信数课题组

北京邮电大学



上次课回顾



同余方程
二次同余方程
二次同余方程求解
模奇素数
模合数
雅可比符号
基本性质
周期性 $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$
完全可乘性 $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$
设 $(a,m)=1$，有 $\left(\frac{a^2}{m}\right)=1$
(1) $\left(\frac{1}{m}\right)=1$; (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$; (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.
$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$
$p-1=2^t\cdot s, t\geqslant 1$, s 是奇整数. n 是模 p 平方非剩余, $b:=n^s \mod p$,
$a^{-1}x_{t-k-1}^2$ 满足同余式 $y^{2^{t-k-1}}\equiv 1 \mod p, k=0,1,\cdots,t-1$, x_0 是同余式 $x^2\equiv a \mod p$ 的解,
这里 $x_{t-1}:=a^{\frac{s+1}{2}} \mod p$, $x_{t-k-1}=x_{t-k}b^{j_{k-1}2^{k-1}}$, 其中 $j_{k-1}=\begin{cases}0, & 如果 (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv 1 \mod p;\\ 1, & 如果 (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv -1 \mod p.\end{cases}$
$x^2\equiv a \mod p^\alpha$, $(a,p)=1,\alpha>0$ 有解
有解时，解数是 2
a 为模 p 平方剩余
$x^2\equiv a \mod 2^\alpha, (a,2)=1$ 有解
当 $\alpha=2$ 时，解数是 2; 当 $\alpha\geqslant 3$ 时，解数是 4.
(i) 当 $\alpha=2$ 时, $a\equiv 1 \mod 4$; (ii) 当 $\alpha\geqslant 3$ 时, $a\equiv 1 \mod 8$.
$\alpha\geqslant 3$, $a\equiv 1 \mod 8$, $x_3\equiv \pm 1,\pm 5 \mod 2^3$
令 $(x_{\alpha-1}+t_{\alpha-1}\cdot 2^{\alpha-2})^2\equiv a \mod 2^\alpha$, 求得 $t_{\alpha-1}\equiv\frac{a-x_{\alpha-1}^2}{2^{\alpha-1}} \mod 2$.
故同余式 $x^2\equiv a \mod 2^\alpha$ 的解可表示为
$\pm(x_{\alpha-1}+\frac{a-x_{\alpha-1}^2}{2^{\alpha-1}}\cdot 2^{\alpha-2}+t_\alpha\cdot 2^{\alpha-1})$, $t_\alpha=0,1,\cdots$
解数：
$T=T_1\cdots T_k$
求解 $f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \mod p$ 其中 $a_n\not\equiv 0 \mod p$
高次同余方程
提升求解法
$f(x)\equiv 0 \mod p^\alpha$
$\begin{cases}x_i\equiv x_{i-1}+p^{i-1}t_{i-1} & (\mathrm{mod}\ p^i)\\ t_{i-1}\equiv -\frac{f(x_{i-1})}{p^{i-1}}(f'(x_1)^{-1}(\mathrm{mod}\ p)) & (\mathrm{mod}\ p)\end{cases}$
多项式欧几里德除法
(模素数)
Fermat 小定理
(部分) 因式分解: $f(x)\equiv f_k(x)\cdot(x-x_1)\cdot\cdots\cdot(x-x_k) \mod p$
简化为次数 n 小于 p 情形: $f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \mod p$ 其中 $a_n\not\equiv 0 \mod p$
解数估计：上界是其次数 n
有 n 个解的充要条件是
x^p-x 被 $f(x)$ 除所得余式 $\equiv 0 \mod p$

目录

目录

定义 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的正整数, 则使得

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

成立的最小正整数 e 叫做 a 对模 m 的**阶** (**或指数**), 记作 $\mathrm{ord}_m(a)$. 如果 a 对模 m 的阶是 $\varphi(m)$, 则 a 叫做模 m 的**原根**.

定义 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的正整数, 则使得

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

成立的最小正整数 e 叫做 a 对模 m 的**阶** (或**指数**), 记作 $\mathrm{ord}_m(a)$. 如果 a 对模 m 的阶是 $\varphi(m)$, 则 a 叫做模 m 的**原根**.

例 4.1.1　设整数 $m = 7$, 这时 $\varphi(7) = 6$. 我们有

$1^1 \equiv 1 \mod 7$, $2^3 = 8 \equiv 1 \mod 7$, $3^3 = 27 \equiv -1 \mod 7$,
$4^3 \equiv (-3)^3 \equiv 1 \mod 7$, $5^3 \equiv (-2)^3 \equiv -1 \mod 7$, $6^2 \equiv (-1)^2 \equiv 1 \mod 7$.

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 4.1.2 设整数 $m = 14 = 2 \cdot 7$, 这时 $\varphi(14) = 6$. 我们有

$$1^1 \equiv 1 \mod 14, \quad 3^3 = 27 \equiv -1 \mod 14, \quad 5^3 = 125 \equiv -1 \mod 14,$$
$$9^3 \equiv 1 \mod 14, \quad 11^3 \equiv 1 \mod 14, \quad 13^2 \equiv 1 \mod 14.$$

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.

例 4.1.2 设整数 $m = 14 = 2 \cdot 7$, 这时 $\varphi(14) = 6$. 我们有

$$1^1 \equiv 1 \mod 14, \quad 3^3 = 27 \equiv -1 \mod 14, \quad 5^3 = 125 \equiv -1 \mod 14,$$
$$9^3 \equiv 1 \mod 14, \quad 11^3 \equiv 1 \mod 14, \quad 13^2 \equiv 1 \mod 14.$$

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.

例 4.1.3 设整数 $m = 21 = 3 \cdot 7$, 这时 $\varphi(21) = 12$. 我们有

$$1^1 \equiv 1, \quad 2^6 = 64 \equiv 1, \quad 4^3 = 64 \equiv 1,$$
$$5^6 = 15625 \equiv 1, \quad 8^2 \equiv 1, \quad 10^6 = (2 \cdot 5)^6 \equiv 1,$$
$$11^6 \equiv (-10)^6 \equiv 1, \quad 13^2 \equiv (-8)^2 \equiv 1, \quad 16^6 \equiv (-5)^6 \equiv 1,$$
$$17^6 \equiv (-4)^6 \equiv 1, \quad 19^6 \equiv (-2)^2 \equiv 1, \quad 20^2 \equiv (-1)^2 \equiv 1 \mod 21.$$

列成表为：

a	1	2	4	5	8	10	11	13	16	17	19	20
$\mathrm{ord}_m(a)$	1	6	3	6	2	6	6	2	6	6	6	2

因此, 没有模 21 的原根.

列成表为：

a	1	2	4	5	8	10	11	13	16	17	19	20
$\mathrm{ord}_m(a)$	1	6	3	6	2	6	6	2	6	6	6	2

因此, 没有模 21 的原根.

例 4.1.4 设整数 $m = 9 = 3^2$, 这时 $\varphi(9) = 6$. 我们有

$$1^1 \equiv 1 \mod 9, \quad 2^3 = 8 \equiv -1 \mod 9, \quad 4^3 = 64 \equiv 1 \mod 9,$$
$$5^3 \equiv (-4)^3 \equiv -1 \mod 9, \quad 7^3 \equiv 1 \mod 9, \quad 8^2 \equiv 1 \mod 9.$$

列成表为：

a	1	2	4	5	7	8
$\mathrm{ord}_m(a)$	1	6	3	6	3	2

因此, 2, 5 是模 9 的原根.

例 4.1.5 设整数 $m = 8 = 2^3$, 这时 $\varphi(8) = 4$. 我们有

$$1^1 \equiv 1 \mod 8, \qquad 3^2 = 9 \equiv 1 \mod 8,$$
$$5^2 = 25 \equiv 1 \mod 8, \quad 7^2 \equiv (-1)^2 \equiv 1 \mod 8.$$

列成表为:

a	1	3	5	7
$\mathrm{ord}_m(a)$	1	2	2	2

因此, 没有模 8 的原根.

例 4.1.5 设整数 $m = 8 = 2^3$, 这时 $\varphi(8) = 4$. 我们有

$$1^1 \equiv 1 \mod 8, \qquad 3^2 = 9 \equiv 1 \mod 8,$$
$$5^2 = 25 \equiv 1 \mod 8, \quad 7^2 \equiv (-1)^2 \equiv 1 \mod 8.$$

列成表为:

a	1	3	5	7
$\mathrm{ord}_m(a)$	1	2	2	2

因此, 没有模 8 的原根.

目录

定理 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的整数, 则整数 d 使得

$$a^d \equiv 1 \mod m$$

的充要条件是

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

定理 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的整数, 则整数 d 使得

$$a^d \equiv 1 \mod m$$

的充要条件是

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

证：充分性. 设 $\mathrm{ord}_m(a) \mid d$, 那么存在整数 k 使得 $d = k \cdot \mathrm{ord}_m(a)$. 因此, 我们有 $a^d = \left(a^{\mathrm{ord}_m(a)}\right)^k \equiv 1 \mod m$.

定理 4.1.1

设 $m>1$ 是整数，a 是与 m 互素的整数，则整数 d 使得

$$a^d \equiv 1 \mod m$$

的充要条件是

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

证：充分性. 设 $\mathrm{ord}_m(a) \mid d$, 那么存在整数 k 使得 $d = k \cdot \mathrm{ord}_m(a)$. 因此，我们有 $a^d = \left(a^{\mathrm{ord}_m(a)}\right)^k \equiv 1 \mod m$.

必要性. 如果 $\mathrm{ord}_m(a) \mid d$ 不成立，则由定理 1.1.11 (欧几里德除法)，存在整数 q, r 使得 $d = q \cdot \mathrm{ord}_m(a) + r,\ 0 < r < \mathrm{ord}_m(a)$.

从而，$a^r \equiv \left(a^{\mathrm{ord}_m(a)}\right)^q \cdot a^r = a^d \equiv 1 \mod m$.

这与 $\mathrm{ord}_m(a)$ 的最小性矛盾.

故 $\mathrm{ord}_m(a) \mid d$.

推论 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的整数, 则 $\mathrm{ord}_m(a) \mid \varphi(m)$.

证：根据定理 2.2.13（欧拉定理），我们有 $a^{\varphi(m)} \equiv 1 \mod m$.

由定理 4.1.1, 我们有 $\mathrm{ord}_m(a) \mid \varphi(m)$.

推论 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的整数, 则 $\mathrm{ord}_m(a) \mid \varphi(m)$.

证：根据定理 2.2.13（欧拉定理），我们有 $a^{\varphi(m)} \equiv 1 \mod m$.

由定理 4.1.1, 我们有 $\mathrm{ord}_m(a) \mid \varphi(m)$.

注：根据推论 4.1.1, 整数 a 模 m 的阶 $\mathrm{ord}_m(a)$ 是 $\varphi(m)$ 的因数, 所以我们可以在 $\varphi(m)$ 的因数中求 $\mathrm{ord}_m(a)$.

推论 4.1.1

设 $m > 1$ 是整数, a 是与 m 互素的整数, 则 $\mathrm{ord}_m(a) \mid \varphi(m)$.

证：根据定理 2.2.13（欧拉定理）, 我们有 $a^{\varphi(m)} \equiv 1 \mod m$.

由定理 4.1.1, 我们有 $\mathrm{ord}_m(a) \mid \varphi(m)$.

注：根据推论 4.1.1, 整数 a 模 m 的阶 $\mathrm{ord}_m(a)$ 是 $\varphi(m)$ 的因数, 所以我们可以在 $\varphi(m)$ 的因数中求 $\mathrm{ord}_m(a)$.

例 5.1.6 求整数 2 模 13 的阶 $\mathrm{ord}_{13}(2)$.

推论 4.1.1

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $\mathrm{ord}_m(a) \mid \varphi(m)$.

证：根据定理 2.2.13（欧拉定理），我们有 $a^{\varphi(m)} \equiv 1 \mod m$.

由定理 4.1.1, 我们有 $\mathrm{ord}_m(a) \mid \varphi(m)$.

注：根据推论 4.1.1, 整数 a 模 m 的阶 $\mathrm{ord}_m(a)$ 是 $\varphi(m)$ 的因数, 所以我们可以在 $\varphi(m)$ 的因数中求 $\mathrm{ord}_m(a)$.

例 5.1.6 求整数 2 模 13 的阶 $\mathrm{ord}_{13}(2)$.

