第 5 章　Elgamal 密码体制与离散对数

5.1　Elgamal 概述

Elgamal 密码体制是埃及密码学家塔希尔·盖莫尔(Taher Elgamal)在 1985 年提出的一种基于离散对数(discrete logarithms)难题的公钥密码算法,此密码体制应用于一些技术标准中,如美国国家标准技术局(NIST)于 1991 年提出作为美国联邦信息处理标准(FIPS)的数字签名标准 DSS(digital signature standard)和 S/MIME 电子邮件标准。

【进一步知识】　Elgamal 和 ElGamal 密码算法

由于塔希尔·盖莫尔是埃及人,按照阿拉伯人的命名习惯,他发明的密码算法最初写法是 ElGamal 或 El Gamal 密码算法。但第二个字母到底是小写的"l"(大写为"L"),还是大写的"I"(小写为"i"),很容易令人混淆。因此,目前通常统一按照英文记录习惯,记录为 Elgamal 密码算法。

在介绍离散对数的理论之前,首先给出 Elgamal 密码的算法描述如图 5.1 所示。

密钥的产生	
选择1个素数:	q
选择1个整数α:	$\alpha \in \mathbb{Z}_q^*$, α是q的一个原根
选择整数d:	$d \in \mathbb{Z}_q^*$, $d>1$
计算e:	$e=\alpha^d \bmod q$
公开密钥:	$k_p=\{q, \alpha, e\}$
私有密钥:	$k_s=\{q, d\}$

加密	
明文:	$m \in \mathbb{Z}_q^*$
选择随机整数r:	$r \in \mathbb{Z}_q^*$
计算c_1:	$c_1=\alpha^r \bmod q$
计算c_2:	$c_2=e^r m \bmod q$
密文:	(c_1, c_2)

解密	
明文:	c_1、$c_2 \in \mathbb{Z}_q^*$
密文:	$m=c_1^{-d}c_2 \bmod q$

图 5.1　Elgamal 加密算法

Elgamal 密码定义在循环群$(\mathbb{Z}_q^*, \times_q)$上，明文分组和密文分组均是$\mathbb{Z}_q^*$中的一个元素，密文比明文要长，长度通常认为是明文长度的 2 倍。Elgamal 加密使用公开密钥$\{q, \alpha, e\}$，解密使用私有密钥$\{q, d\}$，是一种非对称密码体制。

例 5.1　B 要将消息 $m=4$ 发送给 A，选择 Elgamal 算法实现保密传递。假设 A 的公钥为 $q=41, \alpha=6$，A 的私钥 $d=2$，则其公钥 $e=\alpha^d \bmod q=6^2 \bmod 41=36$。B 加密时选择随机数 $r=5$，请问 A 收到的密文是多少？请将其解密还原出消息 m。

解：(1) B 计算 $e^r \bmod q=36^5 \bmod 41=32$，

$c_1=\alpha^r \bmod q=6^5 \bmod 41=27$，

$c_2=e^r m \bmod q=32\times 4 \bmod 41=5$，

所以，A 收到的密文(27,5)。

(2) A 计算 $x=c_1^{-d} \bmod q=27^{-2} \bmod 41$，

因为 $41=27+14, 1=14\times 2-27$，得到 $1=41\times 2-27\times 3$，因此 $27^{-1} \bmod 41=-3$，

所以 $x=c_1^{-d} \bmod q=27^{-2} \bmod 41=(27^{-1})^2 \bmod 41=(-3)^2 \bmod 41=9$，

故计算明文 $m=c_1^{-d} c_2 \bmod q=9\times 5 \bmod 41=4$。

当然，也可以通过

$27^{-2} \bmod 41=27^{(-2) \bmod 40} \bmod 41=27^{38} \bmod 41$，

快速模幂计算：$38=32+4+2=1001010_2$，

$27^2 \bmod 41=32, 27^4 \bmod 41=32^2 \bmod 41=-1, 27^8 \bmod 41=1$，

$27^{32} \bmod 41=27^{16} \bmod 41=1$，

$x=c_1^{-d} \bmod q=27^{-2} \bmod 41=27^{38} \bmod 41=27^{2+4+32} \bmod 41=32\times(-1)\times 1 \bmod 41=9$，进而解密出明文。

【思考】

Elgamal 算法的计算过程并不复杂，为了分析它，需要解决 4 个基本问题，如表 5.1 所示。

表 5.1　Elgamal 算法中的 4 个计算问题

算法环节	计算步骤	序号	问题描述
密钥产生	选择 1 个整数 α 是素数 q 的一个原根	1	什么是原根？素数的原根一定存在吗？如何寻找原根？
加密	选择随机整数 r	2	加密时为什么要选择随机整数 r？
	生成密文(c_1, c_2)	3	为什么密文是 c_1 和 c_2 两个部分？
解密	计算 $m=c_1^{-d} c_2 \bmod q$	4	如何证明 Elgamal 算法的正确性？

