§4.3 指数与n次剩余

- 现在我们来研究同余式$x^n \equiv a \pmod{m}$，其中$m > 1, (a,m) = 1$。

- 定义4.3.1 设$m, a \in Z, m > 1, a \geq 1, (a,m) = 1$，$g$是模$m$的一个原根，则存在且仅存在一个$r \in Z, 0 \leq r < \varphi(m)$，使得$g^r \equiv a \pmod{m}$，该整数$r$称为以$g$为底的$a$对模$m$的指数，记作$ind_g(a)$（或$ind(a)$），有时也将指数称为离散对数。

- 例 作模41的指数表

- 例 作模41的指数表

解：由前例可知6是模41的原根，对$i = 0,1, \ldots, \varphi(41) - 1 = 39$，计算$6^i \ (mod\ 41)$可得

$6^0 \equiv 1, 6^1 \equiv 6, 6^2 \equiv 36, 6^3 \equiv 11, 6^4 \equiv 25, 6^5 \equiv 27, 6^6 \equiv 39, 6^7 \equiv 29, 6^8 \equiv 10, 6^9 \equiv 19, 6^{10} \equiv 32, 6^{11} \equiv 28, 6^{12} \equiv 4, 6^{13} \equiv 24, 6^{14} \equiv 21, 6^{15} \equiv 3, 6^{16} \equiv 18, 6^{17} \equiv 26, 6^{18} \equiv 33, 6^{19} \equiv 34, 6^{20} \equiv 40,$
$6^{21} \equiv 35, 6^{22} \equiv 5, 6^{23} \equiv 30, 6^{24} \equiv 16, 6^{25} \equiv 14, 6^{26} \equiv 2, 6^{27} \equiv 12,$
$6^{28} \equiv 31, 6^{29} \equiv 22, 6^{30} \equiv 9, 6^{31} \equiv 13, 6^{32} \equiv 37, 6^{33} \equiv 17, 6^{34} \equiv 20, 6^{35} \equiv 38, 6^{36} \equiv 23, 6^{37} \equiv 15, 6^{38} \equiv 8, 6^{39} \equiv 7$，

由此可得模41的指数表

	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

即$ind_6(1)=0, ind_6(2)=26, ind_6(2)=15, ind_6(3)=15,\ ind_6(4)=12,$
$ind_6(5)=22, ind_6(6)=1, ind_6(7)=39, ind_6(8)=38, ind_6(9)=30,$
$ind_6(10)=8, ind_6(11)=3, ind_6(12)=27,\ ind_6(13)=31, ind_6(14)=25,$
$ind_6(15)=37, ind_6(16)=24, ind_6(17)=33, ind_6(18)=16, ind_6(19)=9,$
$ind_6(20)=34,\ ind_6(21)=14, ind_6(22)=29, ind_6(23)=36, ind_6(24)=13,$
$ind_6(25)=4, ind_6(26)=17, ind_6(27)=5, ind_6(28)=11, ind_6(29)=7,$
$ind_6(30)=23, ind_6(31)=28, ind_6(32)=10, ind_6(33)=18, ind_6(34)=19,$
$ind_6(35)=21, ind_6(36)=2, ind_6(37)=32, ind_6(38)=35, ind_6(39)=6,$
$ind_6(40)=20$。

- 定理4.3.1 设$m, a \in Z, m > 1, a \geq 1, (a, m) = 1$，$g$是模$m$的一个原根，若存在$r \in Z$，使得$g^r \equiv a \ (mod\ m)$，则$r \equiv ind_g(a) (mod\ \varphi(m))$

- 定理4.3.1 设$m, a \in Z, m > 1, a \geq 1, (a, m) = 1$，$g$是模$m$的一个原根，若存在$r \in Z$，使得$g^r \equiv a\ (mod\ m)$，则$r \equiv ind_g(a)(mod\ \varphi(m))$

证明：由指数定义可知$g^{ind_g(a)} \equiv a \equiv g^r (mod\ m)$，两边同乘以$g^{\varphi(m)-ind_g(a)}$可得$1 \equiv g^{\varphi(m)} \equiv g^{r+\varphi(m)-ind_g(a)}\ (mod\ m)$，因为$g$是模$m$的原根，由定理4.1.1知$\varphi(m) = ord_m(g) | (r + \varphi(m) - ind_g(a))$，即$r - ind_g(a) \equiv 0\ (mod\ \varphi(m))$。

- 定理4.3.2 设$m, r \in Z, m > 1, 0 \leq r < \varphi(m)$，$g$是模$m$的一个原根，则以$g$为底的对模$m$的指数为$r$的所有整数构成模$m$的一个简化剩余类。

