華東師範大學
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础(一)

沈佳辰
jcshen@sei.ecnu.edu.cn

華東師範大學
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础

第四章 原根与指数

§4.1 阶和原根

- 由欧拉定理，若$(a,m)=1$，则有$a^{\varphi(m)}\equiv 1\ (mod\ m)$。因此同余式$a^n\equiv 1\ (mod\ m)$有解，那么它的最小正整数解是什么？又有哪些性质？

§4.1 阶和原根

- 由欧拉定理，若$(a,m)=1$，则有$a^{\varphi(m)}\equiv 1\ (mod\ m)$。因此同余式$a^n\equiv 1\ (mod\ m)$有解，那么它的最小正整数解是什么？又有哪些性质？

- 定义4.1.1 设a,m是正整数，$m>1,(a,m)=1$，则满足同余式

$$a^n\equiv 1\ (mod\ m)\qquad (4.1)$$

的最小正整数n称为a模m的阶或次数，记作$ord_m(a)$或$ord\ (a)$。如果$ord_m(a)=\varphi(m)$，则a叫做模m的原根。

- 例 设m为正整数，$m>2$，则$ord_m(1)=1, ord_m(-1)=2$。

- 例 设m为正整数，$m > 1$，则$ord_m(1) = 1, ord_m(-1) = 2$。

- 例 计算$2^{23456}\ (mod\ 7)$

解：易知$ord_7(2) = 3$，且$23456 = 7818 \times 3 + 2$，因此
$2^{23456} \equiv (2^3)^{7818} \cdot 2^2 \equiv 4\ (mod\ 7)$

- 例 计算$ord_{11}(a)$，其中$a = 1,2, \ldots, 10$

- 例 计算$ord_{11}(a)$，其中$a = 1,2,\dots,10$

解：

	a=1	a=2	a=3	a=4	a=5	a=6	a=7	a=8	a=9	a=10
a^1(mod 11)	1	2	3	4	5	6	7	8	9	10
a^2(mod 11)		4	9	5	3	3	5	9	4	1
a^3(mod 11)		8	5	9	4	7	2	6	3	
a^4(mod 11)		5	4	3	9	9	3	4	5	
a^5(mod 11)		10	1	1	1	10	10	10	1	
a^6(mod 11)		9				5	4	3		
a^7(mod 11)		7				8	6	2		
a^8(mod 11)		3				4	9	5		
a^9(mod 11)		6				2	8	7		
a^{10}(mod 11)		1				1	1	1		

- 例 计算$ord_{11}(a)$，其中$a = 1,2,\ldots,10$

解：

	a=1	a=2	a=3	a=4	a=5	a=6	a=7	a=8	a=9	a=10
a^1(mod 11)	1	2	3	4	5	6	7	8	9	10
a^2(mod 11)		4	9	5	3	3	5	9	4	1
a^3(mod 11)		8	5	9	4	7	2	6	3	
a^4(mod 11)		5	4	3	9	9	3	4	5	
a^5(mod 11)		10	1	1	1	10	10	10	1	
a^6(mod 11)		9				5	4	3		
a^7(mod 11)		7				8	6	2		
a^8(mod 11)		3				4	9	5		
a^9(mod 11)		6				2	8	7		
a^{10}(mod 11)		1				1	1	1		

可见模11的次数可能为1,2,5,10，都是$10 = \varphi(11)$的因数。

- 定理4.1.1 设$m, a \in Z^{+}, m > 1, n \in Z, (a, m) = 1$，那么$a^{n} \equiv 1 \ (mod\ m)$的充要条件是$ord_{m}(a) | n$。

- 定理4.1.1　设$m,a\in Z^+,m>1,n\in Z,(a,m)=1$，那么$a^n\equiv 1\ (mod\ m)$的充要条件是$ord_m(a)|n$。

证明：令$d=ord_m(a)$，则存在$q,r\in Z,0\le r<d$，使得$n=qd+r$。

先证充分性：因为$d|n$，则$r=0$，即$n=qd$，有$a^n=(a^d)^q\equiv 1^q=1\ (mod\ m)$。

再证必要性：因为$1\equiv a^n=\left(a^d\right)^q\cdot a^r\equiv 1^q\cdot a^r=a^r\ (mod\ m)$，但$d$是$a$模$m$的次数，且$0\le r<d$，因此$r=0$，即$d|n$。

- 推论　设 $m, a \in Z^+, m > 1, (a, m) = 1$，那么 $ord_m(a) | \varphi(m)$。

- 推论　设 $m, a \in Z^+, m > 1, (a, m) = 1$，那么 $ord_m(a) | \varphi(m)$。

- 计算 $ord_m(a)$ 时，仅需在 $\varphi(m)$ 的因子中验证是否满足(4.1)。

- 例 求5模17的次数

- 例 求5模17的次数

解：因为$\varphi(17)=16$的因子为1,2,4,8,16，计算

$5^1 \equiv 5\ (mod\ 17), 5^2 \equiv 8\ (mod\ 17), 5^4 \equiv 13\ (mod\ 17),$

$5^8 \equiv -1\ (mod\ 17), 5^{16} \equiv 1\ (mod\ 17),$

因此$ord_{17}(5)=16$，即5是模17的原根。

- 定理4.1.2 设$m, a \in Z^{+}, m > 1, (a, m) = 1$，那么

(i) 若$b \equiv a \ (mod\ m)$，则$ord_m(b) = ord_m(a)$,
(ii) 设a^{-1}为使$a^{-1}a \equiv 1 \ (mod\ m)$成立的正整数，则
$ord_m(a^{-1}) = ord_m(a)$。