5.2　Elgamal 算法分析

1. 证明 Elgamal 算法的正确性

有 $0<m, d, e, r, c_1, c_2<q$，解密时

$$m=c_1^{-d} c_2 \bmod q \Leftrightarrow c_2=c_1^d m \bmod q$$

加密时有

$$c_2 = e^r m \bmod q$$

因此只需要证明

$$e^r \bmod q = c_1^d \bmod q$$

因为加密时有 $c_1 = \alpha^r \bmod q$ 和 $e = \alpha^d \bmod q$，所以有

$$e^r \bmod q = (\alpha^d \bmod q)^r \bmod q = \alpha^{dr} \bmod q$$

$$c_1^d \bmod q = (\alpha^r \bmod q)^d \bmod q = \alpha^{dr} \bmod q$$

所以

$$c_1^{-d} c_2 \bmod q = (e^r)^{-1} c_2 \bmod q = m$$

2. 密文是 c_1 和 c_2 两个部分组成

经过 Elgamal 算法加密后，明文 $m(0<m<q)$ 被加密成两个部分的密文 c_1 和 $c_2(0<c_1, c_2<q)$，按位数来算，密文长度的二进制位数变成了原来明文的二进制位数的 2 倍，这使通信的数据量变成了原来的 2 倍。

明显地，真正和明文 m 有关的密文是 c_2（只有 c_2 的计算有 m 参与），不妨设 $K = e^r \bmod q$，则 c_2 的计算可以写为

$$c_2 = Km \bmod q$$

如前所述，$e^r \bmod q = c_1^d \bmod q$，即 $c_1^{-d} \bmod q = K^{-1} \bmod q$，解密出明文的计算可以写为

$$m = K^{-1} c_2 \bmod q$$

显然，这可视为使用了密钥为 $(K, 0)$ 的仿射密码算法，因此明文本质上是通过对称加密后传递的，K 是对称加密/解密密钥。

但对称密钥 K 不能明文传递，类似 1.2 节介绍的数字信封(digital envelope)方案，密文 c_1 可认为是非对称加密后传递的密钥 K，接收方收到后 c_1 使用自己的私钥 d 解密恢复出对称加密的密钥 K，再利用 K 从 c_2 中恢复出明文 m。

例 5.2 采用 Elgamal 密码，选择素数 $q = 4519$ 及其原根 $\alpha = 3$，B 的私钥 $d = 58$，请计算：

(1) B 的公钥 e；

(2) A 选择随机整数 $r = 36$，将字母“A”加密后发送给 B；

(3) 对 B 收到的密文进行解密验证。

解：(1) $e = \alpha^d \bmod q = 3^{58} \bmod 4519 = 1163$。

(2) A 要加密字母“A”，即明文 $m = 65$，则

$K = e^r \bmod q = 1163^{36} \bmod 4519 = 1627$，

$c_1 = \alpha^r \bmod q = 3^{36} \bmod 4519 = 3975$，

$c_2 = Km \bmod q = 1627 \times 65 \bmod 4519 = 1818$，

所以，A 发出的密文为(3975,1818)；

(3) B 解密：

$K = c_1^d \bmod q = 3975^{58} \bmod 4519 = 1627$

因为 $4519 = 1627 \times 3 - 362$，$1627 = 362 \times 4 + 179$，$362 = 179 \times 2 + 4$，$179 = 4 \times 45 - 1$

所以 $1 = 4 \times 45 - 179 = (362 - 179 \times 2) \times 45 - 179 = 362 \times 45 - 179 \times 91$

$= 362 \times 45 - (1627 - 362 \times 4) \times 91 = 362 \times 409 - 1627 \times 91$

$$=(1627\times3-4519)\times409-1627\times91=1627\times1136-4519\times409$$

故　　$K^{-1} \bmod q=1627^{-1} \bmod 4519=1136$

$m=K^{-1}c_2 \bmod q=1627^{-1}\times1818 \bmod 4519=1136\times1818 \bmod 4519=65$

B 恢复出明文“A”。

当然 B 解密过程也可以计算为

$$m=c_1^{-d}c_2 \bmod q=3975^{-58}\times1818 \bmod 4519=3975^{4460}\times1818 \bmod 4519=65$$

【你应该知道的】 DH 密钥交换算法

实际上，最早、最简单、最具有里程碑意义的公钥算法是 DH 密钥交换（或称为 DH 密钥协商）算法，是美国斯坦福大学的博士生 Whitfield Diffie 和他的导师 Martin E. Hellman 在 1976 年发表的论文《密码学新方向》（“New Direction in Cryptography”）中首次提出的，为密码学的发展提供了新的理论和技术基础。一方面，密码算法的基本工具从代换和置换变为了数学函数；另一方面，两个非对称密钥的使用对保密性、密钥分配、认证等应用具有深刻的意义。可以说，DH 密钥交换算法的出现是密码学史上最大的、真正的革命，DH 两人因此获得了 2015 年的图灵奖。