解：因为 $\varphi(13)=12$, 所以只需要对 12 的因数 $d=1,2,3,4,6,12$, 计算 $2^d \mod m$.

因为 $2^1 \equiv 2 \mod 13$, $2^2 \equiv 4 \mod 13$, $2^3 \equiv 8 \mod 13$, $2^4 \equiv 16 \equiv 3 \mod 13$, $2^6 \equiv 64 \equiv -1 \mod 13$, $2^{12} \equiv (-1)^2 \equiv 1 \mod 13$,

所以 $\mathrm{ord}_{13}(2)=12$. 这说明 2 是模 13 的原根.

推论 4.1.2

设 p 是奇素数，且 $\frac{p-1}{2}$ 也是素数. 如果 a 是一个不被 p 整除的整数，且也不是模 p 的二次单位根，则 $\mathrm{ord}_p(a) = \frac{p-1}{2}$ 或 $p-1$.

推论 4.1.2

设 p 是奇素数，且 $\frac{p-1}{2}$ 也是素数．如果 a 是一个不被 p 整除的整数，且也不是模 p 的二次单位根，则 $\mathrm{ord}_p(a) = \frac{p-1}{2}$ 或 $p-1$.

证：根据定理 2.2.13 (欧拉定理), 有 $a^{\varphi(p)} \equiv 1 \mod p$.

根据推论 4.1.1, 整数 a 模 p 的阶 $\mathrm{ord}_p(a)$ 是 $\varphi(p) = p-1 = 2 \cdot \frac{p-1}{2}$ 的因数.

但 a 不是模 p 的二次单位根, 即 $\mathrm{ord}_p(a) \neq 2$,

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

推论 4.1.2

设 p 是奇素数，且 $\frac{p-1}{2}$ 也是素数. 如果 a 是一个不被 p 整除的整数，且也不是模 p 的二次单位根，则 $\mathrm{ord}_p(a) = \frac{p-1}{2}$ 或 $p-1$.

证：根据定理 2.2.13 (欧拉定理)，有 $a^{\varphi(p)} \equiv 1 \mod p$.

根据推论 4.1.1，整数 a 模 p 的阶 $\mathrm{ord}_p(a)$ 是 $\varphi(p) = p-1 = 2\cdot\frac{p-1}{2}$ 的因数.

但 a 不是模 p 的二次单位根，即 $\mathrm{ord}_p(a) \neq 2$,

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

推论 4.1.3

设 $m > 1$ 是整数，a 是与 m 互素的整数.

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

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

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.
因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

(ii) 因为 $(a^{-1})^{\mathrm{ord}_m(a)} \equiv \left(a^{\mathrm{ord}_m(a)}\right)^{-1} \equiv 1 \mod m$,

因此, 我们有 $\mathrm{ord}_m(a^{-1}) \mid \mathrm{ord}_m(a)$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

(ii) 因为 $(a^{-1})^{\mathrm{ord}_m(a)} \equiv \left(a^{\mathrm{ord}_m(a)}\right)^{-1} \equiv 1 \mod m$,

因此, 我们有 $\mathrm{ord}_m(a^{-1}) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a^{-1})$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

(ii) 因为 $(a^{-1})^{\mathrm{ord}_m(a)} \equiv \left(a^{\mathrm{ord}_m(a)}\right)^{-1} \equiv 1 \mod m$,

因此, 我们有 $\mathrm{ord}_m(a^{-1}) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a^{-1})$.

故 $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

证：(i) 若 $b \equiv a \mod m$, 则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 我们有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

(ii) 因为 $(a^{-1})^{\mathrm{ord}_m(a)} \equiv \left(a^{\mathrm{ord}_m(a)}\right)^{-1} \equiv 1 \mod m$,

因此, 我们有 $\mathrm{ord}_m(a^{-1}) \mid \mathrm{ord}_m(a)$.

同理, 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a^{-1})$.

故 $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

例 4.1.7 整数 28 模 13 的阶为 $\mathrm{ord}_{13}(28) = \mathrm{ord}_{13}(2) = 12$.

整数 7 模 13 的阶为 12, 因为 $2^{-1} \equiv 7 \mod 13$ (由例 4.1.6 可知).

定理 4.1.2

设 $m>1$ 是整数, a 是与 m 互素的整数, 则

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

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

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

组成模 m 的简化剩余系.

定理 4.1.2

设 $m>1$ 是整数, a 是与 m 互素的整数, 则

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

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

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

组成模 m 的简化剩余系.

证：反证法. 若存在整数 $0\leqslant k, l<\mathrm{ord}_m(a)$ 使得 $a^k\equiv a^l \mod m$.

不妨设 $k>l$, 由于 $(a,m)=1$, 得到 $a^{k-l}\equiv 1 \mod m$.

但 $0<k-l<\mathrm{ord}_m(a)$, 这与 $\mathrm{ord}_m(a)$ 的最小性矛盾.

因此, 结论成立.

定理 4.1.2

设 $m>1$ 是整数, a 是与 m 互素的整数, 则

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

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

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

组成模 m 的简化剩余系.

证：反证法. 若存在整数 $0\leqslant k, l<\mathrm{ord}_m(a)$ 使得 $a^k\equiv a^l \mod m$.

不妨设 $k>l$, 由于 $(a,m)=1$, 得到 $a^{k-l}\equiv 1 \mod m$.

但 $0<k-l<\mathrm{ord}_m(a)$, 这与 $\mathrm{ord}_m(a)$ 的最小性矛盾.

因此, 结论成立.

再设 a 是模 m 的原根, 即 $\mathrm{ord}_m(a)=\varphi(m)$,

则我们有 $\varphi(m)$ 个数 $1=a^0, a, \cdots, a^{\varphi(m)-1}$ 模 m 两两不同余.

根据定理 2.2.7, 这 $\varphi(m)$ 个数组成模 m 的简化剩余系.

例 4.1.8 整数 $\{2^k \mid k = 0, \cdots, 11\}$ 组成模 13 的简化剩余系.

例 4.1.8 整数 $\{2^k \mid k = 0, \cdots, 11\}$ 组成模 13 的简化剩余系.

解：作计算如下：

$$
\begin{aligned}
2^0 &\equiv 1 \pmod{13}, & 2^1 &\equiv 2 \pmod{13},\\
2^2 &\equiv 4 \pmod{13}, & 2^3 &\equiv 8 \pmod{13},\\
2^4 &= 16 \equiv 3 \pmod{13}, & 2^5 &\equiv 3 \cdot 2 \equiv 6 \pmod{13},\\
2^6 &\equiv 6 \cdot 2 \equiv 12 \pmod{13}, & 2^7 &\equiv 12 \cdot 2 \equiv 11 \pmod{13},\\
2^8 &\equiv 11 \cdot 2 \equiv 9 \pmod{13}, & 2^9 &\equiv 9 \cdot 2 \equiv 5 \pmod{13},\\
2^{10} &\equiv 5 \cdot 2 \equiv 10 \pmod{13}, & 2^{11} &\equiv 10 \cdot 2 \equiv 7 \pmod{13}.
\end{aligned}
$$

列表为

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	3	6	12	11	9	5	10	7

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \mathrm{ord}_m(a)$.

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \operatorname{ord}_m(a)$.

证：根据定理 1.1.11（欧几里德除法）, 存在整数 q, r 和 q', r' 使得

$$d = q \cdot \operatorname{ord}_m(a) + r,\ 0 \leqslant r < \operatorname{ord}_m(a),$$

$$k = q' \cdot \operatorname{ord}_m(a) + r',\ 0 \leqslant r' < \operatorname{ord}_m(a).$$

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

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

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \mathrm{ord}_m(a)$.

证：根据定理 1.1.11（欧几里德除法）, 存在整数 q, r 和 q', r' 使得

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

$$k = q' \cdot \mathrm{ord}_m(a) + r',\ 0 \leqslant r' < \mathrm{ord}_m(a).$$

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

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

必要性. 若 $a^d \equiv a^k \mod m$, 则 $a^r \equiv a^{r'} \mod m$. 由定理 4.1.2, 得到 $r = r'$. 故 $d \equiv k \mod \mathrm{ord}_m(a)$.

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \mathrm{ord}_m(a)$.

证：根据定理 1.1.11（欧几里德除法）, 存在整数 q, r 和 q', r' 使得

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

$$k = q' \cdot \mathrm{ord}_m(a) + r',\ 0 \leqslant r' < \mathrm{ord}_m(a).$$

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

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

必要性. 若 $a^d \equiv a^k \mod m$, 则 $a^r \equiv a^{r'} \mod m$. 由定理 4.1.2, 得到 $r = r'$. 故 $d \equiv k \mod \mathrm{ord}_m(a)$.

充分性. 若 $d \equiv k \mod \mathrm{ord}_m(a)$, 则 $r = r'$. 因此, $a^d \equiv a^k \mod m$.

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \mathrm{ord}_m(a)$.

证：根据定理 1.1.11（欧几里德除法），存在整数 q, r 和 q', r' 使得

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

$$k = q' \cdot \mathrm{ord}_m(a) + r',\ 0 \leqslant r' < \mathrm{ord}_m(a).$$

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

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

必要性. 若 $a^d \equiv a^k \mod m$, 则 $a^r \equiv a^{r'} \mod m$. 由定理 4.1.2, 得到 $r = r'$. 故 $d \equiv k \mod \mathrm{ord}_m(a)$.

充分性. 若 $d \equiv k \mod \mathrm{ord}_m(a)$, 则 $r = r'$. 因此, $a^d \equiv a^k \mod m$.

例 4.1.9 $\quad 2^{2024} \equiv 2^2 \equiv 4 \mod 7.$

因为整数 2 模 7 的阶为 $\mathrm{ord}_7(2) = 3$, $\quad 2024 \equiv 2 \mod 3$.

定理 4.1.3

设 $m>1$ 是整数, a 是与 m 互素的整数, 则 $a^d \equiv a^k \mod m$ 的充要条件是 $d \equiv k \mod \mathrm{ord}_m(a)$.

证：根据定理 1.1.11（欧几里德除法），存在整数 q, r 和 q', r' 使得

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

$$k = q' \cdot \mathrm{ord}_m(a) + r',\ 0 \leqslant r' < \mathrm{ord}_m(a).$$

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

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

必要性. 若 $a^d \equiv a^k \mod m$, 则 $a^r \equiv a^{r'} \mod m$. 由定理 4.1.2, 得到 $r = r'$. 故 $d \equiv k \mod \mathrm{ord}_m(a)$.

充分性. 若 $d \equiv k \mod \mathrm{ord}_m(a)$, 则 $r = r'$. 因此, $a^d \equiv a^k \mod m$.

例 4.1.9 $\quad 2^{2024} \equiv 2^2 \equiv 4 \mod 7.$

因为整数 2 模 7 的阶为 $\mathrm{ord}_7(2) = 3$, $\ 2024 \equiv 2 \mod 3$.

定理 4.1.4

设 $m>1$ 是整数, a 是与 m 互素的整数, d 为非负整数, 则

$$\mathrm{ord}_m(a^d)=\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}.$$

定理 4.1.4

设 $m>1$ 是整数, a 是与 m 互素的整数, d 为非负整数, 则

$$\mathrm{ord}_m(a^d)=\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}.$$

证：因为 $a^{d\cdot\mathrm{ord}_m(a)}=(a^d)^{\mathrm{ord}_m(a^d)}\equiv 1 \mod m$,

根据定理 4.1.1, $\mathrm{ord}_m(a)\mid d\cdot\mathrm{ord}_m(a^d)$.

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

因为 $\left(\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))},\frac{d}{(d,\mathrm{ord}_m(a))}\right)=1$,

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

定理 4.1.4

设 $m>1$ 是整数, a 是与 m 互素的整数, d 为非负整数, 则

$$\mathrm{ord}_m(a^d)=\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}.$$

证: 因为 $a^{d\cdot\mathrm{ord}_m(a)}=(a^d)^{\mathrm{ord}_m(a^d)}\equiv 1 \mod m$,

根据定理 4.1.1, $\mathrm{ord}_m(a)\mid d\cdot\mathrm{ord}_m(a^d)$.

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

因为 $\left(\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))},\frac{d}{(d,\mathrm{ord}_m(a))}\right)=1$,

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

另一方面, 我们有 $(a^d)^{\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}}=\left(a^{\mathrm{ord}_m(a)}\right)^{\frac{d}{(d,\mathrm{ord}_m(a))}}\equiv 1 \mod m$.

根据定理 4.1.1, $\mathrm{ord}_m(a^d)\mid\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}$.