- 例 求39和7模17的次数

- 例 求39和7模17的次数

解：因为$39 \equiv 5 \ (mod\ 17), 7 \cdot 5 \equiv 1 \ (mod\ 17)$，因此$ord_{17}(39) = ord_{17}(7) = ord_{17}(5) = 16$，即39和7都是模17的原根。

- 定理4.1.3　设$m, a \in Z^{+}, m > 1, (a, m) = 1$，那么$a^{1}, a^{2}, \dots, a^{ord_m(a)}$模$m$两两不同余。

- 定理4.1.3 设$m, a \in Z^+, m > 1, (a, m) = 1$，那么$a^1, a^2, \dots, a^{ord_m(a)}$模$m$两两不同余。

证明：用反证法，设$a^1, a^2, \dots, a^{ord_m(a)}$并非模$m$两两不同余，则存在$1 \le i < j \le ord_m(a)$，使得$a^i \equiv a^j \pmod m$，因此$m | \left(a^j - a^i\right) = a^i(a^{j-i} - 1)$，又因为$(a, m) = 1$，所以$m | (a^{j-i} - 1)$，即$a^{j-i} \equiv 1 \pmod m$，但$0 < j - i < ord_m(a)$，与$ord_m(a)$是$a$模$m$的次数矛盾，故定理得证。

- 定理4.1.4 设$m, a \in Z^{+}, m > 1, (a, m) = 1$，那么$a$是模$m$的原根的充要条件是$a^{1}, a^{2}, \dots, a^{\varphi(m)}$构成一个模$m$的简化剩余系。

- 定理4.1.4 设$m, a \in Z^+, m > 1, (a, m) = 1$，那么$a$是模$m$的原根的充要条件是$a^1, a^2, \dots, a^{\varphi(m)}$构成一个模$m$的简化剩余系。

证明：先证必要性，因为a是模m的原根，由定理4.1.3可知$a^1, a^2, \dots, a^{\varphi(m)}$模$m$两两不同余，又由定理2.2.6可知它们构成一个模$m$的简化剩余系。

- 定理4.1.4 设$m, a \in Z^+, m > 1, (a, m) = 1$，那么$a$是模$m$的原根的充要条件是 $a^1, a^2, \dots, a^{\varphi(m)}$ 构成一个模 m 的简化剩余系。

证明：先证必要性，因为a是模m的原根，由定理4.1.3可知$a^1, a^2, \dots, a^{\varphi(m)}$模$m$两两不同余，又由定理2.2.6可知它们构成一个模$m$的简化剩余系。

再证充分性，因为$a^1, a^2, \dots, a^{\varphi(m)}$是模$m$的简化剩余系，因此它们模$m$两两不同余，又由欧拉定理知$a^{\varphi(m)} \equiv 1 \ (mod\ m)$，因此小于 $\varphi(m)$ 的所有正整数都不满足同余式 $a^n \equiv 1 \ (mod\ m)$，因此$\varphi(m)$是a模m的次数，即a是模m的原根。

- 例 因为5是模17的原根，所以$\{5^k|k=1,2,\dots,16\}$构成了模17的一个简化剩余系。具体来说，有
$5^1\equiv 5\ (mod\ 17), 5^2\equiv 8\ (mod\ 17), 5^3\equiv 6\ (mod\ 17),$
$5^4\equiv 13\ (mod\ 17), 5^5\equiv 14\ (mod\ 17), 5^6\equiv 2\ (mod\ 17),$
$5^7\equiv 10\ (mod\ 17), 5^8\equiv 16\ (mod\ 17), 5^9\equiv 12\ (mod\ 17),$
$5^{10}\equiv 9\ (mod\ 17), 5^{11}\equiv 11\ (mod\ 17), 5^{12}\equiv 4\ (mod\ 17),$
$5^{13}\equiv 3\ (mod\ 17), 5^{14}\equiv 15\ (mod\ 17), 5^{15}\equiv 7\ (mod\ 17),$
$5^{16}\equiv 1\ (mod\ 17).$

如表所示：

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5^k	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

- 定理4.1.5 设$m, a \in Z^+, m > 1, (a, m) = 1, k, d \in Z, k, d \geq 0$，则$a^d \equiv a^k \ (mod\ m)$的充要条件是$d \equiv k \ (mod\ ord_m(a))$。

- 定理4.1.5 设$m, a \in Z^+, m > 1, (a, m) = 1, k, d \in Z, k, d \geq 0$，则$a^d \equiv a^k \ (mod\ m)$的充要条件是$d \equiv k \ (mod\ ord_m(a))$。

证明：先证充分性，因为$d \equiv k \ (mod\ ord_m(a))$，不妨设$d \geq k$，因此存在非负整数$q$，使得$d = k + q \cdot ord_m(a)$，此时有$a^d = a^k \cdot \left(a^{ord_m(a)}\right)^q \equiv a^k \cdot 1 = a^k \ (mod\ m)$。

華東師範大學
EAST CHINA NORMAL UNIVERSITY

- 定理4.1.5 设$m,a \in Z^+, m > 1, (a,m) = 1, k,d \in Z, k,d \geq 0$，则$a^d \equiv a^k \pmod{m}$的充要条件是$d \equiv k \pmod{ord_m(a)}$。

证明：先证充分性，因为$d \equiv k \pmod{ord_m(a)}$，不妨设$d \geq k$，因此存在非负整数$q$，使得$d = k + q \cdot ord_m(a)$，此时有$a^d = a^k \cdot \left(a^{ord_m(a)}\right)^q \equiv a^k \cdot 1 = a^k \pmod{m}$。