DH 密钥交换算法并不能进行数据加密。通信双方 A 和 B 可以通过公开信道交换数据 Y_A 和 Y_B，产生一个随机的只有两人知道的共享密钥，以便在后续通信中能使用该密钥对消息进行对称加密。其具体过程描述如图 5.2 所示。

全局公开的参数	
选择1个素数：	q
选择1个整数α：	$\alpha\in\mathbb{Z}_q^*$，α是q的一个原根

用户A的密钥的产生	
选择私有的X_A：	$1<X_A<q$
计算公开的Y_A：	$Y_A=\alpha^{X_A} \bmod q$

用户B的密钥的产生	
选择私有的X_B：	$1<X_B<q$
计算公开的Y_B：	$Y_B=\alpha^{X_B} \bmod q$

计算A和B的共享密钥	
A根据公开的Y_B计算：	$K_A=Y_B^{X_A} \bmod q$
B根据公开的Y_A计算：	$K_B=Y_A^{X_B} \bmod q$

图 5.2　DH 密钥交换算法

显然，有

$$K_A=Y_B^{X_A} \bmod q=(\alpha^{X_B} \bmod q)^{X_A} \bmod q=\alpha^{X_AX_B} \bmod q$$

$$K_B=Y_A^{X_B} \bmod q=(\alpha^{X_A} \bmod q)^{X_B} \bmod q=\alpha^{X_AX_B} \bmod q$$

所以 A 和 B 各自生成的密钥 $K_A=K_B$，密钥协商一致。

例 5.3　选择素数 $q=4519$ 及其原根 $\alpha=3$，A 选择私钥 $X_A=36$，B 选择私钥 $X_B=58$，A 和 B 利用 DH 密钥交换算法协商得到密钥 K，A 再利用仿射密码（$c=Km \bmod q$）将字母“A”传递给 B，请写出加密解密的计算过程。

解：(1) A 计算公钥：$Y_A=\alpha^{X_A} \bmod q=3^{36} \bmod 4519=3975$；

B 计算公钥：$Y_B=\alpha^{X_B} \bmod q=3^{58} \bmod 4519=1163$。

(2) A 利用 B 的公钥计算加密密钥：$K_A=Y_B^{X_A} \bmod q=1163^{36} \bmod 4519=1627$；

B 利用 A 的公钥计算解密密钥：$K_B=Y_A^{X_B} \bmod q=3975^{58} \bmod 4519=1627$。

(3) A 利用 K_A 使用仿射密码加密“A”：即明文 $m=65$，则 $c=Km \bmod q=1627\times65 \bmod 4519=1818$，A 将 $c=1818$ 发送给 B。

(4) B 利用 K_B 使用仿射密码解密：

因为 $1627\times1136-4519\times409=1$，

所以 $K^{-1} \bmod q=1627^{-1} \bmod 4519=1136$，

则 $m=K^{-1}c \bmod q=1136\times1818 \bmod 4519=65$；

B 恢复出明文“A”。

例 5.4 选择素数 $q=4519$ 及其原根 $\alpha=3$，A 选择私钥 $X_A=36$，B 选择私钥 $X_B=58$，A 和 B 利用 DH 密钥交换算法协商得到密钥 K，再利用指数密码($c=m^K \bmod q$)将字母“A”传递给 B，请写出加密解密的计算过程。

解：(1) A 计算公钥：$Y_A=\alpha^{X_A} \bmod q=3^{36} \bmod 4519=3975$；

B 计算公钥：$Y_B=\alpha^{X_B} \bmod q=3^{58} \bmod 4519=1163$。

(2) A 计算加密密钥：$K_A=Y_B^{X_A} \bmod q=1163^{36} \bmod 4519=1627$；

B 计算解密密钥：$K_B=Y_A^{X_B} \bmod q=3975^{58} \bmod 4519=1627$。

(3) A 利用 K_A 使用指数密码加密“A”：

即明文 $m=65$，则 $c=m^{K_A} \bmod q=65^{1627} \bmod 4519=2836$，

A 将 $c=2836$ 发送给 B。

(4) B 利用 K_B 使用指数密码解密：

因为 $c=m^{K_A} \bmod q$，

所以 $c^{K_B^{-1}(\bmod q-1)}\equiv m^{K_AK_B^{-1}(\bmod q-1)}\equiv m(\bmod q)$

又因为 $4518=1627\times3-363$，$1627=363\times4+175$，$363=175\times2+13$，

$175=13\times13+7$，$13=7\times2-1$，

所以 $1=7\times2-13=175\times2-13\times27=175\times56-363\times27=1627\times56-363\times251$