定理 4.1.4

设 $m>1$ 是整数, a 是与 m 互素的整数, d 为非负整数, 则

$$\mathrm{ord}_m(a^d)=\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}.$$

证：因为 $a^{d\cdot\mathrm{ord}_m(a)}=(a^d)^{\mathrm{ord}_m(a^d)}\equiv 1 \mod m$,

根据定理 4.1.1, $\mathrm{ord}_m(a)\mid d\cdot\mathrm{ord}_m(a^d)$.

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

因为 $\left(\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))},\frac{d}{(d,\mathrm{ord}_m(a))}\right)=1$,

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

另一方面, 我们有 $(a^d)^{\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}}=\left(a^{\mathrm{ord}_m(a)}\right)^{\frac{d}{(d,\mathrm{ord}_m(a))}}\equiv 1 \mod m$.

根据定理 4.1.1, $\mathrm{ord}_m(a^d)\mid\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}$.

因此, $\mathrm{ord}_m(a^d)=\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}$.

例 4.1.10 整数 $2^4 \equiv 3 \mod 13$ 的阶为

$$\mathrm{ord}_{13}(2^4) = \frac{\mathrm{ord}_{13}(2)}{(4, \mathrm{ord}_{13}(2))} = \frac{12}{(12, 4)} = 3.$$

例 4.1.10 整数 $2^4 \equiv 3 \mod 13$ 的阶为

$$\mathrm{ord}_{13}(2^4) = \frac{\mathrm{ord}_{13}(2)}{(4, \mathrm{ord}_{13}(2))} = \frac{12}{(12,4)} = 3.$$

推论 4.1.4

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 m 的原根当且仅当 $(d, \varphi(m)) = 1$.

例 4.1.10 整数 $2^4 \equiv 3 \mod 13$ 的阶为

$$\mathrm{ord}_{13}(2^4) = \frac{\mathrm{ord}_{13}(2)}{(4, \mathrm{ord}_{13}(2))} = \frac{12}{(12, 4)} = 3.$$

推论 4.1.4

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 m 的原根当且仅当 $(d, \varphi(m)) = 1$.

证: 根据定理 4.1.4, 我们有

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

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

例 4.1.10 整数 $2^4 \equiv 3 \mod 13$ 的阶为

$$\operatorname{ord}_{13}(2^4) = \frac{\operatorname{ord}_{13}(2)}{(4, \operatorname{ord}_{13}(2))} = \frac{12}{(12, 4)} = 3.$$

推论 4.1.4

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 m 的原根当且仅当 $(d, \varphi(m)) = 1$.

证: 根据定理 4.1.4, 我们有

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

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

定理 4.1.5

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

定理 4.1.5

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

证：设 g 是模 m 的一个原根.
由定理 4.1.2, $\varphi(m)$ 个整数 $g, g^2, \cdots, g^{\varphi(m)}$ 构成模 m 的一个简化剩余系.
又根据推论 4.1.4, g^d 是模 m 的原根当且仅当 $(d, \varphi(m)) = 1$,
那么这样的 d 共有 $\varphi(\varphi(m))$ 个, 所以模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

定理 4.1.5

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

证：设 g 是模 m 的一个原根.
由定理 4.1.2, $\varphi(m)$ 个整数 $g, g^2, \cdots, g^{\varphi(m)}$ 构成模 m 的一个简化剩余系.
又根据推论 4.1.4, g^d 是模 m 的原根当且仅当 $(d, \varphi(m))=1$,
那么这样的 d 共有 $\varphi(\varphi(m))$ 个, 所以模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

推论 4.1.5

设 $m>1$ 是整数, 且模 m 存在一个原根. 设

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

则整数 a, $(a,m)=1$ 是模 m 原根的概率是

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

证: 根据定理 4.1.5, 整数 a, $(a,m)=1$ 是模 m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}.$$

又根据欧拉函数 $\varphi(m)$ 的性质以及 $\varphi(m)$ 的素因数分解表达式, 我们有

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

因此, 结论成立.

证: 根据定理 4.1.5, 整数 a, $(a,m)=1$ 是模 m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}.$$

又根据欧拉函数 $\varphi(m)$ 的性质以及 $\varphi(m)$ 的素因数分解表达式, 我们有

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

因此, 结论成立.

例 4.1.10　求出模 13 的所有原根.

证: 根据定理 4.1.5, 整数 a, $(a,m)=1$ 是模 m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}.$$

又根据欧拉函数 $\varphi(m)$ 的性质以及 $\varphi(m)$ 的素因数分解表达式, 我们有

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

因此, 结论成立.

例 4.1.10　求出模 13 的所有原根.

解: 由例 4.1.6 知, 2 是模 13 的原根. 再根据定理 4.1.5, 得到 $\varphi(\varphi(13))=\varphi(12)=4$ 个整数

$$2,\ 2^5\equiv 6,\ 2^7\equiv 11,\ 2^{11}\equiv 7 \pmod{13}$$

是模 13 的全部原根.

定理 4.1.6

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

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

反之亦然.

定理 4.1.6

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

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

反之亦然.

证：因为 $(a,m)=1$, $(b,m)=1$, 所以 $(a\cdot b,m)=1$, 且存在 $\mathrm{ord}_m(a\cdot b)$.

定理 4.1.6

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

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

反之亦然.

证：因为 $(a,m)=1$, $(b,m)=1$, 所以 $(a\cdot b,m)=1$, 且存在 $\mathrm{ord}_m(a\cdot b)$.

又因为

$$\begin{aligned}a^{\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)} &\equiv \left(a^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\\ &\equiv \left((ab)^{\mathrm{ord}_m(a\cdot b)}\right)^{\mathrm{ord}_m(b)}\\ &\equiv 1 \mod m,\end{aligned}$$

定理 4.1.6

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

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

反之亦然.

证：因为 $(a,m)=1$, $(b,m)=1$, 所以 $(a\cdot b,m)=1$, 且存在 $\mathrm{ord}_m(a\cdot b)$.

又因为

$$\begin{aligned} a^{\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)} &\equiv \left(a^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)} \\ &\equiv \left((ab)^{\mathrm{ord}_m(a\cdot b)}\right)^{\mathrm{ord}_m(b)} \\ &\equiv 1 \mod m, \end{aligned}$$

因此, $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)$.

定理 4.1.6

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

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

反之亦然.

证：因为 $(a,m)=1$, $(b,m)=1$, 所以 $(a\cdot b,m)=1$, 且存在 $\mathrm{ord}_m(a\cdot b)$.

又因为

$$\begin{aligned} a^{\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)} &\equiv \left(a^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)} \\ &\equiv \left((ab)^{\mathrm{ord}_m(a\cdot b)}\right)^{\mathrm{ord}_m(b)} \\ &\equiv 1 \mod m, \end{aligned}$$

因此, $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)$.

但 $(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$, 则有 $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(a\cdot b)$.

定理 4.1.6

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

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

反之亦然.

证：因为 $(a, m)=1$, $(b, m)=1$, 所以 $(a\cdot b, m)=1$, 且存在 $\mathrm{ord}_m(a\cdot b)$.

又因为

$$\begin{aligned} a^{\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)} &\equiv \left(a^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)} \\ &\equiv \left((ab)^{\mathrm{ord}_m(a\cdot b)}\right)^{\mathrm{ord}_m(b)} \\ &\equiv 1 \mod m, \end{aligned}$$

因此, $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)$.

但 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b))=1$, 则有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a\cdot b)$.

同理, $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a\cdot b)$.

再由 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$ 得到, $\text{ord}_m(a) \cdot \text{ord}_m(b) \mid \text{ord}_m(a \cdot b)$.

再由 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$ 得到, $\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid \mathrm{ord}_m(a \cdot b)$.
另一方面, 我们有

$$(ab)^{\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)} = \left(a^{\mathrm{ord}_m(a)}\right)^{\mathrm{ord}_m(b)} \cdot \left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a)} \equiv 1 \mod m,$$

从而, $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

再由 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$ 得到, $\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid \mathrm{ord}_m(a \cdot b)$.

另一方面, 我们有

$$(ab)^{\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)} = \left(a^{\mathrm{ord}_m(a)}\right)^{\mathrm{ord}_m(b)} \cdot \left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a)} \equiv 1 \mod m,$$

从而, $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

再由 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$ 得到, $\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid \mathrm{ord}_m(a \cdot b)$.
另一方面, 我们有

$(ab)^{\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)} = \left(a^{\mathrm{ord}_m(a)}\right)^{\mathrm{ord}_m(b)} \cdot \left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a)} \equiv 1 \mod m$,

从而, $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.
故 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.
反过来, 如果 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$, 那么由

$(ab)^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} = a^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} \cdot b^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} \equiv 1 \mod m$

推得,

$$\mathrm{ord}_m(ab) \mid [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)],$$

即

$$\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

再由 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$ 得到, $\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid \mathrm{ord}_m(a \cdot b)$.

另一方面, 我们有

$$(ab)^{\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)} = \left(a^{\mathrm{ord}_m(a)}\right)^{\mathrm{ord}_m(b)} \cdot \left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a)} \equiv 1 \mod m,$$

从而, $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

故 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

反过来, 如果 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$, 那么由

$$(ab)^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} = a^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} \cdot b^{[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]} \equiv 1 \mod m$$

推得,

$$\mathrm{ord}_m(ab) \mid [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)],$$

即

$$\mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \mid [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

因此, $(\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)) = 1$.

结论成立.

注：对于模 m, 不一定有

$$\mathrm{ord}_m(a \cdot b) = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

注：对于模 m, 不一定有

$$\mathrm{ord}_m(a \cdot b) = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

例如,

$$\mathrm{ord}_{14}(3 \cdot 3) = 3 \neq [\mathrm{ord}_{14}(3),\ \mathrm{ord}_{14}(3)] = 6,$$
$$\mathrm{ord}_{14}(3 \cdot 5) = 1 \neq [\mathrm{ord}_{14}(3),\ \mathrm{ord}_{14}(5)] = 6.$$

但有

$$\mathrm{ord}_{14}(11 \cdot 13) = \mathrm{ord}_{14}(3) = 6 = [\mathrm{ord}_{14}(11),\ \mathrm{ord}_{14}(13)] = [3, 2] = 6.$$

例 4.1.12 求模 23 的原根.

注：对于模 m, 不一定有

$$\mathrm{ord}_m(a \cdot b) = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

例如,

$$\mathrm{ord}_{14}(3 \cdot 3) = 3 \neq [\mathrm{ord}_{14}(3),\ \mathrm{ord}_{14}(3)] = 6,$$
$$\mathrm{ord}_{14}(3 \cdot 5) = 1 \neq [\mathrm{ord}_{14}(3),\ \mathrm{ord}_{14}(5)] = 6.$$

但有

$$\mathrm{ord}_{14}(11 \cdot 13) = \mathrm{ord}_{14}(3) = 6 = [\mathrm{ord}_{14}(11),\ \mathrm{ord}_{14}(13)] = [3, 2] = 6.$$

例 4.1.12 求模 23 的原根.

解: 计算整数 2 模 23 的阶为 $\mathrm{ord}_{23}(2) = 11$;

因此, 整数 -2 为模 23 的原根,

因为 -2 模 23 的阶为 $\mathrm{ord}_{23}(-2) = \mathrm{ord}_{23}(-1) \cdot \mathrm{ord}_{23}(2) = 22$.

定理 4.1.7

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

定理 4.1.7

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

证： (i) 根据 $\mathrm{ord}_m(a)$ 的定义, 我们有 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 当 $n \mid m$ 时, 可以推出 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod n$.

根据定理 4.1.1, 我们得到 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

定理 4.1.7

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

证： (i) 根据 $\mathrm{ord}_m(a)$ 的定义, 我们有 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 当 $n \mid m$ 时, 可以推出 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod n$.

根据定理 4.1.1, 我们得到 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

(ii) 由 (i) 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a), \mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a)$.

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

定理 4.1.7

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 $\text{ord}_n(a) \mid \text{ord}_m(a)$.

(ii) 若 $(m, n) = 1$, 则 $\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)]$.

证: (i) 根据 $\text{ord}_m(a)$ 的定义, 我们有 $a^{\text{ord}_m(a)} \equiv 1 \mod m$.

因此, 当 $n \mid m$ 时, 可以推出 $a^{\text{ord}_m(a)} \equiv 1 \mod n$.

根据定理 4.1.1, 我们得到 $\text{ord}_n(a) \mid \text{ord}_m(a)$.