再证必要性，仍设$d \geq k$，则存在非负整数$q, r, r < ord_m(a)$，使得$d - k = q \cdot ord_m(a) + r$，则$a^k \equiv a^d = a^k \cdot a^r \cdot \left(a^{ord_m(a)}\right)^q \equiv a^k \cdot a^r \pmod{m}$，因此$m | a^k(a^r - 1)$，又因为$(a,m) = 1$，所以$\left(a^k, m\right) = 1$，所以$m | (a^r - 1)$，即$a^r \equiv 1 \pmod{m}$，则由$ord_m(a)$定义及$0 \leq r < ord_m(a)$可知$r = 0$，即$d \equiv k \pmod{ord_m(a)}$。

- 例 计算$2^{23456}\ (mod\ 7)$

解：由于$ord_7(2)=3$，且$23456\equiv 2\ (mod\ 3)$，因此
$2^{23456}\equiv 2^2\equiv 4\ (mod\ 7)$。

- 定理4.1.6 设$m, a \in Z^{+}, m > 1, (a, m) = 1, d$为非负整数，则$ord_m(a^d) = \frac{ord_m(a)}{(ord_m(a), d)}$。

- 定理4.1.6 设$m,a\in Z^{+},m>1,(a,m)=1,d$为非负整数，则$ord_m(a^d)=\frac{ord_m(a)}{(ord_m(a),d)}$。

证明：因为$a^{d\cdot ord_m(a^d)}=(a^d)^{ord_m(a^d)}\equiv 1\ (mod\ m)$，由定理4.1.1，我们有$ord_m(a)|d\cdot ord_m(a^d)$，因此$\frac{ord_m(a)}{(ord_m(a),d)}|\frac{d}{(ord_m(a),d)}\cdot ord_m(a^d)$，所以$\frac{ord_m(a)}{(ord_m(a),d)}|ord_m(a^d)$。另一方面因为$(a^d)^{\frac{ord_m(a)}{(ord_m(a),d)}}=a^{d\cdot\frac{ord_m(a)}{(ord_m(a),d)}}=a^{ord_m(a)\cdot\frac{d}{(ord_m(a),d)}}=(a^{ord_m(a)})^{\frac{d}{(ord_m(a),d)}}\equiv 1\ (mod\ m)$，由定理4.1.1可知$ord_m(a^d)|\frac{ord_m(a)}{(ord_m(a),d)}$，因此$ord_m(a^d)=\frac{ord_m(a)}{(ord_m(a),d)}$。

- 例 由前例，模11的次数如下表所示，则$ord_{11}(4) = ord_{11}(2^2) = \frac{ord_{11}(2)}{(ord_{11}(2),2)} = \frac{10}{(10,2)} = 5$，$ord_{11}(3) = ord_{11}(25) = ord_{11}(5^2) = \frac{ord_{11}(5)}{(ord_{11}(5),2)} = \frac{5}{(5,2)}$ =5。

	a=1	a=2	a=3	a=4	a=5	a=6	a=7	a=8	a=9	a=10
a^1(mod 11)	1	2	3	4	5	6	7	8	9	10
a^2(mod 11)		4	9	5	3	3	5	9	4	1
a^3(mod 11)		8	5	9	4	7	2	6	3	
a^4(mod 11)		5	4	3	9	9	3	4	5	
a^5(mod 11)		10	1	1	1	10	10	10	1	
a^6(mod 11)		9				5	4	3		
a^7(mod 11)		7				8	6	2		
a^8(mod 11)		3				4	9	5		
a^9(mod 11)		6				2	8	7		
a^{10}(mod 11)		1				1	1	1		

- 推论 设$m, a \in Z^{+}, m > 1$，d为非负整数，a为模m的原根，则a^{d}为模m的原根的充要条件是$(\varphi(m), d)=1$。

- 推论 设$m, a \in Z^+, m > 1$，d为非负整数，a为模m的原根，则a^d为模m的原根的充要条件是$(\varphi(m), d)$=1。

证明，由定理4.1.6可知$ord_m(a^d) = \frac{ord_m(a)}{(ord_m(a),d)} = \frac{\varphi(m)}{(\varphi(m),d)}$，而$a^d$为模$m$的原根，即$ord_m(a^d) = \varphi(m)$当且仅当$(\varphi(m), d)$=1。

- 定理4.1.7 设$m, e \in Z^{+}, m > 1$且模m有原根a，则模m的简化剩余系中次数为e的共有$\varphi(e)$个。特别的，共有$\varphi(\varphi(m))$个模m的原根。

華東師範大學 EAST CHINA NORMAL UNIVERSITY

- 定理4.1.7 设$m, e \in Z^+, m > 1$且模m有原根a，则模m的简化剩余系中次数为e的共有$\varphi(e)$个。特别的，共有$\varphi(\varphi(m))$个模m的原根。

证明：对任意b属于模m的简化剩余系，设b的次数为e，由定理4.1.4可知$a^1, a^2, \ldots, a^{\varphi(m)}$构成一个模$m$的简化剩余系，因此存在整数$d, 1 \le d \le \varphi(m)$，使得 $b \equiv a^d \ (mod\ m)$，所以由定理4.1.6，$e = ord_m(b) = ord_m\left(a^d\right) = \frac{ord_m(a)}{(ord_m(a), d)} = \frac{\varphi(m)}{(\varphi(m), d)}$，即$(\varphi(m), d) = \frac{\varphi(m)}{e}$，令$d' = d \cdot \frac{e}{\varphi(m)} \in Z$，显然$1 \le d' \le e$，且$(e, d') = \left(\frac{\varphi(m)}{(\varphi(m), d)}, \frac{d}{(\varphi(m), d)}\right) = 1$，易知共有$\varphi(e)$个这样的$d'$，故$1, \ldots, \varphi(m)$中共有$\varphi(e)$个$d$满足$\left(e, \frac{d}{(\varphi(m), d)}\right) = 1$，即共有$\varphi(e)$个模$m$的简化剩余系中次数为$e$的数。特别的，令$e = \varphi(m)$，则共有$\varphi(\varphi(m))$个模$m$的原根。