$=1627\times697-4518\times251$，

故 $K_B^{-1} \bmod q=1627^{-1} \bmod 4518=697$，

则 $m=c^{K_B^{-1}(\bmod q-1)} \bmod q=2836^{697} \bmod 4519=65$；

B 恢复出明文“A”。

3. 加密时要选择随机整数 r 的原因

从例 5.2 和例 5.3 的对比可以看出，Elgamal 算法发送方加密时选择随机整数 r，相当于 DH 密钥交换算法中发送方的私钥，只有收、发双方同时选择了各自的私钥时，才可以协商出加密消息的密钥 K。但 Elgamal 算法没有将其固定为私钥，每次加密时需要随机选择。若对同一个明文进行两次加密，由于每次随机选择的整数 r 不同，加密消息的密钥 K 就不同，相同的明文就会被加密成不同的密文。

那么，为什么不直接使用私钥，而是每次都要生成随机数 r？不妨设两次加密使用了相同的 r，明文分别为 m_1 和 m_2，加密计算过程如下：

$$K_1=e^{r_1} \bmod q;\quad c_{1,1}=\alpha^{r_1} \bmod q;\quad c_{2,1}=K_1 m_1 \bmod q。$$

$$K_2=e^{r_2} \bmod q;\quad c_{1,2}=\alpha^{r_2} \bmod q;\quad c_{2,2}=K_2 m_2 \bmod q。$$

显然，若 $r_1=r_2$ 有 $K_1=K_2$，$c_{1,1}=c_{1,2}$，于是有

$$\frac{c_{2,1}}{c_{2,2}}=\frac{K_1 m_1 \bmod q}{K_2 m_2 \bmod q}=\frac{m_1 \bmod q}{m_2 \bmod q}=\frac{m_1}{m_2}$$

若 m_1 已知，则很容易计算出 m_2，即

$$m_2=[(c_{2,1})^{-1}\times c_{2,2}\times m_1] \bmod q$$

因此，每次加密必须使用随机的整数 r。

4. 什么是原根、原根一定存在吗以及如何寻找原根

为了说明 α 是原根的价值，不妨设素数 $q=41$，随机选择 $1<\alpha<q$ 的整数 $\alpha=2$，A 的私钥 $d=2$，满足 $1<d<q-1$，则其公钥 $e=\alpha^d \bmod q=2^2 \bmod 41=4$。B 需要加密后发送给 A 的明文 $m=4$，随机选择 $1<r<q$ 的整数 $r=3$，有

$$K=e^r \bmod q=4^3 \bmod 41=23$$

$$c_1=\alpha^r \bmod q=2^3 \bmod 41=8$$

$$c_2=Km \bmod q=23\times 4 \bmod 41=10$$

A 收到(8,10)后，计算为

$$m=c_1^{-d}c_2 \bmod q=8^{-2}\times 10 \bmod 41=(-5)^2\times 10 \bmod 41=25\times 10 \bmod 41=4$$

不妨再修改上例中的 $\alpha=10$，其余参数不变，则其公钥 $e=\alpha^d \bmod q=10^2 \bmod 41=18$，有

$$K=e^r \bmod q=18^3 \bmod 41=10$$

$$c_1=\alpha^r \bmod q=10^3 \bmod 41=16$$

$$c_2=Km \bmod q=10\times 4 \bmod 41=40$$

A 收到(16,40)后，计算为

$$m=c_1^{-d}c_2 \bmod q=16^{-2}\times 40 \bmod 41=(18)^2\times 40 \bmod 41=-4\times 40 \bmod 41=4$$

正如上文证明 Elgamal 算法的正确性时，推导过程中并没有使用 α 是原根这个前提，在这里的两个例子中，随机选择的底数 α 也不影响加密解密计算。那么为什么还需要提出 α 是原根这个条件呢？