(ii) 由 (i) 我们有 $\text{ord}_m(a) \mid \text{ord}_{mn}(a), \text{ord}_n(a) \mid \text{ord}_{mn}(a)$.

从而, $[\text{ord}_m(a), \text{ord}_n(a)] \mid \text{ord}_{mn}(a)$.

又由 $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \mod m$, $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \mod n$ 以及性质 2.1.7 可推出 $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \mod (mn)$.

从而, $\text{ord}_{mn}(a) \mid [\text{ord}_m(a), \text{ord}_n(a)]$.

定理 4.1.7

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

证： (i) 根据 $\mathrm{ord}_m(a)$ 的定义, 我们有 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod m$.

因此, 当 $n \mid m$ 时, 可以推出 $a^{\mathrm{ord}_m(a)} \equiv 1 \mod n$.

根据定理 4.1.1, 我们得到 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

(ii) 由 (i) 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a), \mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a)$.

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

又由 $a^{[\mathrm{ord}_m(a), \mathrm{ord}_n(a)]} \equiv 1 \mod m$, $a^{[\mathrm{ord}_m(a), \mathrm{ord}_n(a)]} \equiv 1 \mod n$ 以及性质 2.1.7 可推出 $a^{[\mathrm{ord}_m(a), \mathrm{ord}_n(a)]} \equiv 1 \mod (mn)$.

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

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

推论 4.1.6

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

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

推论 4.1.6

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

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

推论 4.1.7

设 m 是大于 1 的整数, a 是与 m 互素的整数, 则当 m 的标准分解式为 $m = 2^n \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 时, 我们有

$$\mathrm{ord}_m(a) = [\mathrm{ord}_{2^n}(a), \mathrm{ord}_{p_1^{\alpha_1}}(a), \cdots, \mathrm{ord}_{p_k^{\alpha_k}}(a)].$$

推论 4.1.6

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

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

推论 4.1.7

设 m 是大于 1 的整数, a 是与 m 互素的整数, 则当 m 的标准分解式为 $m=2^n\cdot p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 时, 我们有

$$\mathrm{ord}_m(a)=[\mathrm{ord}_{2^n}(a),\mathrm{ord}_{p_1^{\alpha_1}}(a),\cdots,\mathrm{ord}_{p_k^{\alpha_k}}(a)].$$

定理 4.1.8

设 m,n 都是大于 1 的整数, 且 $(m,n)=1$. 则对与 mn 互素的任意整数 a_1,a_2, 存在整数 a 使得 $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)]$.

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

根据中国剩余定理, 这个同余方程组有唯一解 $x \equiv a \mod (mn)$.

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

根据中国剩余定理, 这个同余方程组有唯一解 $x \equiv a \mod (mn)$.

根据推论 4.1.3, 我们有 $\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1)$, $\mathrm{ord}_n(a) = \mathrm{ord}_n(a_2)$.

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

根据中国剩余定理, 这个同余方程组有唯一解 $x \equiv a \mod (mn)$.

根据推论 4.1.3, 我们有 $\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1)$, $\mathrm{ord}_n(a) = \mathrm{ord}_n(a_2)$.

从定理 4.1.7, 得出 $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)] = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

根据中国剩余定理, 这个同余方程组有唯一解 $x \equiv a \mod (mn)$.
根据推论 4.1.3, 我们有 $\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1)$, $\mathrm{ord}_n(a) = \mathrm{ord}_n(a_2)$.
从定理 4.1.7, 得出 $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)] = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

在定理 4.1.6 的注记中提到, 对于模 m, 不一定有

$$\mathrm{ord}_m(a \cdot b) = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]$$

成立. 但我们有下面的结论成立.

证：考虑同余方程组

$$\begin{cases} x \equiv a_1 \mod m, \\ x \equiv a_2 \mod n. \end{cases}$$

根据中国剩余定理, 这个同余方程组有唯一解 $x \equiv a \mod (mn)$.
根据推论 4.1.3, 我们有 $\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1)$, $\mathrm{ord}_n(a) = \mathrm{ord}_n(a_2)$.
从定理 4.1.7, 得出 $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)] = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

在定理 4.1.6 的注记中提到, 对于模 m, 不一定有

$$\mathrm{ord}_m(a \cdot b) = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)]$$

成立. 但我们有下面的结论成立.

定理 4.1.9

设 $m > 1$ 是整数, 则对与 m 互素的任意整数 a, b, 存在整数 c 使得

$$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

证：对于整数 $\mathrm{ord}_m(a)$ 和 $\mathrm{ord}_m(b)$, 存在整数 u, v 满足

$$u \mid \mathrm{ord}_m(a),\ \ v \mid \mathrm{ord}_m(b),\ \ (u, v) = 1$$

使得

$$[\mathrm{ord}_m(a), \mathrm{ord}_m(b)] = u \cdot v.$$

证：对于整数 $\mathrm{ord}_m(a)$ 和 $\mathrm{ord}_m(b)$, 存在整数 u, v 满足

$$u \mid \mathrm{ord}_m(a),\ \ v \mid \mathrm{ord}_m(b),\ \ (u, v) = 1$$

使得

$$[\mathrm{ord}_m(a), \mathrm{ord}_m(b)] = u \cdot v.$$

现在令

$$s = \frac{\mathrm{ord}_m(a)}{u},\ \ t = \frac{\mathrm{ord}_m(b)}{v},$$

根据定理 4.1.4, 我们有

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(s, \mathrm{ord}_m(a))} = u,\ \ \mathrm{ord}_m(b^t) = v.$$

证：对于整数 $\mathrm{ord}_m(a)$ 和 $\mathrm{ord}_m(b)$，存在整数 u, v 满足

$$u \mid \mathrm{ord}_m(a),\ \ v \mid \mathrm{ord}_m(b),\ \ (u, v) = 1$$

使得

$$[\mathrm{ord}_m(a), \mathrm{ord}_m(b)] = u \cdot v.$$

现在令

$$s = \frac{\mathrm{ord}_m(a)}{u},\ \ t = \frac{\mathrm{ord}_m(b)}{v},$$

根据定理 4.1.4, 我们有

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(s, \mathrm{ord}_m(a))} = u,\ \ \mathrm{ord}_m(b^t) = v.$$

再根据定理 4.1.6, 我们得到

$$\mathrm{ord}_m(a^s \cdot b^t) = \mathrm{ord}_m(a^s)\mathrm{ord}_m(b^t) = u \cdot v = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

证：对于整数 $\mathrm{ord}_m(a)$ 和 $\mathrm{ord}_m(b)$, 存在整数 u, v 满足

$$u \mid \mathrm{ord}_m(a),\ \ v \mid \mathrm{ord}_m(b),\ \ (u, v) = 1$$

使得

$$[\mathrm{ord}_m(a), \mathrm{ord}_m(b)] = u \cdot v.$$

现在令

$$s = \frac{\mathrm{ord}_m(a)}{u},\ \ t = \frac{\mathrm{ord}_m(b)}{v},$$

根据定理 4.1.4, 我们有

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(s, \mathrm{ord}_m(a))} = u,\ \ \mathrm{ord}_m(b^t) = v.$$

再根据定理 4.1.6, 我们得到

$$\mathrm{ord}_m(a^s \cdot b^t) = \mathrm{ord}_m(a^s)\mathrm{ord}_m(b^t) = u \cdot v = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

因此, 取 $c = a^s \cdot b^t \mod m$, 即为所求.

例 4.1.13 设整数 $m=3631$, m 是素数, 有
$\varphi(3631)=3630=2\cdot 3\cdot 5\cdot 11^2$, 以及

$$
\begin{array}{ll}
\mathrm{ord}_{3631}(2)=605=5\cdot 11^2, & \mathrm{ord}_{3631}(3)=1210=2\cdot 5\cdot 11^2, \\
\mathrm{ord}_{3631}(5)=363=3\cdot 11^2, & \mathrm{ord}_{3631}(6)=1210=2\cdot 5\cdot 11^2, \\
\mathrm{ord}_{3631}(7)=33=3\cdot 11, & \mathrm{ord}_{3631}(10)=1815=3\cdot 5\cdot 11^2, \\
\mathrm{ord}_{3631}(11)=330=2\cdot 3\cdot 5\cdot 11, & \mathrm{ord}_{3631}(12)=1210=2\cdot 5\cdot 11^2, \\
\mathrm{ord}_{3631}(13)=1815=3\cdot 5\cdot 11^2, & \mathrm{ord}_{3631}(14)=1815=3\cdot 5\cdot 11^2, \\
\mathrm{ord}_{3631}(15)=3630=2\cdot 3\cdot 5\cdot 11^2, & \mathrm{ord}_{3631}(17)=1210=2\cdot 5\cdot 11^2.
\end{array}
$$

例 4.1.13 设整数 $m=3631$, m 是素数, 有
$\varphi(3631)=3630=2\cdot3\cdot5\cdot11^2$, 以及

$$
\begin{aligned}
&\mathrm{ord}_{3631}(2)=605=5\cdot11^2, &&\mathrm{ord}_{3631}(3)=1210=2\cdot5\cdot11^2,\\
&\mathrm{ord}_{3631}(5)=363=3\cdot11^2, &&\mathrm{ord}_{3631}(6)=1210=2\cdot5\cdot11^2,\\
&\mathrm{ord}_{3631}(7)=33=3\cdot11, &&\mathrm{ord}_{3631}(10)=1815=3\cdot5\cdot11^2,\\
&\mathrm{ord}_{3631}(11)=330=2\cdot3\cdot5\cdot11, &&\mathrm{ord}_{3631}(12)=1210=2\cdot5\cdot11^2,\\
&\mathrm{ord}_{3631}(13)=1815=3\cdot5\cdot11^2, &&\mathrm{ord}_{3631}(14)=1815=3\cdot5\cdot11^2,\\
&\mathrm{ord}_{3631}(15)=3630=2\cdot3\cdot5\cdot11^2, &&\mathrm{ord}_{3631}(17)=1210=2\cdot5\cdot11^2.
\end{aligned}
$$

根据定理 4.1.9, 取整数 $a=3, b=5$ 以及 $u=1230, v=3$, 这时 $s=1, t=11^2$, 而整数 $c=a^s\cdot b^t=3^1\cdot5^{121}\equiv2623 \mod 3631$ 的阶为

$$
\begin{aligned}
\mathrm{ord}_{3631}(2623)&=\mathrm{ord}_{3631}(3^1)\cdot\mathrm{ord}_{3631}(5^{121})=3630\\
&=[\mathrm{ord}_{3631}(3),\mathrm{ord}_{3631}(5)].
\end{aligned}
$$

例 4.1.13 设整数 $m = 3631$, m 是素数, 有 $\varphi(3631) = 3630 = 2\cdot 3\cdot 5\cdot 11^2$, 以及

$$\begin{aligned}
&\mathrm{ord}_{3631}(2) = 605 = 5\cdot 11^2, && \mathrm{ord}_{3631}(3) = 1210 = 2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(5) = 363 = 3\cdot 11^2, && \mathrm{ord}_{3631}(6) = 1210 = 2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(7) = 33 = 3\cdot 11, && \mathrm{ord}_{3631}(10) = 1815 = 3\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(11) = 330 = 2\cdot 3\cdot 5\cdot 11, && \mathrm{ord}_{3631}(12) = 1210 = 2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(13) = 1815 = 3\cdot 5\cdot 11^2, && \mathrm{ord}_{3631}(14) = 1815 = 3\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(15) = 3630 = 2\cdot 3\cdot 5\cdot 11^2, && \mathrm{ord}_{3631}(17) = 1210 = 2\cdot 5\cdot 11^2.
\end{aligned}$$

根据定理 4.1.9, 取整数 $a = 3, b = 5$ 以及 $u = 1230, v = 3$, 这时 $s = 1, t = 11^2$, 而整数 $c = a^s\cdot b^t = 3^1\cdot 5^{121} \equiv 2623 \mod 3631$ 的阶为

$$\begin{aligned}
\mathrm{ord}_{3631}(2623) &= \mathrm{ord}_{3631}(3^1)\cdot \mathrm{ord}_{3631}(5^{121}) = 3630\\
&= [\mathrm{ord}_{3631}(3), \mathrm{ord}_{3631}(5)].
\end{aligned}$$

因此, $c = 2623$ 是模 3631 的原根.