- 例 求模17的所有原根。

- 例 求模17的所有原根。

解：由前例知5是模17的一个原根，又因为$\varphi(17)=16$，因此$5^1,5^3,5^5,5^7,5^9,5^{11},5^{13},5^{15}$是模17的所有原根，查表可知5,6,14,10,12,11,3,7为模17的所有原根。

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5^k	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

- 定理4.1.8 设$m, a \in Z^+, m > 1, (a, m) = 1$，$\varphi(m)$的标准分解式为$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，则$a$是模$m$的原根当且仅当

$$a^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \ (mod\ m) \ \ i = 1,2,\ldots,s$$

- 定理4.1.8 设$m, a \in Z^+, m > 1, (a, m) = 1$，$\varphi(m)$的标准分解式为$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，则$a$是模$m$的原根当且仅当

$$a^{\frac{\varphi(m)}{p_i}} \not\equiv 1\ (mod\ m)\ \ i = 1,2, \ldots, s$$

证明：先证必要性，因为a是模m的一个原根，所以$ord_m(a) = \varphi(m)$，又对任意$i = 1,2, \ldots, s$，显然有$0 < \frac{\varphi(m)}{p_i} < \varphi(m)$，由$ord_m(a)$定义知$a^{\frac{\varphi(m)}{p_i}} \not\equiv 1\ (mod\ m)$。

再证充分性，用反证法，设a不是模m的原根，设a模m的次数为$e < \varphi(m)$，由定理4.1.1得$e|\varphi(m)$，因此$\frac{\varphi(m)}{e} > 1$且为整数，所以存在整数$1 \le j \le s$，使得$p_j | \frac{\varphi(m)}{e}$，因此存在整数$q$，使得$\frac{\varphi(m)}{e} = q \cdot p_j$，所以$\frac{\varphi(m)}{p_j} = qe$，此时有$a^{\frac{\varphi(m)}{p_j}} = a^{qe} = (a^e)^q \equiv 1 \ (mod\ m)$，与假设矛盾。

- 由定理4.1.8和定理4.1.6推论可求模m的所有原根.

- 由定理4.1.8和定理4.1.6推论可求模m的所有原根.

- 例 求模41的所有原根。

- 由定理4.1.8和定理4.1.6推论可求模m的所有原根.

- 例 求模41的所有原根。

解1：$\varphi(41) = 40 = 2^3 \cdot 5$，因此对$a = 2,3,\ldots$，逐个检验$a^8, a^{20}$是否与1模41同余：$2^8 \equiv 10, 2^{20} \equiv 1, 3^8 \equiv 1, 4^8 \equiv 18, 4^{20} \equiv 1, 5^8 \equiv 18, 5^{20} \equiv 1, 6^8 \equiv 10, 6^{20} \equiv 40$，因此6是模41的一个原根，当$d$遍历模$\varphi(41) = 40$的简化剩余系时，$6^d$遍历模41的所有原根，共$\varphi(\varphi(41)) = 16$个：

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

- 定理4.1.9 设$m, a \in Z^{+}, m > 1, (a, m) = 1$， a不是模m的原根，设a模m的次数为d，则a^{k}不是模m的原根，其中$k = 1, 2, \ldots, d$ 。

- 定理4.1.9 设$m, a \in Z^+, m > 1, (a, m) = 1$， a不是模m的原根，设a模m的次数为d，则a^k不是模m的原根，其中$k = 1,2, \dots, d$ 。

证明：因为a不是模m的原根，所以$d < \varphi(m)$，由定理4.1.6可知$ord_m(a^k) = \frac{d}{(k,d)} \le d < \varphi(m)$，因此$a^k$不是模$m$的原根。

- 由定理4.1.9可得求模m的所有原根的另一种方法。
- 例 求模41的所有原根。

- 由定理4.1.9可得求模m的所有原根的另一种方法。

- 例 求模41的所有原根。

解2：列出$1,2,\ldots,\varphi(41)=40$这$\varphi(41)$个数，再对$a=2,3,\ldots$，依次计算其模41的次数，因为$ord_{41}(2)$=20，从上述数列中删去$2^k\ (mod\ 41), k=1,2,\ldots,20$这20个数，计算可得它们是2,4,8,16,32,23,5, 10,20,40,39,37,33,25,9,18,36,31,21,1；再求得$ord_{41}(3)=8$，再删去$3^k\ (mod\ 41), k=1,2,\ldots,8$这8个数，它们分别是3,9,27,40,38,32,14,1；这时数列中还剩6,7,11,12, 13,15,17,19,22,24,26,28,29,30,34,35这16个数，因为$ord_{41}(6)=40=\varphi(41)$，所以6是模41的一个原根，又因为$\varphi\big(\varphi(41)\big)=16$，所以这16个数是模41的所有原根。

- 定理4.1.10 设$m, a, b \in Z^+, m > 1, (a, m) = (b, m) = 1$，则$\left(ord_m(a), ord_m(b)\right) = 1$当且仅当$ord_m(ab) = ord_m(a)ord_m(b)$。

- 定理4.1.10 设$m, a, b \in Z^+, m > 1, (a, m) = (b, m) = 1$， 则$\left(ord_m(a), ord_m(b)\right) = 1$当且仅当$ord_m(ab) = ord_m(a)ord_m(b)$。