- 定理4.3.2 设$m, r \in Z, m > 1, 0 \leq r < \varphi(m)$，$g$是模$m$的一个原根，则以$g$为底的对模$m$的指数为$r$的所有整数构成模$m$的一个简化剩余类。

证明：令$A = \{a \in Z | ind_g(a) = r\}$，则显然有$g^r \in A$，即$A$非空。对任意$a, b \in A$，由指数定义可得$g^r \equiv a \ (mod\ m), g^r \equiv b \ (mod\ m)$，因此有$a \equiv b \ (mod\ m)$，另一方面，若$b \in A$，对任意整数$a$满足$a \equiv b \ (mod\ m)$，则有$g^r \equiv a \ (mod\ m)$，因此$ind_g(a) = r$，故$a \in A$，因此$A$是模$m$的一个剩余类。又因为$g$是模$m$的一个原根，因此$(g, m) = 1$，所以$(g^r, m) = 1$，故$A$是模$m$的一个简化剩余类。

- 定理4.3.3 设$m,n,a_i \in Z, m>1, n\geq 1, (a_i,m)=1, i=1,2,\ldots,n$，$g$是模$m$的一个原根，则$ind_g(a_1a_2\cdots a_n) \equiv ind_g(a_1)+ind_g(a_2)+\cdots+ind_g(a_n)\ (mod\ \varphi(m))$。

- 定理4.3.3 设$m, n, a_i \in Z, m > 1, n \geq 1, (a_i, m) = 1, i = 1,2, \ldots, n$，$g$是模$m$的一个原根，则$ind_g(a_1 a_2 \cdots a_n) \equiv ind_g(a_1) + ind_g(a_2) + \cdots + ind_g(a_n) \ (mod\ \varphi(m))$。

证明：对$i = 1,2, \ldots, n$，令$r_i = ind_g(a_i)$，则有$a_i \equiv g^{r_i} \ (mod\ m)$，因此$a_1 a_2 \cdots a_n \equiv g^{r_1 + r_2 + \cdots + r_n} \ (mod\ m)$，则由定理4.3.1，$r_1 + r_2 + \cdots + r_n \equiv ind_g(a_1 a_2 \cdots a_n) \ (mod\ \varphi(m))$，定理得证。

- 定理4.3.3 设$m, n, a_i \in Z, m > 1, n \geq 1, (a_i, m) = 1, i = 1,2, \ldots, n$，$g$是模$m$的一个原根，则$ind_g(a_1 a_2 \cdots a_n) \equiv ind_g(a_1) + ind_g(a_2) + \cdots + ind_g(a_n) \ (mod\ \varphi(m))$。

证明：对$i = 1,2, \ldots, n$，令$r_i = ind_g(a_i)$，则有$a_i \equiv g^{r_i} \ (mod\ m)$，因此$a_1 a_2 \cdots a_n \equiv g^{r_1 + r_2 + \cdots + r_n} \ (mod\ m)$，则由定理4.3.1，$r_1 + r_2 + \cdots + r_n \equiv ind_g(a_1 a_2 \cdots a_n) \ (mod\ \varphi(m))$，定理得证。

- 推论 设$m, n, a \in Z, m > 1, n \geq 1, (a, m) = 1$，$g$是模$m$的一个原根，则$ind_g(a^n) \equiv n \cdot ind_g(a) \ (mod\ \varphi(m))$。

- 定义4.3.2 设$m, n, a \in Z, m, n > 1, (a, m) = 1$，若同余式$x^n \equiv a \ (mod\ m)$有解，则称$a$为模$m$的$n$次剩余，否则称$a$为模$m$的$n$次非剩余。

- 定理4.3.4 设$m,n,a\in Z,m,n>1,(a,m)=1$，g是模m的一个原根，则同余式$x^n\equiv a\ (mod\ m)$有解当且仅当$\big(n,\varphi(m)\big)|ind_g(a)$，若有解，其解数为$\big(n,\varphi(m)\big)$。

- 定理4.3.4 设$m,n,a\in Z,m,n>1,(a,m)=1$，g是模m的一个原根，则同余式$x^n\equiv a\ (mod\ m)$有解当且仅当$\big(n,\varphi(m)\big)|ind_g(a)$，若有解，其解数为$\big(n,\varphi(m)\big)$。