目录

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

证：(方法一：构造性) 在模 p 的简化剩余系 $1,\cdots,p-1$ 中, 记

$$e_r = \mathrm{ord}_p(r),\ 1 \leqslant r \leqslant p-1, \quad e = [e_1,\cdots,e_{p-1}].$$

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

证：(方法一：构造性) 在模 p 的简化剩余系 $1, \cdots, p-1$ 中, 记

$$e_r = \mathrm{ord}_p(r),\ 1 \leqslant r \leqslant p-1, \quad e = [e_1, \cdots, e_{p-1}].$$

那么根据定理 4.1.8, 存在整数 g, 使得 $\mathrm{ord}_p(g) = e$.

进而, 有 $g^e \equiv 1 \mod p$. 因此, $e \mid \varphi(p)$, 即 $e \mid p-1$.

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

证：(方法一：构造性) 在模 p 的简化剩余系 $1,\cdots,p-1$ 中, 记

$$e_r=\mathrm{ord}_p(r),\ 1\leqslant r\leqslant p-1,\quad e=[e_1,\cdots,e_{p-1}].$$

那么根据定理 4.1.8, 存在整数 g, 使得 $\mathrm{ord}_p(g)=e$.

进而, 有 $g^e\equiv 1 \mod p$. 因此, $e\mid\varphi(p)$, 即 $e\mid p-1$.

又因为 $e_r\mid e$, $r=1,\cdots,p-1$, 从而推出同余方程 $x^e\equiv 1 \mod p$ 有 $p-1$ 个解 $x\equiv 1,\cdots,p-1 \mod p$.

根据定理 3.4.4, 我们有 $p-1\leqslant e$.

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

证：(方法一：构造性) 在模 p 的简化剩余系 $1,\cdots,p-1$ 中, 记

$$e_r = \mathrm{ord}_p(r),\ 1 \leqslant r \leqslant p-1, \quad e = [e_1,\cdots,e_{p-1}].$$

那么根据定理 4.1.8, 存在整数 g, 使得 $\mathrm{ord}_p(g) = e$.

进而, 有 $g^e \equiv 1 \mod p$. 因此, $e \mid \varphi(p)$, 即 $e \mid p-1$.

又因为 $e_r \mid e$, $r = 1,\cdots,p-1$, 从而推出同余方程 $x^e \equiv 1 \mod p$ 有 $p-1$ 个解 $x \equiv 1,\cdots,p-1 \mod p$.

根据定理 3.4.4, 我们有 $p-1 \leqslant e$.

故 $e = p-1$, 即 g 的阶是 $p-1$, 亦即 g 是模 p 的原根.

首先, 我们考虑模为奇素数 p 的情形.

定理 4.2.1

设 p 是奇素数, 则模 p 的原根存在, 且有 $\varphi(p-1)$ 个原根.

证：(方法一：构造性) 在模 p 的简化剩余系 $1,\cdots,p-1$ 中, 记

$$e_r = \mathrm{ord}_p(r),\ 1 \leqslant r \leqslant p-1, \quad e = [e_1,\cdots,e_{p-1}].$$

那么根据定理 4.1.8, 存在整数 g, 使得 $\mathrm{ord}_p(g) = e$.

进而, 有 $g^e \equiv 1 \mod p$. 因此, $e \mid \varphi(p)$, 即 $e \mid p-1$.

又因为 $e_r \mid e$, $r = 1,\cdots,p-1$, 从而推出同余方程 $x^e \equiv 1 \mod p$ 有 $p-1$ 个解 $x \equiv 1,\cdots,p-1 \mod p$.

根据定理 3.4.4, 我们有 $p-1 \leqslant e$.

故 $e = p-1$, 即 g 的阶是 $p-1$, 亦即 g 是模 p 的原根.

此外, 根据推论 4.1.4, 当有原根时, 有 $\varphi(p-1)$ 个原根.

(方法二：存在性) 设 $d \mid p-1$. 用 $F(d)$ 表示模 p 的简化剩余系中阶为 d 的元素个数.

根据推论 4.1.1, 模 p 简化剩余系中每个元素的阶是 $p-1$ 的因数, 所以有

$$\sum_{d \mid p-1} F(d) = p-1.$$

(方法二：存在性) 设 $d \mid p-1$. 用 $F(d)$ 表示模 p 的简化剩余系中阶为 d 的元素个数.

根据推论 4.1.1, 模 p 简化剩余系中每个元素的阶是 $p-1$ 的因数, 所以有

$$\sum_{d \mid p-1} F(d) = p-1.$$

因为模 p 阶为 d 的元素满足同余方程 $x^d - 1 \equiv 0 \mod p$, 根据推论 3.4.3, 同余方程 $x^d - 1 \equiv 0 \mod p$ 有 d 个模 p 不同的解.

(方法二：存在性) 设 $d \mid p-1$. 用 $F(d)$ 表示模 p 的简化剩余系中阶为 d 的元素个数.

根据推论 4.1.1, 模 p 简化剩余系中每个元素的阶是 $p-1$ 的因数, 所以有

$$\sum_{d \mid p-1} F(d) = p-1.$$

因为模 p 阶为 d 的元素满足同余方程 $x^d - 1 \equiv 0 \mod p$, 根据推论 3.4.3, 同余方程 $x^d - 1 \equiv 0 \mod p$ 有 d 个模 p 不同的解.

现在, 若 a 是模 p 阶为 d 的元素, 则同余方程 $x^d - 1 \equiv 0 \mod p$ 的解可以表示成 $x \equiv a^0, a, \cdots, a^{d-1} \mod p$.

根据定理 4.1.4, 这些数中有 $\varphi(d)$ 个阶为 d 的元素.

因此, $F(d) = \varphi(d)$.

(方法二：存在性) 设 $d \mid p-1$. 用 $F(d)$ 表示模 p 的简化剩余系中阶为 d 的元素个数.

根据推论 4.1.1, 模 p 简化剩余系中每个元素的阶是 $p-1$ 的因数, 所以有

$$\sum_{d \mid p-1} F(d) = p-1.$$

因为模 p 阶为 d 的元素满足同余方程 $x^d - 1 \equiv 0 \mod p$, 根据推论 3.4.3, 同余方程 $x^d - 1 \equiv 0 \mod p$ 有 d 个模 p 不同的解.

现在, 若 a 是模 p 阶为 d 的元素, 则同余方程 $x^d - 1 \equiv 0 \mod p$ 的解可以表示成 $x \equiv a^0, a, \cdots, a^{d-1} \mod p$.

根据定理 4.1.4, 这些数中有 $\varphi(d)$ 个阶为 d 的元素.

因此, $F(d) = \varphi(d)$.

而若没有模 p 阶为 d 的元素, 则 $F(d) = 0$.

总之, 我们有 $F(d) \leqslant \varphi(d)$.

但是, 我们又有

$$\sum_{d \mid p-1} \varphi(d) = p - 1.$$

这样, 可以推出

$$\sum_{d \mid p-1} (\varphi(d) - F(d)) = 0.$$

因此, 对所有正整数 $d \mid p-1$, 有

$$F(d) = \varphi(d).$$

但是, 我们又有

$$\sum_{d \mid p-1} \varphi(d) = p - 1.$$

这样, 可以推出

$$\sum_{d \mid p-1} (\varphi(d) - F(d)) = 0.$$

因此, 对所有正整数 $d \mid p-1$, 有

$$F(d) = \varphi(d).$$

特别地, 有 $F(p-1) = \varphi(p-1)$. 这说明存在模 p 阶为 $p-1$ 的元素, 即模 p 的原根存在, 且共有 $\varphi(p-1)$ 个.

但是, 我们又有

$$\sum_{d \mid p-1} \varphi(d) = p - 1.$$

这样, 可以推出

$$\sum_{d \mid p-1} (\varphi(d) - F(d)) = 0.$$

因此, 对所有正整数 $d \mid p-1$, 有

$$F(d) = \varphi(d).$$

特别地, 有 $F(p-1) = \varphi(p-1)$. 这说明存在模 p 阶为 $p-1$ 的元素, 即模 p 的原根存在, 且共有 $\varphi(p-1)$ 个.

推论 4.2.1

设 p 是奇素数, d 是 $p-1$ 的正因数. 则模 p 阶为 d 的元素存在.

目录

其次, 我们考虑一般情形, 给出模 m 的原根存在的充要条件.

定理 4.2.2

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

其次, 我们考虑一般情形, 给出模 m 的原根存在的充要条件.

定理 4.2.2

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

为了证明模 m 原根存在的充要条件 (定理 4.2.2), 现需要给出如下一些定理.

定理 4.2.3

设 g 是模 p 的一个原根, 则 g 或者 $g + p$ 是模 p^2 的原根.

其次, 我们考虑一般情形, 给出模 m 的原根存在的充要条件.

定理 4.2.2

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

为了证明模 m 原根存在的充要条件 (定理 4.2.2), 现需要给出如下一些定理.

定理 4.2.3

设 g 是模 p 的一个原根, 则 g 或者 $g+p$ 是模 p^2 的原根.

证：设 g 模 p^2 的阶为 n, 则 $g^n \equiv 1 \mod p^2$.

显然, 我们有 $g^n \equiv 1 \mod p$.

因为 g 是模 p 的一个原根, 根据定理 4.1.1 得到 $p-1 = \mathrm{ord}_p(g) \mid n$.

又根据推论 4.1.1, 我们有 $n \mid \varphi(p^2) = p(p-1)$.

因此, $n = p-1$, 或者 $n = p(p-1)$.

如果 $n = p(p-1) = \varphi(p^2)$, 则 g 是模 p^2 的原根.

如果 $n = p-1$, 则 $g^{n-1} \equiv 1 \mod p^2$. 下证 $g+p$ 是模 p^2 的原根.

事实上, 我们有

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} \cdot g^{p-2} \cdot p + \binom{p-1}{2} \cdot g^{p-3} \cdot p^2 + \cdots + p^{p-1} \\ &\equiv g^{p-1} + (p-1) \cdot g^{p-2} \cdot p \mod p^2.\end{aligned}$$

进而有

$$(g+p)^{p-1} \equiv 1 + (p-1) \cdot g^{p-2} \cdot p \equiv 1 - g^{p-2} \cdot p \mod p^2.$$

这说明 $(g+p)^{p-1} \not\equiv 1 \mod p^2$.

否则, 如果 $(g+p)^{p-1} \equiv 1 \mod p^2$, 则有 $g^{p-2}p \equiv 0 \mod p^2$, 进而 $g^{p-2} \equiv 0 \mod p$. 这与 g 是模 p 的原根矛盾.

如果 $n = p(p-1) = \varphi(p^2)$, 则 g 是模 p^2 的原根.

如果 $n = p - 1$, 则 $g^{n-1} \equiv 1 \mod p^2$. 下证 $g+p$ 是模 p^2 的原根.

事实上, 我们有

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} \cdot g^{p-2} \cdot p + \binom{p-1}{2} \cdot g^{p-3} \cdot p^2 + \cdots + p^{p-1} \\ &\equiv g^{p-1} + (p-1) \cdot g^{p-2} \cdot p \mod p^2.\end{aligned}$$

进而有

$$(g+p)^{p-1} \equiv 1 + (p-1) \cdot g^{p-2} \cdot p \equiv 1 - g^{p-2} \cdot p \mod p^2.$$

这说明 $(g+p)^{p-1} \not\equiv 1 \mod p^2$.

否则, 如果 $(g+p)^{p-1} \equiv 1 \mod p^2$, 则有 $g^{p-2}p \equiv 0 \mod p^2$, 进而 $g^{p-2} \equiv 0 \mod p$. 这与 g 是模 p 的原根矛盾.

因此, $\mathrm{ord}_{p^2}(g+p) = p(p-1) = \varphi(p^2)$.

故 $g+p$ 是模 p^2 的原根.

定理 4.2.4

设 p 是一个奇素数, 则对任意正整数 α, 模 p^α 的原根存在. 更确切地说, 如果 g 是模 p^2 的一个原根, 则对任意正整数 α, g 是模 p^α 的原根.

定理 4.2.4

设 p 是一个奇素数, 则对任意正整数 α, 模 p^α 的原根存在. 更确切地说, 如果 g 是模 p^2 的一个原根, 则对任意正整数 α, g 是模 p^α 的原根.

证：(i) 我们知道, 模 p 的原根存在, 由定理 4.2.3 及其证明知, 模 p^2 的原根 g 也存在, 并且有 $g^{p-1} \not\equiv 1 \mod p^2$.