证明：先证必要性，$a^{ord_m(b)ord_m(ab)} = (a^{ord_m(b)})^{ord_m(ab)}$. $(1)^{ord_m(ab)} = \left(a^{ord_m(b)}\right)^{ord_m(ab)} \cdot \left(b^{ord_m(b)}\right)^{ord_m(ab)} = \left(ab^{ord_m(b)}\right)^{ord_m(ab)} = \left(ab^{ord_m(ab)}\right)^{ord_m(b)} \equiv 1 \ (mod\ m)$，因此$ord_m(a)|ord_m(b)ord_m(ab)$，$\left(ord_m(a), ord_m(b)\right) = 1$，所以$ord_m(a)|ord_m(ab)$。同理可知$ord_m(b)|ord_m(ab)$，又因为$\left(ord_m(a), ord_m(b)\right) = 1$，故$ord_m(a)ord_m(b)|ord_m(ab)$。

另一方面，$ab^{ord_m(a)ord_m(b)}=\left(a^{ord_m(a)}\right)^{ord_m(b)}\cdot\left(b^{ord_m(b)}\right)^{ord_m(a)}\equiv 1\ (mod\ m)$，因此$ord_m(ab)|ord_m(a)ord_m(b)$，故有$ord_m(ab)=ord_m(a)ord_m(b)$，必要性得证。

再证充分性，$ab^{[ord_m(a),ord_m(b)]}=a^{[ord_m(a),ord_m(b)]}\cdot b^{[ord_m(a),ord_m(b)]}\equiv 1\ (mod\ m)$，因此$ord_m(ab)|[ord_m(a),ord_m(b)]$，又因为$ord_m(ab)=ord_m(a)ord_m(b)$，故$ord_m(a)ord_m(b)|[ord_m(a),ord_m(b)]$，但我们知道$ord_m(a)ord_m(b)=[ord_m(a),ord_m(b)]\cdot\left(ord_m(a),ord_m(b)\right)$，所以有$\left(ord_m(a),ord_m(b)\right)=1$，定理得证。

例 求模71的一个原根。

例 求模71的一个原根。

解：计算2模71的指数为$ord_{71}(2)=35$，且显然有$ord_{71}(-1)=2$，因为$(2,35)=1$，所以$ord_{71}(-2)=ord_{71}(-1)\cdot ord_{71}(2)=2\cdot 35=70=\varphi(71)$，因此$-2$是模71的一个原根。

例 求模71的一个原根。

解：计算2模71的指数为$ord_{71}(2) = 35$，且显然有$ord_{71}(-1) = 2$，因为$(2,35) = 1$，所以$ord_{71}(-2) = ord_{71}(-1) \cdot ord_{71}(2) = 2 \cdot 35 = 70 = \varphi(71)$，因此$-2$是模71的一个原根。

验算：计算$(-2)^{10}, (-2)^{14}, (-2)^{35} \equiv 30,54,-1\ (mod\ 71)$，因此$-2$是模71的一个原根。

- 定理4.1.11 设$m,n,a \in Z^+, m,n > 1, (a,m) = 1$，则

(i) 若$m|n$，那么$ord_m(a)|ord_n(a)$

(ii) 若$(m,n) = 1$，那么$ord_{mn}(a) = [ord_m(a), ord_n(a)]$

- 定理4.1.11 设$m, n, a \in Z^+, m, n > 1, (a, m) = 1$，　则

(i) 若$m|n$，那么$ord_m(a)|ord_n(a)$

(ii) 若$(m, n) = 1$，那么$ord_{mn}(a) = [ord_m(a), ord_n(a)]$

证明：　(i) 因为$a^{ord_n(a)} \equiv 1 \ (mod\ n)$，所以$n|(a^{ord_n(a)} - 1)$，又因为$m|n$，因此$m|(a^{ord_n(a)} - 1)$，即$a^{ord_n(a)} \equiv 1 \ (mod\ m)$，所以$ord_m(a)|ord_n(a)$。

(ii) 显然$a^{[ord_m(a),ord_n(a)]} \equiv 1\ (mod\ m)$, $a^{[ord_m(a),ord_n(a)]} \equiv 1\ (mod\ n)$，因此$m|(a^{[ord_m(a),ord_n(a)]}-1)$, $n|(a^{[ord_m(a),ord_n(a)]}-1)$，又因为$(m,n)=1$，所以 $mn|(a^{[ord_m(a),ord_n(a)]}-1)$，即 $a^{[ord_m(a),ord_n(a)]} \equiv 1\ (mod\ mn)$，所以$ord_{mn}(a)|[ord_m(a),ord_n(a)]$。

另一方面，因为$a^{ord_{mn}(a)} \equiv 1\ (mod\ mn)$，所以有$a^{ord_{mn}(a)} \equiv 1\ (mod\ m)$, $a^{ord_{mn}(a)} \equiv 1\ (mod\ n)$，所以$ord_m(a)|ord_{mn}(a)$, $ord_n(a)|ord_{mn}(a)$，因此$[ord_m(a),ord_n(a)]|ord_{mn}(a)$，所以有$ord_{mn}(a)=[ord_m(a),ord_n(a)]$。

例 求$ord_{28}(3)$

例 求$ord_{28}(3)$

解1：因为$\varphi(28)=12$，因此令$n=1,2,3,4,6,12$，分别计算$3^n\ (mod\ 28)$，第一个满足式(4.1)的$n=6$，即为所求。

例 求$ord_{28}(3)$

解1：因为$\varphi(28) = 12$，因此令$n = 1,2,3,4,6,12$，分别计算$3^n \ (mod\ 28)$，第一个满足式(4.1)的$n = 6$，即为所求。