下面换一个角度分析，仍然选择素数 $q=41$，随机选择整数 $\alpha=10$，公钥 $e=18$，若

随机 $r=3$，则 $K=e^r \bmod q=18^3 \bmod 41=10$，

随机 $r=4$，则 $K=e^r \bmod q=18^4 \bmod 41=16$；

随机 $r=5$，则 $K=e^r \bmod q=18^5 \bmod 41=1$；

随机 $r=6$，则 $K=e^r \bmod q=18^6 \bmod 41=18$；

随机 $r=7$，则 $K=e^r \bmod q=18^7 \bmod 41=37$；

随机 $r=8$，则 $K=e^r \bmod q=18^8 \bmod 41=10$；

随机 $r=9$，则 $K=e^r \bmod q=18^9 \bmod 41=16$；

随机 $r=10$，则 $K=e^r \bmod q=18^{10} \bmod 41=1$；

随机 $r=11$，则 $K=e^r \bmod q=18^{11} \bmod 41=18$；

…

可以看出，虽然 r 为 1～40 的随机数，但是 K 的随机性明显不足，只能在循环 1、18、37、10、

16 中取值，也就是说，加密 m 的密钥空间显著减小了，使蛮力攻击的难度显著降低。

相似地，选择素数 $q=41$，随机选择整数 $\alpha=10$，若：

随机 $r=3$，则 $c_1=a^r \bmod q=10^3 \bmod 41=16$，

随机 $r=4$，则 $c_1=a^r \bmod q=10^4 \bmod 41=37$；

随机 $r=5$，则 $c_1=a^r \bmod q=10^5 \bmod 41=1$；

随机 $r=6$，则 $c_1=a^r \bmod q=10^6 \bmod 41=10$；

随机 $r=7$，则 $c_1=a^r \bmod q=10^7 \bmod 41=18$；

随机 $r=8$，则 $c_1=a^r \bmod q=10^8 \bmod 41=16$；

随机 $r=9$，则 $c_1=a^r \bmod q=10^9 \bmod 41=37$；

随机 $r=10$，则 $c_1=a^r \bmod q=10^{10} \bmod 41=1$；

随机 $r=11$，则 $c_1=a^r \bmod q=10^{11} \bmod 41=10$；

……

相似地，虽然 r 为 1～40 的随机数，但是密文 c_1 的随机性明显不足，只能在循环 1、10、18、16、37 中取值，也就是说，密文空间显著减小了，使蛮力攻击的难度显著降低。

【思考】

当 r 是某个伪随机数生成器产生的周期为 m 的伪随机序列，密钥 $e^r \bmod q$ 和密文 $a^r \bmod q$ 两个序列有何联系与差异？它们的空间一定是相同的吗？它们的周期一定是相同的吗？

反之，若选择一个模 q 的原根作为底数 α，则可以使密钥、密文空间大小达到最大，即 $q-1$。5.3 节中将继续分析什么是原根、原根存在性问题以及如何寻找原根。

5.3 原根与指数

在 5.2 节的例子中，根据欧拉定理有 $18^{\varphi(41)} \bmod 41=18^{40} \bmod 41=1$，考虑中间的计算过程，即

$$18^1 \equiv 18, 18^2 \equiv 37, 18^3 \equiv 10, 18^4 \equiv 16, 18^5 \equiv 1 \pmod{41}$$

因此，$18^k \bmod 41$ 实际上会形成一个周期为 5 的循环。

实际上，上述运算定义在群 $(\mathbb{Z}_{41}^*, \times_{41})$ 中，$\mathbb{Z}_{41}^* = \mathbb{Z}_{41} - \{0\} = \{x \mid 0 < x < 41, x \in \mathbb{Z}\}$，对 $\forall x, y \in \mathbb{Z}_{41}^*$，$x \times_{41} y = xy \bmod 41$，$(\mathbb{Z}_{41}^*, \times_{41})$ 的阶为 40，对任意 $(\mathbb{Z}_{41}^*, \times_{41})$ 中的元素，阶均为 40 的因子，即 $x \in \mathbb{Z}_{41}^*$ 时，x 的阶可能为 1、2、4、5、8、10、20 和 40。如 $18 \in \mathbb{Z}_{41}^*$，$K \in \langle 18 \rangle$，18 的阶为 5，$\langle 18 \rangle = \{1, 18, 37, 10, 16\}$。因此，若选择素数 $q=41$，底数 $\alpha=18$，密钥 K 空间大小为 5。

若底数 $\alpha=6 \in \mathbb{Z}_{41}^*$，在群 $(\mathbb{Z}_{41}^*, \times_{41})$ 中有

$6^1=6$，　$6^2=36$，　$6^3=11$，　$6^4=25$，　$6^5=27$，　$6^6=39$，　$6^7=29$，　$6^8=10$，

$6^9=19$，　$6^{10}=32$，　$6^{11}=28$，　$6^{12}=4$，　$6^{13}=24$，　$6^{14}=21$，　$6^{15}=3$，　$6^{16}=18$，

$6^{17}=26$，　$6^{18}=33$，　$6^{19}=34$，　$6^{20}=40$，　$6^{21}=35$，　$6^{22}=5$，　$6^{23}=30$，　$6^{24}=16$，

$6^{25}=14$，　$6^{26}=2$，　$6^{27}=12$，　$6^{28}=31$，　$6^{29}=22$，　$6^{30}=9$，　$6^{31}=13$，　$6^{32}=37$，

$6^{33}=17$，　$6^{34}=20$，　$6^{35}=38$，　$6^{36}=23$，　$6^{37}=15$，　$6^{38}=8$，　$6^{39}=7$，　$6^{40}=1$