我们对于 α 做数学归纳法, 来证明关系式 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \mod p^\alpha$.

$\alpha = 2$ 时, 命题成立.

假设 $\alpha \geq 2$ 时, 命题成立, 即 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \mod p^\alpha$.

这个关系可以写成 $g^{p^{\alpha-2}(p-1)} = 1 + u_{\alpha-2}p^{\alpha-1}, p \nmid u_{\alpha-2}$.

两端做 p 次平方, 我们有

$$
\begin{aligned}
g^{p^{\alpha-1}(p-1)} &= (1 + u_{\alpha-2}p^{\alpha-1})^p \\
&= 1 + \binom{p}{1} u_{\alpha-2}p^{\alpha-1} + \binom{p}{2} (u_{\alpha-2}p^{\alpha-1})^2 + \cdots + (u_{\alpha-2}p^{\alpha-1})^p \\
&\equiv 1 + u_{\alpha-2}p^\alpha \mod p^{\alpha+1}.
\end{aligned}
$$

因为 $p \nmid u_{\alpha-2}$, 所以 $g^{p^{\alpha-1}(p-1)} \not\equiv 1 \mod p^{\alpha+1}$.

也就是说, 对于 $\alpha+1$ 成立,

根据数学归纳法原理, 对于所有整数 $\alpha \geq 2$ 成立.

因为 $p \nmid u_{\alpha-2}$, 所以 $g^{p^{\alpha-1}(p-1)} \not\equiv 1 \mod p^{\alpha+1}$.

也就是说, 对于 $\alpha+1$ 成立,

根据数学归纳法原理, 对于所有整数 $\alpha \geq 2$ 成立.

(ii) 设 g 是模 p^{α} 的阶为 d, 则 $g^d \equiv 1 \mod p^{\alpha}$,

从而 $g^d \equiv 1 \mod p^2$.

因为 g 是模 p^2 的原根,

根据定理 4.1.1, g 模 p^2 的阶为 $p(p-1) = \varphi(p^2) \mid d$.

同时, $d \mid \varphi(p^{\alpha})$,

因此, 我们可将 d 写成 $d = p^{r-1}(p-1)$, $2 \leq r \leq \alpha$.

再将上式代入, 得到 $1 + u_{r-1}p^r = g^{p^{r-1}(p-1)} \equiv 1 \mod p^{\alpha}$,

或者, $u_{r-1}p^r \equiv 0 \mod p^{\alpha}$.

因为 $p \nmid u_{r-1}$, 所以 $r \geq \alpha$.

因此, $r = \alpha$. 就是说, g 是模 p^{α} 的原根.

定理 4.2.5

设 $\alpha \geqslant 1$, g 是模 p^α 原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

定理 4.2.5

设 $\alpha \geqslant 1$, g 是模 p^α 原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

证： (i) 设奇数 a 满足同余方程 $a^d \equiv 1 \mod p^\alpha$,

又显然有 $a^d \equiv 1 \mod 2$, 则根据性质 2.1.7, $a^d \equiv 1 \mod (2p^\alpha)$.

反之亦然.

定理 4.2.5

设 $\alpha \geqslant 1$, g 是模 p^α 原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

证： (i) 设奇数 a 满足同余方程 $a^d \equiv 1 \mod p^\alpha$,

又显然有 $a^d \equiv 1 \mod 2$, 则根据性质 2.1.7, $a^d \equiv 1 \mod (2p^\alpha)$.

反之亦然.

(ii) 若 g 是奇数, 令 $d = \varphi(p^\alpha)$, 则 $\varphi(2p^\alpha) = \varphi(p^\alpha) = d$.

又当 $g^d \equiv 1 \mod p^\alpha, g^r \not\equiv 1 \mod p^\alpha, \quad 0 < r < d$ 时, 有

$$g^d \equiv 1 \mod (2p^\alpha), g^r \not\equiv 1 \mod (2p^\alpha), \quad 0 < r < d.$$

故 g 是模 $2p^\alpha$ 的一个原根.

定理 4.2.5

设 $\alpha \geqslant 1$, g 是模 p^α 原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

证： (i) 设奇数 a 满足同余方程 $a^d \equiv 1 \mod p^\alpha$,

又显然有 $a^d \equiv 1 \mod 2$, 则根据性质 2.1.7, $a^d \equiv 1 \mod (2p^\alpha)$.

反之亦然.

(ii) 若 g 是奇数, 令 $d = \varphi(p^\alpha)$, 则 $\varphi(2p^\alpha) = \varphi(p^\alpha) = d$.

又当 $g^d \equiv 1 \mod p^\alpha, g^r \not\equiv 1 \mod p^\alpha, \quad 0 < r < d$ 时, 有

$$g^d \equiv 1 \mod (2p^\alpha), g^r \not\equiv 1 \mod (2p^\alpha), \quad 0 < r < d.$$

故 g 是模 $2p^\alpha$ 的一个原根.

(iii) 若 g 是偶数, 则 $g+p^\alpha$ 是奇数.

类似 (ii) 可得, $g+p^\alpha$ 是模 $2p^\alpha$ 的一个原根.

定理 4.2.6

设 a 是一个奇数. 则对任意整数 $\alpha \geqslant 3$, 有

$$a^{\frac{\varphi(2^{\alpha})}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^{\alpha}.$$

定理 4.2.6

设 a 是一个奇数. 则对任意整数 $\alpha \geqslant 3$, 有

$$a^{\frac{\varphi(2^\alpha)}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^\alpha.$$

证：我们用数学归纳法来证明这个结论,

将奇数 a 写成 $a = 2b+1$, 我们有 $a^2 = 4b(b+1)+1 \equiv 1 \mod 2^3$.

因此, 结论对于 $\alpha = 3$ 成立.

定理 4.2.6

设 a 是一个奇数. 则对任意整数 $\alpha \geqslant 3$, 有

$$a^{\frac{\varphi(2^\alpha)}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^\alpha.$$

证：我们用数学归纳法来证明这个结论,

将奇数 a 写成 $a = 2b+1$, 我们有 $a^2 = 4b(b+1)+1 \equiv 1 \mod 2^3$.

因此, 结论对于 $\alpha = 3$ 成立.

假设对于 $\alpha - 1$, 结论也成立, 即 $a^{2^{(\alpha-1)-2}} \equiv 1 \mod 2^{\alpha-1}$.

故存在整数 $t_{\alpha-1}$ 使得 $a^{2^{(\alpha-1)-2}} = 1 + t_{\alpha-1}2^{\alpha-1}$.

两端平方, 得到

$$a^{2^{\alpha-2}} = (1+2^{\alpha-1}t_{\alpha-1})^2 = 1 + (t_{\alpha-1} + 2^{\alpha-2}t_{\alpha-1}^2)2^\alpha \equiv 1 \mod 2^\alpha.$$

这就是说, 结论对 α 成立.

根据数学归纳法原理, 同余方程对于所有 $\alpha \geq 3$ 成立.

定理 4.2.6

设 a 是一个奇数. 则对任意整数 $\alpha \geqslant 3$, 有

$$a^{\frac{\varphi(2^\alpha)}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^\alpha.$$

证：我们用数学归纳法来证明这个结论,

将奇数 a 写成 $a = 2b+1$, 我们有 $a^2 = 4b(b+1)+1 \equiv 1 \mod 2^3$.

因此, 结论对于 $\alpha = 3$ 成立.

假设对于 $\alpha - 1$, 结论也成立, 即 $a^{2^{(\alpha-1)-2}} \equiv 1 \mod 2^{\alpha-1}$.

故存在整数 $t_{\alpha-1}$ 使得 $a^{2^{(\alpha-1)-2}} = 1 + t_{\alpha-1}2^{\alpha-1}$.

两端平方, 得到

$$a^{2^{\alpha-2}} = (1+2^{\alpha-1}t_{\alpha-1})^2 = 1 + (t_{\alpha-1} + 2^{\alpha-2}t_{\alpha-1}^2)2^\alpha \equiv 1 \mod 2^\alpha.$$

这就是说, 结论对 α 成立.

根据数学归纳法原理, 同余方程对于所有 $\alpha \geq 3$ 成立.

注：定理 4.2.6 说明对于任意整数 $\alpha \geq 3$, 模 2^α 没有原根.

下面给出定理 4.2.2 的证明.

证：必要性. 设 m 的标准分解式为 $m = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

下面给出定理 4.2.2 的证明.

证：必要性. 设 m 的标准分解式为 $m = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

若 $(a, m) = 1$, 则 $(a, 2^{\alpha}) = 1, (a, p_i^{\alpha_i}) = 1, i = 1, \cdots, k$.

根据定理 2.2.13(欧拉定理) 及定理 4.2.6, 我们有

$$\begin{cases} a^{\tau} & \equiv 1 \mod 2^{\alpha}, \\ a^{\varphi(p_1^{\alpha_1})} & \equiv 1 \mod p_1^{\alpha_1}, \\ & \vdots \\ a^{\varphi(p_k^{\alpha_k})} & \equiv 1 \mod p_k^{\alpha_k}. \end{cases}$$

其中 $\tau = \begin{cases} \varphi(2^{\alpha}), & \alpha \leqslant 2, \\ \frac{\varphi(2^{\alpha})}{2}, & \alpha \geqslant 3. \end{cases}$

下面给出定理 4.2.2 的证明.

证：必要性. 设 m 的标准分解式为 $m = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

若 $(a, m) = 1$, 则 $(a, 2^\alpha) = 1, (a, p_i^{\alpha_i}) = 1, i = 1, \cdots, k$.

根据定理 2.2.13(欧拉定理) 及定理 4.2.6, 我们有

$$\begin{cases} a^\tau & \equiv 1 \mod 2^\alpha, \\ a^{\varphi(p_1^{\alpha_1})} & \equiv 1 \mod p_1^{\alpha_1}, \\ & \vdots \\ a^{\varphi(p_k^{\alpha_k})} & \equiv 1 \mod p_k^{\alpha_k}. \end{cases}$$

其中 $\tau = \begin{cases} \varphi(2^\alpha), & \alpha \leqslant 2, \\ \frac{\varphi(2^\alpha)}{2}, & \alpha \geqslant 3. \end{cases}$

令 $h = [\tau, \varphi(p_1^{\alpha_1}), \cdots, \varphi(p_k^{\alpha_k})]$.

下面给出定理 4.2.2 的证明.

证：必要性. 设 m 的标准分解式为 $m = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

若 $(a, m) = 1$, 则 $(a, 2^{\alpha}) = 1, (a, p_i^{\alpha_i}) = 1, i = 1, \cdots, k$.

根据定理 2.2.13(欧拉定理) 及定理 4.2.6, 我们有

$$\begin{cases} a^{\tau} & \equiv 1 \pmod{2^{\alpha}}, \\ a^{\varphi(p_1^{\alpha_1})} & \equiv 1 \pmod{p_1^{\alpha_1}}, \\ & \vdots \\ a^{\varphi(p_k^{\alpha_k})} & \equiv 1 \pmod{p_k^{\alpha_k}}. \end{cases}$$

其中 $\tau = \begin{cases} \varphi(2^{\alpha}), & \alpha \leqslant 2, \\ \frac{\varphi(2^{\alpha})}{2}, & \alpha \geqslant 3. \end{cases}$

令 $h = [\tau, \varphi(p_1^{\alpha_1}), \cdots, \varphi(p_k^{\alpha_k})]$.

对所有整数 a, $(a, m) = 1$, 我们有 $a^h \equiv 1 \pmod{m}$.

因此, 若 $h < \varphi(m)$, 则模 m 的原根不存在.

现在讨论何时 $h = \varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

现在讨论何时 $h = \varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(1) 当 $\alpha \geqslant 3$ 时, $\tau = \frac{\varphi(2^\alpha)}{2}$. 因此, $h \leqslant \frac{\varphi(m)}{2} < \varphi(m)$.

现在讨论何时 $h=\varphi(m)=\varphi(2^{\alpha})\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(1) 当 $\alpha\geqslant 3$ 时, $\tau=\frac{\varphi(2^{\alpha})}{2}$. 因此, $h\leqslant\frac{\varphi(m)}{2}<\varphi(m)$.

(2) 当 $k\geqslant 2$ 时, $2\mid\varphi(p_1^{\alpha_1}),2\mid\varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}),\varphi(p_2k^{\alpha_2})]\leqslant\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})<\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}).$$

因此, $h<\varphi(m)$.