解2：易求$ord_4(3) = 2, ord_7(3) = 6$，因此由定理4.1.11可知$ord_{28}(3) = [ord_4(3), ord_7(3)] = 6$。

- 推论 设p,q是不相同的素数，a是正整数，则$ord_{pq}(a) = [ord_p(a), ord_q(a)]$。

例 设p,q是不相同的素数，$a,e\in Z^+,n=pq$，$(a,n)=1,1\leq e<\varphi(n),\left(e,\varphi(n)\right)=1$，则存在$d\in Z,1\leq d<ord_n(a)$，使得$ed\equiv 1\ (mod\ ord_n(a))$。而且若令$c=a^e\ (mod\ n)$，有$c^d\equiv a\ (mod\ n)$。

华东师范大学
EAST CHINA NORMAL UNIVERSITY

例 设p,q是不相同的素数，$a,e\in Z^+,n=pq$，$(a,n)=1,1\le e<\varphi(n),\big(e,\varphi(n)\big)=1$，则存在$d\in Z,1\le d<ord_n(a)$，使得$ed\equiv 1\ (mod\ ord_n(a))$。而且若令$c=a^e\ (mod\ n)$，有$c^d\equiv a\ (mod\ n)$。

证明：因为$(a,n)=1$，所以$a^{\varphi(n)}\equiv 1\ (mod\ n)$，因此$ord_n(a)|\varphi(n)$，又因为$\big(e,\varphi(n)\big)=1$，所以$\big(e,ord_n(a)\big)=1$，故由辗转相除法，存在$d,s\in Z,1\le d<ord_n(a)$，使得$ed+ord_n(a)\cdot s=1$，即$ed\equiv 1\ (mod\ ord_n(a))$。

因为$a^{ord_n(a)}\equiv 1\ (mod\ n)$，所以$a^{-ord_n(a)\cdot s}=(a^{ord_n(a)})^{-s}\equiv 1\ (mod\ n)$，此时$c^d=a^{ed}=a^{1-ord_n(a)\cdot s}=a\cdot a^{-ord_n(a)\cdot s}\equiv a\ (mod\ n)$。

- 推论 设$m,a\in Z^{+},(a,m)=1$，m的标准分解式为$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则$ord_m(a)=[ord_{p_1^{\alpha_1}}(a),ord_{p_2^{\alpha_2}}(a),\ldots,ord_{p_s^{\alpha_s}}(a)]$。

- 定理4.1.12 设$m,n\in Z^+,(m,n)=1$，则对与mn互素的整数a_1,a_2，都存在整数a，使得$ord_{mn}(a)=[ord_m(a_1),ord_n(a_2)]$。

- 定理4.1.12 设$m,n \in Z^+, (m,n)=1$，则对与mn互素的整数a_1,a_2，都存在整数a，使得$ord_{mn}(a)=[ord_m(a_1),ord_n(a_2)]$。

证明：考虑同余式组$\begin{cases} x \equiv a_1 \ (mod\ m) \\ x \equiv a_2 \ (mod\ n) \end{cases}$，因为$(m,n)=1$，由孙子定理可知它有唯一解，令其为$x \equiv a\ (mod\ mn)$，则由阶的性质可知$ord_m(a_1)=ord_m(a), ord_n(a_2)=ord_n(a)$，且由定理4.1.11可知$ord_{mn}(a)=[ord_m(a),ord_n(a)]=[ord_m(a_1),ord_n(a_2)]$。

- 定理4.1.13 设$m, a, b \in Z^+, (a, m) = (b, m) = 1$，则存在$c \in Z^+$，使得$ord_m(c) = [ord_m(a), ord_m(b)]$。

- 定理4.1.13 设$m,a,b\in Z^+,(a,m)=(b,m)=1$，则存在$c\in Z^+$，使得$ord_m(c)=[ord_m(a),ord_m(b)]$。

证明：设$ord_m(a)=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},ord_m(b)=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，其中$\alpha_i\ge\beta_i\ge 0\ (i=1,2,\ldots,l),\beta_i>\alpha_i\ge 0\ (i=l+1,l+2,\ldots,n)$，令$u=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}\in Z^+,v=p_{l+1}^{\beta_{l+1}}p_{l+2}^{\beta_{l+2}}\cdots p_n^{\beta_n}\in Z^+$，则$(u,v)=1,u|ord_m(a),v|ord_m(b),[ord_m(a),ord_m(b)]=uv$，再令$s=\frac{ord_m(a)}{u}\in Z^+,t=\frac{ord_m(b)}{v}\in Z^+,c=a^sb^t\in Z^+$，则由定理4.1.6可知$ord_m(a^s)=\frac{ord_m(a)}{(ord_m(a),s)}=\frac{ord_m(a)}{s}=u$，同理可知$ord_m(b^t)=v$，再由定理4.1.10，因为$(u,v)=1$，因此$ord_m(c)=ord_m(a^sb^t)=ord_m(a^s)ord_m(b^t)=uv=[ord_m(a),ord_m(b)]$。

§4.2 原根存在的条件

- 定理4.2.1 设$m \in Z^+$，则模m有原根当且仅当$m = 2,4,p^\alpha,2p^\alpha$，其中$p$为奇素数，$\alpha \in Z^+$。

§4.2 原根存在的条件

- 定理4.2.1 设$m \in Z^+$，则模m有原根当且仅当$m = 2,4,p^\alpha,2p^\alpha$，其中$p$为奇素数，$\alpha \in Z^+$。

- 例 1是模2的原根，3是模4的原根，5是模6的原根，2是模9的原根。

§4.2 原根存在的条件

- 定理4.2.1 设$m \in Z^+$，则模m有原根当且仅当$m = 2,4,p^\alpha,2p^\alpha$，其中$p$为奇素数，$\alpha \in Z^+$。