因此，6 的阶为 40，$<6>=(\mathbb{Z}_{41}^{*},\times_{41})$，6 是$(\mathbb{Z}_{41}^{*},\times_{41})$的生成元。$6^k \bmod 41$ 形成了一个周期为 40 的循环，当 k 遍历模 41 的缩系时，$6^k \bmod 41$ 也遍历模 41 的缩系，此时称底数 6 就是模 41 的原根。

定义 5.1　原根(primitive root)

$m\in\mathbb{Z}^{+}$，对 $a\in\mathbb{Z}$，$(a,m)=1$，使 $a^k \bmod m=1$ 成立的最小正整数 k 称为 a 模 m 的指数(the order of $a \bmod m$)，记为 $\mathrm{ord}_m(a)$。若 $\mathrm{ord}_m(a)=\varphi(m)$，则称 a 为模 m 的原根。

例 5.5　$\mathrm{ord}_{41}(18)=5$，$\mathrm{ord}_{41}(6)=40$，

$\mathrm{ord}_m(1)=1$，$\mathrm{ord}_m(-1)=2(m>2)$。

【请你注意】

(1) 如果$(a,m)>1$，则规定 $\mathrm{ord}_m(a)=0$。

(2) ***a* 模 *m* 的指数就是$(\mathbb{Z}_m^{*},\times_m)$群中 *a* 的阶**，$\mathbb{Z}_m^{*}=\{x\mid 0<x<m,(x,m)=1\}$，对 $\forall x、y\in\mathbb{Z}_m^{*}$，$x\times_m y=xy \bmod m$。因此，指数也称为阶，$\mathrm{ord}_m(a)$还可以记为 $\delta_m(a)$。

(3) 群$(\mathbb{Z}_m^{*},\times_m)$的阶为 $\varphi(m)$，根据定理 2.9，元素 a 的阶必然整除于群的阶，因此元素的阶最大为 $\varphi(m)$。

(4) 若 a 是模 m 的原根，意味着 a 是群$(\mathbb{Z}_m^{*},\times_m)$的生成元，也叫本原元(primitive elements)。

例 5.6　请计算 $\mathrm{ord}_7(5)$。

解：因为 $5^1 \bmod 7=5$，$5^2 \bmod 7=4$，$5^3 \bmod 7=6$，$5^4 \bmod 7=2$，$5^5 \bmod 7=3$，$5^6 \bmod 7=1$，

所以 $\mathrm{ord}_7(5)=6$。

定理 5.1　设 $a、m、n\in\mathbb{Z}$，$m>1$，$(a,m)=1$

(1) 若 $s、t\in\mathbb{Z}$，$a^s\equiv a^t \pmod m \Leftrightarrow s\equiv t \pmod{\mathrm{ord}_m(a)}$，特别地，

$a^s \bmod m=1\Leftrightarrow s \bmod \mathrm{ord}_m(a)=0$，特别地，

$\varphi(m) \bmod \mathrm{ord}_m(a)=0$，即 $\mathrm{ord}_m(a)\mid\varphi(m)$；

(2) 记 $n=\mathrm{ord}_m(a)$，则 $a^0,a^1,\cdots,a^{n-1}$模 m 两两不同余，特别地，

a 是原根$\Leftrightarrow a^0,a^1,\cdots,a^{\varphi(m)-1}$是模 m 的缩系；

(3) 若 $a\equiv b \pmod m$，则 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$；

(4) 若 $ab\equiv 1 \pmod m$，则 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$；

(5) 若 $m \bmod n=0$，则 $\mathrm{ord}_m(a) \bmod \mathrm{ord}_n(a)=0$；

(6) 若$(m,n)=1$，$(a,mn)=1$，则 $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$；

(7) 若$(ab,m)=1$，$(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$，则 $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\mathrm{ord}_m(b)$。

证明：(1) 设 $s=\mathrm{ord}_m(a)q_1+r_1$，$s=\mathrm{ord}_m(a)q_2+r_2$，$0\leqslant r_1,r_2<\mathrm{ord}_m(a)$，$q_1、q_2、r_1、r_2\in\mathbb{Z}$，则有

$$a^s\equiv a^{\mathrm{ord}_m(a)q_1+r_1}\equiv a^{\mathrm{ord}_m(a)q_1}a^{r_1}\equiv a^{r_1} \pmod m$$

$$a^t\equiv a^{\mathrm{ord}_m(a)q_2+r_2}\equiv a^{\mathrm{ord}_m(a)q_2}a^{r_2}\equiv a^{r_2} \pmod m$$

所以 $a^s \equiv a^t \pmod m \Leftrightarrow a^{r_1} \equiv a^{r_2} \pmod m \Leftrightarrow a^{r_1 - r_2} \equiv 1 \pmod m$。