证明：先证必要性，设$x\equiv x_0\ (mod\ m)$为同余式$x^n\equiv a\ (mod\ m)$的解，则显然$(x_0,m)=1$，因为g是模m的一个原根，因此存在$u\in Z$，使得$x_0\equiv g^u(mod\ m)$，因此$g^{nu}\equiv a\ (mod\ m)$，由定理4.3.1可知$nu\equiv ind_g(a)(mod\ \varphi(m))$，所以同余式$ny\equiv ind_g(a)(mod\ \varphi(m))$有解，则由定理2.3.2，有$\big(n,\varphi(m)\big)|ind_g(a)$。

再证充分性。因为$(n,\varphi(m))|ind_g(a)$，由定理2.3.2可知，同余式$ny\equiv ind_g(a)(mod\ \varphi(m))$有解，设$y\equiv u\ (mod\ \varphi(m))$是它的解，则$nu\equiv ind_g(a)(mod\ \varphi(m))$，则存在$k\in Z$，使得$nu=ind_g(a)+k\cdot\varphi(m)$，因此$g^{nu}=g^{ind_g(a)+k\cdot\varphi(m)}=g^{ind_g(a)}\cdot(g^{\varphi(m)})^k\equiv g^{ind_g(a)}\equiv a\ (mod\ m)$，即同余式$x^n\equiv a\ (mod\ m)$有解$x\equiv g^u\ (mod\ m)$。

再证充分性。因为$(n,\varphi(m))|ind_g(a)$，由定理2.3.2可知，同余式$ny\equiv ind_g(a)(mod\ \varphi(m))$有解，设$y\equiv u\ (mod\ \varphi(m))$是它的解，则$nu\equiv ind_g(a)(mod\ \varphi(m))$，则存在$k\in Z$，使得$nu=ind_g(a)+k\cdot\varphi(m)$，因此$g^{nu}=g^{ind_g(a)+k\cdot\varphi(m)}=g^{ind_g(a)}\cdot(g^{\varphi(m)})^k\equiv g^{ind_g(a)}\equiv a\ (mod\ m)$，即同余式$x^n\equiv a\ (mod\ m)$有解$x\equiv g^u\ (mod\ m)$。

进一步，当$(n,\varphi(m))|ind_g(a)$时，由定理2.3.2可知，同余式$ny\equiv ind_g(a)(mod\ \varphi(m))$有$(n,\varphi(m))$个解。又因为对任意$u_1,u_2\in Z,u_1\not\equiv u_2\ (mod\ \varphi(m))$，当且仅当$g^{u_1}\not\equiv g^{u_2}(mod\ m)$，因此同余式$ny\equiv ind_g(a)(mod\ \varphi(m))$的不同解对应同余式$x^n\equiv a\ (mod\ m)$的不同解，即两个同余式的解数相等，都为$(n,\varphi(m))$。

- 推论 设$m,n,a\in Z,m,n>1,(a,m)=1$， g是模m的一个原根，则a是模m的n次剩余的充要条件是$a^{\frac{\varphi(m)}{(n,\varphi(m))}}\equiv 1\ (mod\ m)$ 。

证明：由定理4.3.4可知，同余式$x^n\equiv a\ (mod\ m)$有解当且仅当$\left(n,\varphi(m)\right)|ind_g(a)$，当且仅当$ord_m(g)=\varphi(m)=\frac{\varphi(m)}{(n,\varphi(m))}\left(n,\varphi(m)\right)|\frac{\varphi(m)}{(n,\varphi(m))}ind_g(a)$，当且仅当$1\equiv g^{\frac{\varphi(m)}{(n,\varphi(m))}ind_g(a)}=\left(g^{ind_g(a)}\right)^{\frac{\varphi(m)}{(n,\varphi(m))}}\equiv a^{\frac{\varphi(m)}{(n,\varphi(m))}}\ (mod\ m)$。

- 例 求解同余式$x^8 \equiv 23 \ (mod\ 41)$

- 例 求解同余式$x^8 \equiv 23\ (mod\ 41)$

解：由定理4.3.4，同余式$x^8 \equiv 23\ (mod\ 41)$有解当且仅当$\left(8,\varphi(41)\right)|ind_6(23)$，因为$\left(8,\varphi(41)\right)=8$，并查表得$ind_6(23)=36$，因此$\left(8,\varphi(41)\right)|ind_6(23)$不成立，故同余式$x^8 \equiv 23\ (mod\ 41)$无解。

	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

- 例 求解同余式$x^{12} \equiv 37\ (mod\ 41)$

解：因为$\big(12, \varphi(41)\big) = 4$，并查表得$ind_6(37) = 32$，由定理4.3.4，同余式$x^{12} \equiv 37\ (mod\ 41)$有4个解。