- 例 1是模2的原根，3是模4的原根，3是模5的原根，2是模9的原根。

- 例 模8无原根，模15无原根。

- 定理4.2.2 设p为奇素数，则存在模p的原根。

- 定理4.2.2 设p为奇素数，则存在模p的原根。

证明：令$e = [ord_p(1), ord_p(2), \dots, ord_p(p-1)]$，则由定理4.1.13，存在$g \in Z^+$，使得$ord_p(g) = e$，由定理4.1.1推论可知$e|\varphi(p)$。另一方面，对$a = 1,2,\dots,p-1$，都有$a^e = a^{[ord_p(1), ord_p(2),\dots,ord_p(p-1)]} = (a^{ord_p(a)})^{k_a} \equiv 1^{k_a} = 1 \ (mod\ p)$，其中$k_a = \frac{[ord_p(1), ord_p(2),\dots,ord_p(p-1)]}{ord_p(a)} \in Z^+$，因此同余式$x^e \equiv 1 \ (mod\ p\ )$至少有$p-1$个解，因此$e \geq p - 1 = \varphi(p)$，故$e = p - 1$，即$g$为模$p$的原根。

- 定理4.2.3 设p为奇素数，g为模p的原根，则g和$(g+p)$中必有一个是模p^2的原根。

- 定理4.2.3 设p为奇素数，g为模p的原根，则g和$(g+p)$中必有一个是模p^2的原根。

证明：显然 $ord_p(g+p)=ord_p(g)=p-1$ ，因此由定理4.1.11，有 $(p-1)|ord_{p^2}(g)$，又因为$ord_{p^2}(g)|\varphi(p^2)=p(p-1)$，因此$ord_{p^2}(g)=p-1$或$p(p-1)$，同理可知$ord_{p^2}(g+p)=p-1$或$p(p-1)$。若$ord_{p^2}(g)=p(p-1)$，则$g$即为模$p^2$的原根。若$ord_{p^2}(g)\neq p(p-1)$，则有$ord_{p^2}(g)=p-1$，因此$g^{p-1}\equiv 1\ (mod\ p^2)$，由于$(g,p)=1$，此时$(g+p)^{p-1}\equiv g^{p-1}+(p-1)pg^{p-2}\equiv 1-pg^{p-2}\not\equiv 1\ (mod\ p^2)$，即$ord_{p^2}(g+p)\neq p-1$，所以$ord_{p^2}(g+p)=p(p-1)$，即$(g+p)$是模$p^2$的原根。

- 例 求模1681的所有原根。

- 例 求模1681的所有原根。

解：因为$1681 = 41^2$，再由前例知6是模41的一个原根，则由定理4.2.3可知6或者$6 + 41 = 47$中满足$x^{40} \not\equiv 1\ (mod\ 41^2)$的是模$41^2$的原根，易求$6^{40} \equiv 143 \not\equiv 1\ (mod\ 41^2), 47^{40} \equiv 1518 \not\equiv 1\ (mod\ 41^2)$，因此6和47都是模1681的原根。

当d遍历模$\varphi(1681)$的简化剩余系时，6^d遍历模1681的所有原根，共$\varphi\big(\varphi(1681)\big) = 640$个。

- 定理4.2.4 设p为奇素数，$\alpha \geq 2$，g为模p^2的原根，则g是模p^α的原根。

- 定理4.2.4 设p为奇素数，$\alpha \geq 2$，g为模p^2的原根，则g是模p^α的原根。

证明：首先我们证明对$\alpha \geq 2$，都存在$u_\alpha \in Z, p \nmid u_\alpha$，使得$g^{p^{\alpha-2}(p-1)} = u_\alpha p^{\alpha-1} + 1$。事实上，当$\alpha = 2$时，由定理4.2.3证明可知$g^{p-1} \equiv 1 \ (mod\ p)$且$g^{p-1} \not\equiv 1 \ (mod\ p^2)$，结论成立。设当$\alpha = k \geq 2$时，结论成立，即$g^{p^{k-2}(p-1)} = u_k p^{k-1} + 1$且$p \nmid u_k$，两边取$p$次方得

$$g^{p^{k-1}(p-1)} = 1 + u_k p^k + u p^{k+1} \quad (*)$$

其中$u \in Z$，令$u_{k+1} = u_k + up$，则有$g^{p^{k-1}(p-1)} = 1 + u_{k+1} p^k$且$p \nmid u_{k+1}$，结论成立。

设$ord_{p^\alpha}(g)=d$，则有$d|\varphi(p^\alpha)=p^{\alpha-1}(p-1)$且$g^d\equiv 1\ (mod\ p^\alpha)$，因此$g^d\equiv 1\ (mod\ p^2)$，所以$p(p-1)=ord_{p^2}(g)|d$，所以存在$r\in Z, 2\le r\le\alpha$，使得$d=p^{r-1}(p-1)$，由(*)式可知，$u_{r+1}p^r+1=g^{p^{r-1}(p-1)}\equiv 1\ (mod\ p^\alpha)$，其中$u_{r+1}\in Z, p\nmid u_{r+1}$，即$u_{r+1}p^r\equiv 0\ (mod\ p^\alpha)$，又因为$p\nmid u_{r+1}$，因此$r\ge\alpha$，故$r=\alpha$，即$g$是模$p^\alpha$的原根。

- 例 求模2825761的一个原根。

- 例 求模2825761的一个原根。

解：因为$2825761 = 41^4$，且由前例知6和47都是模41^2的原根，则由定理4.2.4可知，它们也都是模41^4的原根，即6和47都是模2825761的原根。

- 定理4.2.5 设p为奇素数，$\alpha \geq 2$，g为模p^{α}的原根，则g和$(g+p^{\alpha})$中必有一个是模$2p^{\alpha}$的原根。

- 定理4.2.5 设p为奇素数，$\alpha \geq 2$，g为模p^α的原根，则g和$(g+p^\alpha)$中必有一个是模$2p^\alpha$的原根。

证明：因为p为奇素数，所以g和$(g+p^\alpha)$中有且仅有一个奇数，令其为a，由于g为模p^α的原根，故$(g,p)=1$且$ord_{p^\alpha}(g)=ord_{p^\alpha}(g+p^\alpha)=d=\varphi(p^\alpha)$，因此$ord_{p^\alpha}(a)=d$，又因为$a$是奇数，所以$(a,2p^\alpha)=1$， 由定理4.1.11可知$d=ord_{p^\alpha}(a)|ord_{2p^\alpha}(a)$，又因为$ord_{2p^\alpha}(a)|\varphi(2p^\alpha)=\varphi(2)\varphi(p^\alpha)=d$，因此$ord_{2p^\alpha}(a)=d$，即$a$是模$2p^\alpha$的原根。

- 例 求模5651522的一个原根。

- 例 求模5651522的一个原根。

解：因为$5651522 = 2 \cdot 41^4$，由前例知6和47都是模41^4的原根，则由定理4.2.5可知，47和$6 + 41^4 = 2825767$都是模5651522的原根。

- 定理4.2.6 设a为奇数，$\alpha \geq 3$，则$a^{\frac{\varphi(2^{\alpha})}{2}} = a^{2^{\alpha-2}} \equiv 1 \ (mod\ 2^{\alpha})$。

- 定理4.2.6 设a为奇数，$\alpha \geq 3$，则$a^{\frac{\varphi(2^{\alpha})}{2}} = a^{2^{\alpha-2}} \equiv 1\ (mod\ 2^{\alpha})$。

证明：用数学归纳法。当$\alpha = 3$时，因为a为奇数，则存在整数k，使得$a = 2k + 1$，所以$a^{2^{\alpha-2}} = a^2 = (2k + 1)^2 = 4k(k + 1) + 1 \equiv 1\ (mod\ 2^3)$。设当$\alpha = s \geq 3$时，结论成立，即$a^{2^{s-2}} \equiv 1\ (mod\ 2^s)$，则存在整数$u_s$，使得$a^{2^{s-2}} = 1 + u_s \cdot 2^s$，当$\alpha = s + 1$时，$a^{2^{s-1}} = (a^{2^{s-2}})^2 = (1 + u_s \cdot 2^s)^2 = 1 + u_s \cdot 2^{s+1} + 2^{2s} \equiv 1\ (mod\ 2^{s+1})$，结论成立。

定理4.2.1的证明：先证充分性，由定理4.2.2-4.2.5可知，$m = p^{\alpha}, 2p^{\alpha}, \alpha \geq 1$时，存在模$m$的原根，再由前例知，1是模2的原根，3是模4的原根，故当$m = 2,4, p^{\alpha}, 2p^{\alpha}$，存在模$m$ 的原根。

再证必要性，设m的标准分解式为$m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，其中$s, \alpha \geq 0, \alpha_1, \alpha_2 \ldots, \alpha_s \geq 1$，对任意与$m$互素的整数$a$，由欧拉定理可知$a^{\varphi(p_i^{\alpha_i})} \equiv 1 \left(mod\ p_i^{\alpha_i}\right)$，其中$i = 1,2, \ldots, s$，且$a^{\varphi(2)} \equiv 1\ (mod\ 2), a^{\varphi(4)} \equiv 1\ (mod\ 4)$，再由定理4.2.6知，当$\alpha \geq 3$时，$a^{\frac{\varphi(2^{\alpha})}{2}} \equiv 1\ (mod\ 2^{\alpha})$，令$\tau = \begin{cases} \varphi(2^{\alpha}) & \alpha = 1,2 \\ \frac{\varphi(2^{\alpha})}{2} & \alpha \geq 3 \end{cases}$，则有$a^{\tau} \equiv 1\ (mod\ 2^{\alpha})$，

令$e=[\tau,\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})]$，则显然有

$$\begin{cases} a^e\equiv 1\ (mod\ 2^{\alpha}) \\ a^e\equiv 1\ (mod\ p_1^{\alpha_1}) \\ a^e\equiv 1\ (mod\ p_2^{\alpha_2}) \\ \vdots \\ a^e\equiv 1\ (mod\ p_s^{\alpha_s}) \end{cases}$$

因此$a^e\equiv 1\ (mod\ m)$，所以有$ord_m(a)|e$，因为存在模m 的原根，故必存在 a 使得 $ord_m(a)=\varphi(m)=\varphi(2^{\alpha})\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_s^{\alpha_s})$，所以$\tau,\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})$两两互素且$\tau=\varphi(2^{\alpha})$，由$\tau=\varphi(2^{\alpha})$可知$\alpha\le 2$，另一方面，若$s\ge 2$，因为$2|\varphi(p_1^{\alpha_1}),2|\varphi(p_2^{\alpha_2})$，所以$\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2})$不互素，故$s\le 1$，当$s=1,\alpha=2$时，因为$2|\varphi(p_1^{\alpha_1}),2|\varphi(2^{\alpha})=2$，因此$\varphi(p_1^{\alpha_1}),\varphi(2^{\alpha})$不互素，故$m$只可能有$2^1,2^2,2^0\cdot p_1^{\alpha_1},2^1\cdot p_1^{\alpha_1}$这4种情形，必要性得证。