现在讨论何时 $h=\varphi(m)=\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(1) 当 $\alpha\geqslant 3$ 时, $\tau=\frac{\varphi(2^\alpha)}{2}$. 因此, $h\leqslant\frac{\varphi(m)}{2}<\varphi(m)$.

(2) 当 $k\geqslant 2$ 时, $2\mid\varphi(p_1^{\alpha_1}), 2\mid\varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}),\varphi(p_2k^{\alpha_2})]\leqslant\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})<\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}).$$

因此, $h<\varphi(m)$.

(3) 当 $\alpha=2, k=1$ 时, $\varphi(2^\alpha)=2, 2\mid\varphi(p_1^{\alpha_1})$.

因此, $h=\varphi(p_1^{\alpha_1})<\varphi(2^\alpha)\varphi(p_1^{\alpha_1})=\varphi(m)$.

现在讨论何时 $h = \varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(1) 当 $\alpha \geqslant 3$ 时, $\tau = \frac{\varphi(2^\alpha)}{2}$. 因此, $h \leqslant \frac{\varphi(m)}{2} < \varphi(m)$.

(2) 当 $k \geqslant 2$ 时, $2 \mid \varphi(p_1^{\alpha_1}), 2 \mid \varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}), \varphi(p_2k^{\alpha_2})] \leqslant \frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) < \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}).$$

因此, $h < \varphi(m)$.

(3) 当 $\alpha = 2, k = 1$ 时, $\varphi(2^\alpha) = 2, 2 \mid \varphi(p_1^{\alpha_1})$.

因此, $h = \varphi(p_1^{\alpha_1}) < \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) = \varphi(m)$.

故只有在 (α, k) 是 $(1,0),(2,0),(0,1),(1,1)$ 这四种情形之一, 即只有在 m 是 $2, 4, p^\alpha, 2p^\alpha$ 这四个数之一时, 才可能使 $h = \varphi(m)$. 因此必要性成立.

现在讨论何时 $h=\varphi(m)=\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(1) 当 $\alpha\geqslant 3$ 时, $\tau=\frac{\varphi(2^\alpha)}{2}$. 因此, $h\leqslant\frac{\varphi(m)}{2}<\varphi(m)$.

(2) 当 $k\geqslant 2$ 时, $2\mid\varphi(p_1^{\alpha_1}), 2\mid\varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}),\varphi(p_2k^{\alpha_2})]\leqslant\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})<\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}).$$

因此, $h<\varphi(m)$.

(3) 当 $\alpha=2,k=1$ 时, $\varphi(2^\alpha)=2, 2\mid\varphi(p_1^{\alpha_1})$.

因此, $h=\varphi(p_1^{\alpha_1})<\varphi(2^\alpha)\varphi(p_1^{\alpha_1})=\varphi(m)$.

故只有在 (α,k) 是 $(1,0),(2,0),(0,1),(1,1)$ 这四种情形之一, 即只有在 m 是 $2,4,p^\alpha,2p^\alpha$ 这四个数之一时, 才可能使 $h=\varphi(m)$. 因此必要性成立.

充分性. 当 $m=2$ 时, $\varphi(2)=1$, 整数 1 是模 2 的原根;

当 $m=4$ 时, $\varphi(4)=2$, 整数 3 是模 2 的原根;

当 $m=p^\alpha$ 时, 根据定理 4.2.4, 模 m 的原根存在;

当 $m=2p^\alpha$ 时, 根据定理 4.2.5, 模 m 的原根存在.

因此, 充分性成立.

目录

接下来, 给出模 m 原根的构造方法.

定理 4.2.7

设 $m>1$, $\varphi(m)$ 的所有不同素因数是 $q_1,\cdots,q_k$, 则 g 是模 m 的一个原根的充要条件是 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m,\quad i=1,\cdots,k.$

接下来, 给出模 m 原根的构造方法.

定理 4.2.7

设 $m > 1$, $\varphi(m)$ 的所有不同素因数是 $q_1, \cdots, q_k$, 则 g 是模 m 的一个原根的充要条件是 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m, \quad i = 1, \cdots, k$.

证：设 g 是模 m 的一个原根, 则 g 对模 m 的阶是 $\varphi(m)$. 但

$$0 < \varphi(m)/q_i < \varphi(m), \quad i = 1, \cdots, k.$$

根据定理 4.1.2, 有 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m, \quad i = 1, \cdots, k$.

接下来, 给出模 m 原根的构造方法.

定理 4.2.7

设 $m>1$, $\varphi(m)$ 的所有不同素因数是 $q_1,\cdots,q_k$, 则 g 是模 m 的一个原根的充要条件是 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m, \quad i=1,\cdots,k.$

证：设 g 是模 m 的一个原根, 则 g 对模 m 的阶是 $\varphi(m)$. 但

$$0<\varphi(m)/q_i<\varphi(m), \quad i=1,\cdots,k.$$

根据定理 4.1.2, 有 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m, \quad i=1,\cdots,k.$

反过来, 若 g 对模 m 的阶 $e<\varphi(m)$, 则根据定理 4.1.1, 我们有 $e \mid \varphi(m)$. 因而, 存在一个素数 q 使得 $q \mid \frac{\varphi(m)}{e}$, 即

$$\frac{\varphi(m)}{e}=u\cdot q \quad 或 \quad \frac{\varphi(m)}{q}=u\cdot e.$$

进而, $g^{\frac{\varphi(m)}{q}}=(g^e)^u\equiv 1 \mod p.$ 与假设矛盾.

例 4.2.1　求模 41 的所有原根.

例 4.2.1 求模 41 的所有原根.

解: 因为 $\varphi(m) = \varphi(40) = 2^3 \cdot 5$,

所以 $\varphi(m)$ 的素因数为 $q_1 = 2, q_2 = 5$.

进而, 只需证明: g^{20}, g^8 模 m 是否同余于 1.

对于 $2, 3, \cdots, 40$, 逐个验算:

例 4.2.1 求模 41 的所有原根.

解: 因为 $\varphi(m)=\varphi(40)=2^3\cdot 5$,

所以 $\varphi(m)$ 的素因数为 $q_1=2, q_2=5$.

进而, 只需证明: g^{20}, g^8 模 m 是否同余于 1.

对于 $2, 3, \cdots, 40$, 逐个验算:

$$
\begin{aligned}
2^8 &\equiv 10 \mod 41, & 2^{20} &\equiv 1 \mod 41,\\
3^8 &\equiv 1 \mod 41, & 3^{20} &\equiv -1 \mod 41,\\
4^8 &\equiv 18 \mod 41, & 4^{20} &\equiv 1 \mod 41,\\
5^8 &\equiv 18 \mod 41, & 5^{20} &\equiv 1 \mod 41,\\
6^8 &\equiv 10 \mod 41, & 6^{20} &\equiv -1 \mod 41.
\end{aligned}
$$

例 4.2.1 求模 41 的所有原根.

解: 因为 $\varphi(m)=\varphi(40)=2^3\cdot 5$,

所以 $\varphi(m)$ 的素因数为 $q_1=2, q_2=5$.

进而, 只需证明: g^{20}, g^8 模 m 是否同余于 1.

对于 $2,3,\cdots,40$, 逐个验算:

$$
\begin{aligned}
2^8 &\equiv 10 \mod 41, & 2^{20} &\equiv 1 \mod 41,\\
3^8 &\equiv 1 \mod 41, & 3^{20} &\equiv -1 \mod 41,\\
4^8 &\equiv 18 \mod 41, & 4^{20} &\equiv 1 \mod 41,\\
5^8 &\equiv 18 \mod 41, & 5^{20} &\equiv 1 \mod 41,\\
6^8 &\equiv 10 \mod 41, & 6^{20} &\equiv -1 \mod 41.
\end{aligned}
$$

故 $g=6$ 是模 41 的原根.

进一步, $(d,\varphi(m))=1$ 时, $\mathrm{ord}_m(g^d)=\mathrm{ord}_m(g)$,
因此, d 遍历模 $\varphi(m)=40$ 的简化剩余系,

$$1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39,$$

共 $\varphi(\varphi(m))=16$ 个数时, g^d 遍历模 41 的所有原根:

$$\begin{aligned}
6^1 &\equiv 6 \mod 41, & 6^3 &\equiv 11 \mod 41,\\
6^7 &\equiv 29 \mod 41, & 6^9 &\equiv 19 \mod 41,\\
6^{11} &\equiv 28 \mod 41, & 6^{13} &\equiv 24 \mod 41,\\
6^{17} &\equiv 26 \mod 41, & 6^{19} &\equiv 34 \mod 41,\\
6^{21} &\equiv 35 \mod 41, & 6^{23} &\equiv 30 \mod 41,\\
6^{27} &\equiv 12 \mod 41, & 6^{29} &\equiv 22 \mod 41,\\
6^{31} &\equiv 13 \mod 41, & 6^{33} &\equiv 17 \mod 41,\\
6^{37} &\equiv 15 \mod 41, & 6^{39} &\equiv 7 \mod 41.
\end{aligned}$$

例 4.2.2 求模 43 的所有原根.

例 4.2.2 求模 43 的所有原根.

解: 设 $m=43$, 则 $\varphi(m)=\varphi(43)=2\cdot 3\cdot 7$, $q_1=2, q_2=3, q_3=7$.

因此, $\varphi(m)/q_1=21, \varphi(m)/q_2=14, \varphi(m)/q_3=6$.

这样, 只需证明: $g^{21}, g^{1}4, g^{6}$ 模 m 是否同余于 1.

对于 $2, 3, \cdots,$ 逐个验算:

例 4.2.2 求模 43 的所有原根.

解: 设 $m = 43$, 则 $\varphi(m) = \varphi(43) = 2 \cdot 3 \cdot 7$, $q_1 = 2, q_2 = 3, q_3 = 7$.

因此, $\varphi(m)/q_1 = 21, \varphi(m)/q_2 = 14, \varphi(m)/q_3 = 6$.

这样, 只需证明: $g^{21}, g^{1}4, g^{6}$ 模 m 是否同余于 1.

对于 $2, 3, \cdots,$ 逐个验算:

$$2^6 \equiv 21 \mod 43,\quad 2^{14} \equiv 1 \mod 43,\quad 2^{21} \equiv -1 \mod 43,$$

$$3^6 \equiv -2 \mod 43,\ 3^{14} \equiv 36 \mod 43,\ 3^{21} \equiv -1 \mod 43.$$

例 4.2.2 求模 43 的所有原根.

解: 设 $m=43$, 则 $\varphi(m)=\varphi(43)=2\cdot 3\cdot 7$, $q_1=2, q_2=3, q_3=7$.

因此, $\varphi(m)/q_1=21, \varphi(m)/q_2=14, \varphi(m)/q_3=6$.

这样, 只需证明: $g^{21}, g^{1}4, g^{6}$ 模 m 是否同余于 1.

对于 $2, 3, \cdots$, 逐个验算:

$$2^6 \equiv 21 \mod 43, \quad 2^{14} \equiv 1 \mod 43, \quad 2^{21} \equiv -1 \mod 43,$$
$$3^6 \equiv -2 \mod 43, \; 3^{14} \equiv 36 \mod 43, \; 3^{21} \equiv -1 \mod 43.$$

因此, 3 是模 43 的原根.

当 d 遍历模 $\varphi(m)=42$ 的简化剩余系, $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$, 共 $\varphi(\varphi(43))=12$ 个数时, 3^d 遍历模 43 的所有原根:

$3^1 \equiv 3 \mod 43$, $3^5 \equiv 28 \mod 43$, $3^{11} \equiv 12 \mod 43$, $3^{13} \equiv 12 \mod 43$,
$3^{17} \equiv 26 \mod 43$, $3^{19} \equiv 19 \mod 43$, $3^{23} \equiv 34 \mod 43$, $3^{25} \equiv 5 \mod 43$,
$3^{29} \equiv 18 \mod 43$, $3^{31} \equiv 33 \mod 43$, $3^{37} \equiv 20 \mod 43$, $3^{41} \equiv 29 \mod 43$.

例 4.2.3 设 $m = 41^2 = 1681$, 求模 m 的原根.

例 4.2.3　设 $m = 41^2 = 1681$, 求模 m 的原根.

解: 因为已知 6 是模 $p = 41$ 的原根, 所以根据定理 4.2.3, 可知 6 或者 $6 + 41 = 47$ 是模 $41^2 = 1681$ 的原根. 事实上, 我们有

$$6^{40} \equiv 143 \equiv 1 + 3 \cdot 41 \mod 41^2,$$

$$47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \mod 41^2.$$

这就是说, $6^{40} \not\equiv 1 \mod 41^2$, $47^{40} \not\equiv 1 \mod 41^2$. 因此, 6 和 47 都是模 $m = 41^2 = 1681$ 的原根, 它们也是模 41^α 的原根.