故 $r_1 - r_2 = 0$，即 $s \equiv t \pmod{\mathrm{ord}_m(a)}$，

特别地，$a^s \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \pmod m \Leftrightarrow s \bmod \mathrm{ord}_m(a) = \mathrm{ord}_m(a) \bmod \mathrm{ord}_m(a) = 0$，

特别地，根据欧拉定理，$a^{\varphi(m)} \equiv 1 \pmod m$，所以 $\mathrm{ord}_m(a) \mid \varphi(m)$，证毕。

(2) (反证法)若 $0 \leqslant i < j \leqslant n-1$，有 $a^i \equiv a^j \pmod m$，

由(1)得 $j \equiv i \pmod n$，因为 $j - i < n$，所以 $j - i = 0$，矛盾，

所以 $a^0, a^1, \cdots, a^{n-1}$ 对模 m 两两不同余；

若 a 是原根，则 $\mathrm{ord}_m(a) = \varphi(m)$，

所以 $a^0, a^1, \cdots, a^{\varphi(m)-1}$ 这 $\varphi(m)$ 个数模 m 两两不同余，

故 $a^0, a^1, \cdots, a^{\varphi(m)-1}$ 是模 m 的缩系，证毕。

(3) 若 $a \equiv b \pmod m$，则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \pmod m$，

由(1)有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$，同理 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$，故 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$，证毕。

(4) 若 $ab \equiv 1 \pmod m$，则 $b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} b^{\mathrm{ord}_m(a)} \equiv (ab)^{\mathrm{ord}_m(a)} \equiv 1^{\mathrm{ord}_m(a)} \equiv 1 \pmod m$，

由(1)有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$，同理 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$，故 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$，证毕。

(5) 若 $m \bmod n = 0$，则 $a^{\mathrm{ord}_m(a)} \bmod m = 1 \Rightarrow a^{\mathrm{ord}_m(a)} \bmod n \equiv 1$，

由(1)有 $\mathrm{ord}_m(a) \bmod \mathrm{ord}_n(a) = 0$，证毕。

(6) 若 $(m, n) = 1$，$(a, mn) = 1$，则由(5)有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a)$，$\mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a)$，

设 $s = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$，有 $s \mid \mathrm{ord}_{mn}(a)$，

又因为 $\mathrm{ord}_m(a) \mid s$，$\mathrm{ord}_n(a) \mid s$，所以 $a^s \equiv 1 \pmod m$，$a^s \equiv 1 \pmod n$，

则 $a^s \equiv 1 \pmod{mn}$，由(1)有 $\mathrm{ord}_{mn}(a) \mid s$，

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

(7) 若 $(ab, m) = 1$，有 $a^{\mathrm{ord}_m(a)\mathrm{ord}_m(ab)} \equiv 1^{\mathrm{ord}_m(ab)} \equiv (ab)^{\mathrm{ord}_m(a)\mathrm{ord}_m(ab)} \equiv 1 \pmod m$，

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

由(1)有 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(ab)\mathrm{ord}_m(a)$

又因为 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，所以 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(ab)$，

同理，$\mathrm{ord}_m(a) \mid \mathrm{ord}_m(ab)\mathrm{ord}_m(b)$，所以 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(ab)$，

故 $\mathrm{ord}_m(a)\ \mathrm{ord}_m(b) \mid \mathrm{ord}_m(ab)$；

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

则由(1)有 $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a)\ \mathrm{ord}_m(b)$

故 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a)\mathrm{ord}_m(b)$，证毕。

例 5.7 请计算 $\mathrm{ord}_{17}(5)$。

解：因为 $\varphi(17) = 16$，所以 $\mathrm{ord}_{17}(5) \mid 16$，则 $\mathrm{ord}_{17}(5)$ 可能为 1、2、4、8、16。

又因为 $5^1 \bmod 17 = 5$，$5^{16} \bmod 17 \equiv 1$，所以只需计算 5^2、5^4、$5^8 \pmod{17}$，

由 $5^2 \bmod 17 = 8$，$5^4 \bmod 17 = 64 \bmod 17 = 13$，$5^8 \bmod 17 = 169 \bmod 17 = -1$，

则 $\mathrm{ord}_{17}(5) = 16$，即 5 是模 17 的原根。

例 5.8 请计算 $\mathrm{ord}_{17}(39)$ 和 $\mathrm{ord}_{17}(7)$。

解：因为 $39 \bmod 17 = 5$，所以 $\mathrm{ord}_{17}(39) = \mathrm{ord}_{17}(5) = 16$。

又因为 $7 \times 5 \equiv 1 \pmod{17}$，所以 $7^{-1} \bmod 17 = 5$，故 $\mathrm{ord}_{17}(7) = \mathrm{ord}_{17}(5) = 16$。

例 5.9 请计算 $\mathrm{ord}_{49}(3)$。

解：因为 $\varphi(49)=7^2-7=42$，所以 $\mathrm{ord}_{49}(3)$可能为 1、2、3、6、7、14、21、42，

又因为 $\mathrm{ord}_7(3)=6\mid\mathrm{ord}_{49}(3)$，所以 $\mathrm{ord}_{49}(3)$只可能为 6 或 42，

则只需计算 $3^6 \bmod 49$，由 $3^6 \bmod 49=-6$，有 $\mathrm{ord}_{49}(3)=42$。

例 5.10　请计算 $\mathrm{ord}_{28}(3)$。

解：因为 $\varphi(28)=\varphi(4\times7)=\varphi(4)\times\varphi(7)=2\times6=12$，所以 $\mathrm{ord}_{28}(3)\mid12$。

(法一)因为 $\mathrm{ord}_7(3)\mid\mathrm{ord}_{28}(3)$，$\mathrm{ord}_4(3)\mid\mathrm{ord}_{28}(3)$，而 $\mathrm{ord}_7(3)=6$，$\mathrm{ord}_4(3)=2$，

所以 $6\mid\mathrm{ord}_{28}(3)$，故 $\mathrm{ord}_{28}(3)$可能为 6 或 12，

又因为 $3^6 \bmod 28=27^2 \bmod 28=1$，所以 $\mathrm{ord}_{28}(3)=6$。

(法二)因为$(4,7)=1$，所以 $\mathrm{ord}_{28}(3)=[\mathrm{ord}_7(3),\mathrm{ord}_4(3)]=[6,2]=6$。

例 5.11　请计算模 23 的一个原根。

解：因为 $\varphi(23)=22$，所以 $\mathrm{ord}_{23}(a)$可能为 1、2、11、22，

又因为 $2^2 \bmod 23=4$，$2^{11} \bmod 23=1$，所以 $\mathrm{ord}_{23}(2)=11$，

又由 $\mathrm{ord}_{23}(-1)=2$，有$(\mathrm{ord}_{23}(2),\mathrm{ord}_{23}(-1))=1$，

而$(-1\times2,23)=(21,23)=1$，

故 $\mathrm{ord}_{23}(21)=\mathrm{ord}_{23}(-2)=\mathrm{ord}_{23}(-1)\times\mathrm{ord}_{23}(2)=22$，即 21 为模 23 的一个原根。

定理 5.2　设 a、m、$k\in\mathbb{Z}^+$，$(a,m)=1$，则

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

证明：设 $n=\mathrm{ord}_m(a)$，$s=\mathrm{ord}_m(a^k)$，即需要证明 $s=n/(k,n)$，

因为 $a^{ks}\equiv(a^k)^s\equiv1\ (\mathrm{mod}\ m)$，所以 $ks \bmod n=0$，

根据定理 2.3(2)，有 $s \bmod (n/(k,n))=0$，

又因为$(a^k)^{n/(k,n)}=(a^n)^{k/(k,n)}\equiv1^{k/(k,n)}\equiv1\ (\mathrm{mod}\ m)$，所以$(n/(k,n)) \bmod s=0$，

故 $s=n/(k,n)$。证毕。

【你应该知道的】

(1) 推广到一般群中，有定理 2.9(3)：群 G 中有元素 a，$\forall m\in\mathbb{Z}$，则$|a^m|=|a|/(|a|,m)$。

(2) 当$(k,\mathrm{ord}_m(a))=1$ 时，有 $\mathrm{ord}_m(a^k)=\mathrm{ord}_m(a)$，因此有限循环群$(\mathbb{Z}_m^*,\times_m)$中，与 a 指数相同的数有 $\varphi(\mathrm{ord}_m(a))$个，简记为：循环群 $\mathbb{Z}_m^*$ 中阶为 n 的元素有 $\varphi(n)$个，其中 n 是 $\varphi(m)$的因子。

(3) 若 a 是模 m 的原根，则当$(k,\varphi(m))=1$ 时，a^k 也是模 m 的原根。

(4) 如果模 m 存在原根，则不同的原根有 $\varphi(\varphi(m))$个。

例 5.12　请计算模 23 的所有原根。

解：因为−2 为模 23 的一个原根(见例 5.11)，

所以模 23 的原根有 $\varphi(\varphi(23))=\varphi(22)=\varphi(2)\times\varphi(11)=10$ 个，

所有原根可以表示为$(-2)^k \bmod 23$，其中$(k,\varphi(23))=1$，即 $k=1$、3、5、7、9、13、15、17、19、21，

故模 23 的所有原根有−2、−8、−9、−13、−6、−4、7、5、20、−12，

即模 23 的所有原根有 5、7、10、11、14、15、17、19、20、21。