先求解同余式$12 ind_6(x) \equiv ind_6(37) = 32\ (mod\ 40)$，化简得$3 ind_6(x) \equiv 8\ (mod\ 10)$，解得 $ind_6(x) \equiv 6\ (mod\ 10)$，因此$12 ind_6(x) \equiv 32\ (mod\ 40)$的全部解为$ind_6(x) \equiv$ 6,16,26,36 $(mod\ 40)$，故$x^{12} \equiv 37\ (mod\ 41)$的全部解为$x \equiv 6^6 \equiv 39, 6^{16} \equiv 18, 6^{26} \equiv 2, 6^{36} = 23\ (mod\ 41)$。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 定理4.3.5 设$m, a \in Z, m > 1, (a, m) = 1$，$g$是模$m$的一个原根，则$ord_m\,(a) = \frac{\varphi(m)}{(\varphi(m), ind_g(a))}$，特别的，$a$是模$m$的原根当且仅当$\left(\varphi(m), ind_g(a)\right) = 1$。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 定理4.3.5 设$m,a\in Z,m>1,(a,m)=1$，g是模m的一个原根，则$ord_m\,(a)=\frac{\varphi(m)}{(\varphi(m),ind_g(a))}$，特别的，$a$是模$m$的原根当且仅当$\left(\varphi(m),ind_g(a)\right)=1$。

证明：因为g是模m的原根，所以$ord_m(g)=\varphi(m)$，又显然有$g^{ind_g(a)}\equiv a\,(mod\,m)$，则由定理4.1.6，$ord_m(a)=ord_m\left(g^{ind_g(a)}\right)=\frac{ord\,(g)}{\left(ord\,(g),ind_g(a)\right)}=\frac{\varphi(m)}{(\varphi(m),ind_g(a))}$，故$a$是模$m$的原根当且仅当$\frac{\varphi(m)}{(\varphi(m),ind_g(a))}=\varphi(m)$，当且仅当$\left(\varphi(m),ind_g(a)\right)=1$。

§4.4 基于离散对数的密码方案

- El'Gamal公钥方案
  - 设p是一个大素数，α是模p的一个本原元，随机选择整数a，$0 < a < \varphi(p)$，计算$\beta = \alpha^a \ (mod\ p)$，则公钥为$(p, \alpha, \beta)$，私钥是$a$
  - 对消息$m, 0 < m < p$，取随机整数r，$0 < r < \varphi(p)$，计算$c_1 = \alpha^r (mod\ p), c_2 = m \cdot \beta^r (mod\ p)$，则密文为$(c_1, c_2)$
  - 对密文(c_1, c_2)，首先计算$y = c_1^a (mod\ p)$，然后计算y'，满足$y'y \equiv 1\ (mod\ p)$，最后计算$m' = y'c_2\ (mod\ p)$，m'即为明文输出。

正确性：

因为$m' \equiv y'^{c_2} \equiv y' m \beta^r \equiv m y' \alpha^{ar} = m y' c_1^a \equiv m y' y \equiv m \pmod p$，且$0 \leq m, m' < p$，所以$m' = m$。

- 由Whitefileld Diffie和Martin Hellman在1976年提出
- 是最早的密钥交换算法之一
- 是最早提出私钥和相应公钥概念的公开方案
- 使得通信的双方能在非安全的信道中安全的交换密钥，用于加密后续的通信消息

- Diffie-Hellman密钥交换协议
  - 设p是一个大素数，α是模p的一个本原元，则(p, α)是公共参数（A和B共有）
  - A拥有秘密x，B拥有秘密y，则A计算$X = \alpha^x$并发送给B，B计算$Y = \alpha^y$并发送给A
  - 收到X后，B计算$K = X^y$，作为和A通信的密钥；类似的，收到Y后，A计算$K' = Y^x$作为和B通信的密钥。

- 正确性：容易验证$K = K' = \alpha^{xy}$。

实验3

- El'Gamal公钥方案
  - 取随机大素数p，搜索模p的一个本原元作为生成元α。
  - 在$Z_{\varphi(p)}$中取一个随机数作为私钥a，计算公钥，输出公钥和私钥。
  - 在Z_p中取一个随机消息m，$Z_{\varphi(p)}$中取随机数r，计算并密文(c_1, c_2)。
  - 对密文(c_1, c_2)做解密运算，计算并输出明文m'。
- 要求：输出中间结果和最终结果，包括$x, y, c, \left(\frac{c}{p}\right), \left(\frac{c}{q}\right), m'$
- 语言：C/C++或Python
- 使用头歌平台搭建环境并提交作业