例 4.2.3 设 $m = 41^2 = 1681$, 求模 m 的原根.

解: 因为已知 6 是模 $p = 41$ 的原根, 所以根据定理 4.2.3, 可知 6 或者 $6 + 41 = 47$ 是模 $41^2 = 1681$ 的原根. 事实上, 我们有

$$6^{40} \equiv 143 \equiv 1 + 3 \cdot 41 \mod 41^2,$$

$$47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \mod 41^2.$$

这就是说, $6^{40} \not\equiv 1 \mod 41^2$, $47^{40} \not\equiv 1 \mod 41^2$. 因此, 6 和 47 都是模 $m = 41^2 = 1681$ 的原根, 它们也是模 41^α 的原根.

由于 $(d, \varphi(m)) = 1$ 时, $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, 因此, 当 d 遍历模 $\varphi(41^2) = 1640$ 的简化剩余系时, 6^d 遍历模 41^2 的所有原根.

例 4.2.3　设 $m = 41^2 = 1681$, 求模 m 的原根.

解: 因为已知 6 是模 $p = 41$ 的原根, 所以根据定理 4.2.3, 可知 6 或者 $6 + 41 = 47$ 是模 $41^2 = 1681$ 的原根. 事实上, 我们有

$$6^{40} \equiv 143 \equiv 1 + 3 \cdot 41 \mod 41^2,$$

$$47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \mod 41^2.$$

这就是说, $6^{40} \not\equiv 1 \mod 41^2$, $47^{40} \not\equiv 1 \mod 41^2$. 因此, 6 和 47 都是模 $m = 41^2 = 1681$ 的原根, 它们也是模 41^α 的原根.

由于 $(d, \varphi(m)) = 1$ 时, $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, 因此, 当 d 遍历模 $\varphi(41^2) = 1640$ 的简化剩余系时, 6^d 遍历模 41^2 的所有原根.

例 4.2.4　设 $m = 2 \cdot 41^2 = 3362$, 求模 m 的原根.

例 4.2.3 设 $m = 41^2 = 1681$, 求模 m 的原根.

解: 因为已知 6 是模 $p = 41$ 的原根, 所以根据定理 4.2.3, 可知 6 或者 $6 + 41 = 47$ 是模 $41^2 = 1681$ 的原根. 事实上, 我们有

$$6^{40} \equiv 143 \equiv 1 + 3 \cdot 41 \pmod{41^2},$$

$$47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \pmod{41^2}.$$

这就是说, $6^{40} \not\equiv 1 \pmod{41^2}$, $47^{40} \not\equiv 1 \pmod{41^2}$. 因此, 6 和 47 都是模 $m = 41^2 = 1681$ 的原根, 它们也是模 41^α 的原根.

由于 $(d, \varphi(m)) = 1$ 时, $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, 因此, 当 d 遍历模 $\varphi(41^2) = 1640$ 的简化剩余系时, 6^d 遍历模 41^2 的所有原根.

例 4.2.4 设 $m = 2 \cdot 41^2 = 3362$, 求模 m 的原根.

解: 这里应用定理 4.2.5 及例 4.2.3, 即可得到 $6 + 41^2 = 1687$ 和 47 (是两个奇数) 是模 $2 \cdot 41^2 = 3362$ 的原根.

目录

本小节利用原根引入指标的概念，并应用指标的性质研究同余方程

$$x^n \equiv a \mod m, (a, m) = 1$$

有解的条件及解数.

根据定理 4.1.2 可知，当 r 遍历模 $\varphi(m)$ 的最小完全剩余系时，g^r 遍历模 m 的一个简化剩余系.

因此，对任意的整数 a, $(a, m) = 1$, 存在唯一的整数

$$r,\ 1 \leqslant r \leqslant \varphi(m),$$

使得 $g^r \equiv a \mod m$, 其中 g 是模 m 的一个原根.

本小节利用原根引入指标的概念，并应用指标的性质研究同余方程

$$x^n \equiv a \mod m, (a, m) = 1$$

有解的条件及解数.

根据定理 4.1.2 可知，当 r 遍历模 $\varphi(m)$ 的最小完全剩余系时，g^r 遍历模 m 的一个简化剩余系.

因此，对任意的整数 a，$(a, m) = 1$，存在唯一的整数

$$r,\ 1 \leqslant r \leqslant \varphi(m),$$

使得 $g^r \equiv a \mod m$，其中 g 是模 m 的一个原根.

定义 4.2.1

设 $m > 1$ 是整数，g 是模 m 的一个原根. 设 a 是与 m 互素的整数，则存在唯一的整数 r 使得 $g^r \equiv a \mod m$，$1 \leqslant r \leqslant \varphi(m)$ 成立，这个整数 r 叫做以 g 为底的 a 对模 m 的一个**指标**，记作 $r = \mathrm{ind}_g a$ 或 $r = \mathrm{ind}\ a$.

注：从整数 r 计算 $g^r \equiv a \mod m$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \mod m$ (**离散对数问题**) 却非常困难.

注：从整数 r 计算 $g^r \equiv a \mod m$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \mod m$ (**离散对数问题**) 却非常困难.

根据上述定义, 我们可以得到如下结论.

定理 4.2.8

设 $m > 1$ 是整数, g 是模 m 的一个原根, a 是与 m 互素的整数, 则同余方程 $x^n \equiv a \mod m$ 有解的充要条件是 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 且在有解的情况下, 解数为 $(n, \varphi(m))$.

注：从整数 r 计算 $g^r \equiv a \mod m$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \mod m$ (**离散对数问题**) 却非常困难.

根据上述定义, 我们可以得到如下结论.

定理 4.2.8

设 $m > 1$ 是整数, g 是模 m 的一个原根, a 是与 m 互素的整数, 则同余方程 $x^n \equiv a \mod m$ 有解的充要条件是 $(n, \varphi(m)) \mid \text{ind}_g a$, 且在有解的情况下, 解数为 $(n, \varphi(m))$.

证：若同余方程 $x^n \equiv a \mod m$ 有解 $x \equiv x_0 \mod m$, 则分别存在非负整数 u, r 使得 $x_0 \equiv g^u \mod m, a \equiv g^r \mod m$.

注：从整数 r 计算 $g^r \equiv a \mod m$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \mod m$ (**离散对数问题**) 却非常困难.

根据上述定义, 我们可以得到如下结论.

定理 4.2.8

设 $m > 1$ 是整数, g 是模 m 的一个原根, a 是与 m 互素的整数, 则同余方程 $x^n \equiv a \mod m$ 有解的充要条件是 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 且在有解的情况下, 解数为 $(n, \varphi(m))$.

证：若同余方程 $x^n \equiv a \mod m$ 有解 $x \equiv x_0 \mod m$, 则分别存在非负整数 u, r 使得 $x_0 \equiv g^u \mod m, a \equiv g^r \mod m$.

进而, $g^{un} \equiv g^r \mod m$, 即有, $un \equiv r \mod \varphi(m)$. 亦即同余方程

$$nX \equiv r \mod \varphi(m)$$

有解 $X \equiv u \mod \varphi(m)$.

注：从整数 r 计算 $g^r \equiv a \mod m$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \mod m$ (**离散对数问题**) 却非常困难.

根据上述定义, 我们可以得到如下结论.

定理 4.2.8

设 $m > 1$ 是整数, g 是模 m 的一个原根, a 是与 m 互素的整数, 则同余方程 $x^n \equiv a \mod m$ 有解的充要条件是 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 且在有解的情况下, 解数为 $(n, \varphi(m))$.

证：若同余方程 $x^n \equiv a \mod m$ 有解 $x \equiv x_0 \mod m$, 则分别存在非负整数 u, r 使得 $x_0 \equiv g^u \mod m, a \equiv g^r \mod m$.

进而, $g^{un} \equiv g^r \mod m$, 即有, $un \equiv r \mod \varphi(m)$. 亦即同余方程

$$nX \equiv r \mod \varphi(m)$$

有解 $X \equiv u \mod \varphi(m)$.

因此, $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 成立.

反过来, 若 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 成立,
则同余方程

$$nX \equiv r \mod \varphi(m)$$

有解 $X \equiv u \mod \varphi(m)$, 且解数为 $(n, \varphi(m))$.

反过来, 若 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 成立,

则同余方程

$$nX \equiv r \mod \varphi(m)$$

有解 $X \equiv u \mod \varphi(m)$, 且解数为 $(n, \varphi(m))$.

因此, 同余方程 $x^n \equiv a \mod m$ 有解且解数为 $(n, \varphi(m))$.

反过来, 若 $(n, \varphi(m)) \mid \mathrm{ind}_g a$, 成立,
则同余方程

$$nX \equiv r \mod \varphi(m)$$

有解 $X \equiv u \mod \varphi(m)$, 且解数为 $(n, \varphi(m))$.
因此, 同余方程 $x^n \equiv a \mod m$ 有解且解数为 $(n, \varphi(m))$.

由此, 类似于二次剩余, 我们可以给出如下定义.

定义 4.2.2

设 $m > 1$ 是整数, a 是与 m 互素的整数, 如果 n 次同余方程

$$x^n \equiv a \mod m$$

有解, 则称 a 叫做对模 m 的 n **次剩余**; 否则, a 叫做对模 m 的 n **次非剩余**.

进而，我们得到如下推论.

推论 4.2.2

在定理 4.2.8 的假设条件下，a 是模 m 的 n 次剩余的充要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m)).$$

进而, 我们得到如下推论.

推论 4.2.2

在定理 4.2.8 的假设条件下, a 是模 m 的 n 次剩余的充要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m)).$$

证：由定理 4.2.8 的证明知, 同余方程 $x^n \equiv a \mod m$ 有解的充要条件是同余方程 $nX \equiv r \mod \varphi(m)$ 有解.

进而, 我们得到如下推论.

推论 4.2.2

在定理 4.2.8 的假设条件下, a 是模 m 的 n 次剩余的充要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m)).$$

证: 由定理 4.2.8 的证明知, 同余方程 $x^n \equiv a \mod m$ 有解的充要条件是同余方程 $nX \equiv r \mod \varphi(m)$ 有解.

而这等价于 $(n, \varphi(m)) \mid \mathrm{ind}_g a$,, 其中 g 是模 m 的一个原根, 也即

$$\mathrm{ind}_g a \equiv 0 \mod d.$$

进而, 我们得到如下推论.

推论 4.2.2

在定理 4.2.8 的假设条件下, a 是模 m 的 n 次剩余的充要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m)).$$

证：由定理 4.2.8 的证明知, 同余方程 $x^n \equiv a \mod m$ 有解的充要条件是同余方程 $nX \equiv r \mod \varphi(m)$ 有解.

而这等价于 $(n, \varphi(m)) \mid \mathrm{ind}_g a$,, 其中 g 是模 m 的一个原根, 也即

$$\mathrm{ind}_g a \equiv 0 \mod d.$$

两端同乘以 $\frac{\varphi(m)}{d}$ 得,

$$\frac{\varphi(m)}{d} \mathrm{ind}_g a \equiv 0 \mod \varphi(m).$$

进而, 我们得到如下推论.

推论 4.2.2

在定理 4.2.8 的假设条件下, a 是模 m 的 n 次剩余的充要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m)).$$

证：由定理 4.2.8 的证明知, 同余方程 $x^n \equiv a \mod m$ 有解的充要条件是同余方程 $nX \equiv r \mod \varphi(m)$ 有解.

而这等价于 $(n, \varphi(m)) \mid \text{ind}_g a$,, 其中 g 是模 m 的一个原根, 也即

$$\text{ind}_g a \equiv 0 \mod d.$$

两端同乘以 $\frac{\varphi(m)}{d}$ 得,

$$\frac{\varphi(m)}{d}\text{ind}_g a \equiv 0 \mod \varphi(m).$$

这等价于 $a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m, \quad d = (n, \varphi(m))$.

结论成立.

本课作业

1. 计算 $3, 7, 10$ 模 19 的阶.
2. 求模 11 的所有原根, 并一一列出.
3. 设 $m = 11^2 = 121$, 求模 m 的原根.
4. 已知 5 是模 17 的原根, 求 5 对 17 的指标.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn