# 第 4 章　原根与指数

原根和指数是数论及其应用中一个重要的概念，是后面一些问题的基础. 抽象代数中循环群的概念，就与此紧密相关. 同时，其在 ElGamal 密码算法、Diffie-Hellman 密钥交换协议（简记 DH）、椭圆曲线密码学和数字签名理论中有广泛的应用. 本章将介绍原根以及与其相关的基本知识.

学习本章之后，我们应该能够

- 掌握次数和原根的概念和性质，以及相关的计算方法和应用；
- 掌握指数和高次剩余的概念与性质，以及相关的计算方法和应用。

## 4.1　次数

次数是本章中的一个重要概念，接下去我们给出其准确的数学定义.

设 $m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的整数，我们考虑 $a$ 的正整数次幂

$$a, a^2, a^3, \dots,$$

由欧拉定理可知，有

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

然而，对很多 $m$ 来说，往往存在比 $\varphi(m)$ 还小的正整数 $k$，就已经使得$a^k \equiv 1 \pmod m$. 这就提示我们先来研究使

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

成立的最小正整数 $l$，并进一步讨论关于 $l$ 的一些性质.

**定义 4.1.1**　设 $m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的整数，使

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

成立的最小正整数 $l$ 叫作 $a$ 对模 $m$ 的**次数**，记作 $\mathrm{ord}_m(a)$或$\delta_m(a)$，在不致误会的情况下，简记为 $\mathrm{ord}(a)$或$\delta(a)$.

**注意**：若 $\mathrm{ord}_m(a) = \varphi(m)$，则 $a$ 叫作 $m$ 的**原根**. 我们将在 4.2 节详细讨论.

由次数的定义可知，对任意大于 1 的整数 $m$，有 $\mathrm{ord}_m(1)=1$, $\mathrm{ord}_m(-1)=2$.

**例 4.1.1**　求 $\mathrm{ord}_{11}(a)$，其中$a = 1,2,\dots,10$.

**解**　分别求 $a^i \pmod{11}$, $i = 1,2,\dots,10$，直至出现 $a^i \equiv 1 \pmod{11}$为止，如下表所示.

| | $a$=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 | | |

可得

$\mathrm{ord}_{11}(1) = 1$；

$\mathrm{ord}_{11}(2) = \mathrm{ord}_{11}(6) = \mathrm{ord}_{11}(7) = \mathrm{ord}_{11}(8) = 10$；

$\mathrm{ord}_{11}(3) = \mathrm{ord}_{11}(4) = \mathrm{ord}_{11}(5) = \mathrm{ord}_{11}(9) = 5$；

$\mathrm{ord}_{11}(10) = 2$.

□

我们需要注意的是，在上面的定义里面只考虑那些与 $m$ 互素的整数 $a$，对于$(a, m)>1$ 的情况, 不可能存在一个正整数 $l$，使得关系式

$$a^l \equiv 1 \pmod m \quad (l \geqslant 1)$$

成立．于是，当我们谈到"$a$ 对模 $m$ 的次数"的时候，即使没有明确地陈述条件$(a, m) = 1$，我们也是暗含地假设这个条件成立（同时，也隐含地认为 $m>1$ 的条件成立），这样会使许多定理和问题的陈述变得简洁并容易记忆.

**定理 4.1.1** 设 $a$ 对模 $m$ 的次数是 $\mathrm{ord}_m(a)$，则非负整数 $n$ 使得

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

的充要条件是 $\mathrm{ord}_m(a) \mid n$.

**证明** 先证必要性．用反证法，假设 $\mathrm{ord}_m(a) \mid n$ 不成立，则存在整数 $q, r$ 使得

$$n = \mathrm{ord}_m(a)q + r,\quad 0 < r < \mathrm{ord}_m(a),$$

于是

$$a^r \equiv a^r\left(a^{\mathrm{ord}_m(a)}\right)^q = a^n \equiv 1 \pmod m,$$

这与次数的定义中 $\mathrm{ord}_m(a)$的"最小"性质矛盾，故假设不成立，必要性得证.

再证充分性．由于 $\mathrm{ord}_m(a) \mid n$，故存在整数 $k$ 使得 $n = k\,\mathrm{ord}_m(a)$，于是

$$a^n = \left(a^{\mathrm{ord}_m(a)}\right)^k \equiv 1 \pmod m.$$

定理得证.

□

根据定理 4.1.1，我们可以得到关于次数的如下的一些性质.

**定理 4.1.2** 设 $a$ 对模 $m$ 的次数是 $\mathrm{ord}_m(a)$，则有

(1) $\mathrm{ord}_m(a) \mid \varphi(m)$；

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

**证明** (1) 根据欧拉定理，我们有

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

再根据定理 4.1.1, 显然 $\mathrm{ord}_m(a) \mid \varphi(m)$.

(2) 由同余的基本性质，如果 $b \equiv a \pmod{m}$，则 $b$ 和 $a$ 的任意相同次幂都同余，故显然二者次数相同，即 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$. 定理得证.

□

定理 4.1.2 可用来简化次数的计算，以下举一个例子.

**例 4.1.2** 计算 5 对模 17 的次数 $\mathrm{ord}_{17}(5)$.

**解** 由于φ(17)=16, 而 16 的因子有 1, 2, 4, 8, 16, 所以只需计算 5 的 1, 2, 4, 8, 16 次方

$$5^1 \equiv 5 \pmod{17},$$
$$5^2 \equiv 8 \pmod{17},$$
$$5^4 \equiv 13 \pmod{17},$$
$$5^8 \equiv 16 \pmod{17},$$
$$5^{16} \equiv 1 \pmod{17},$$

所以 $\mathrm{ord}_{17}(5)=16$.

□

由这个定理，我们知道 $\mathrm{ord}_m(a)$必然是 $\varphi(m)$ 的因子，但是对于 $\varphi(m)$ 的任意一个选定的因子 $d$，未必存在整数 $a$，使得 $\mathrm{ord}_m(a)=d$.

**例 4.1.3** 对于 $m=12$，有 $\varphi(12)=4$，但是不存在整数对模 12 的次数是 4. 因为我们通过计算可以得到

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}.$$

因此，任意整数的对模 12 的次数只能是 1 或者 2，而不可能是 4.

□

**定理 4.1.3** 设 $a$ 对模 $m$ 的次数是 $\mathrm{ord}_m(a)$，则对任意非负整数 $s, t$,

$$a^s \equiv a^t \pmod{m}$$

成立的充要条件是

$$s \equiv t \pmod{\mathrm{ord}_m(a)}.$$

**证明** 先证必要性. 不妨设 $s \geqslant t$，若

$$a^s \equiv a^t \pmod{m},$$

即$m|(a^s - a^t)$，则有$m|a^t(a^{s-t} - 1)$，因为$\gcd(m, a) = 1$，所以$m|(a^{s-t} - 1)$，即

$$a^{s-t} \equiv 1 \pmod{m},$$

由定理 4.1.1 可知，$\mathrm{ord}_m(a)|(s-t)$，即

$$s \equiv t \pmod{\mathrm{ord}_m(a)}.$$

再证充分性. 若

$$s \equiv t \pmod{\mathrm{ord}_m(a)},$$

则存在整数 $q$, 使得 $s=t+q\,\mathrm{ord}_m(a)$，于是

$$a^s = a^{t+q\mathrm{ord}_m(a)} = a^t(a^{\mathrm{ord}_m(a)})^q \equiv a^t(1)^q = a^t \pmod m,$$

即

$$a^s \equiv a^t \pmod m.$$

定理得证.

□

**例 4.1.4** 观察序列 $a^i \pmod 7$ ($i = 1,2,\ldots,6$)，如下表所示，可验证定理 4.1.3 的正确性.

| $a$ | $a^1 \pmod 7$ | $a^2 \pmod 7$ | $a^3 \pmod 7$ | $a^4 \pmod 7$ | $a^5 \pmod 7$ | $a^6 \pmod 7$ | $\mathrm{ord}_m(a)$ |
|---|---|---|---|---|---|---|---|
| **2** | 2 | 4 | 1 | 2 | 4 | 1 | $\mathrm{ord}_7(2)=3$ |
| **3** | 3 | 2 | 6 | 4 | 5 | 1 | $\mathrm{ord}_7(3)=6$ |
| **4** | 4 | 2 | 1 | 4 | 2 | 1 | $\mathrm{ord}_7(4)=3$ |
| **5** | 5 | 4 | 6 | 2 | 3 | 1 | $\mathrm{ord}_7(5)=6$ |
| **6** | 6 | 1 | 6 | 1 | 6 | 1 | $\mathrm{ord}_7(6)=2$ |

□

定理 4.1.3 揭示了一个深刻的事实，即当 $m>1$，并且$(a, m) = 1$ 时，序列 $a^i \pmod m$ ($i = 1,2,3,\ldots$)是周期序列，周期为 $\mathrm{ord}_m(a)$.

**定理 4.1.4** 设 $a$ 对模 $m$ 的次数是 $\mathrm{ord}_m(a)$，则

$$1, a, a^2, \ldots, a^{\mathrm{ord}_m(a)-1}$$

两两模 $m$ 不同余.

**证明** 假设存在整数 $s, t$，$0 \leqslant s \leqslant t \leqslant \mathrm{ord}_m(a) - 1$，使得

$$a^s \equiv a^t \pmod m.$$

则由定理 4.1.3 可知

$$s \equiv t \pmod{\mathrm{ord}_m(a)},$$

显然在 $0 \leqslant s \leqslant t \leqslant \mathrm{ord}_m(a) - 1$ 这个范围中，$s=t$ 是唯一的可能，定理得证.

□

**定理 4.1.5** 设 $a$ 对模 $m$ 的次数是 $\mathrm{ord}_m(a)$，对任意非负整数 $n$，有

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

**证明** 由于

$$a^{n\cdot\mathrm{ord}_m(a^n)} = (a^n)^{\mathrm{ord}_m(a^n)} \equiv 1 \pmod m,$$

根据定理 4.1.1，我们有 $\mathrm{ord}_m(a) \mid n\,\mathrm{ord}_m(a^n)$，于是

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

又因为$\left(\dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), n)}, \dfrac{n}{(\mathrm{ord}_m(a), n)}\right) = 1$，所以

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

另一方面，由于

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

根据定理 4.1.1，我们有 $\operatorname{ord}_m(a^n) \mid \frac{\operatorname{ord}_m(a)}{(\operatorname{ord}_m(a), n)}$.

所以，

$$\operatorname{ord}_m(a^n) = \frac{\operatorname{ord}_m(a)}{(\operatorname{ord}_m(a), n)}.$$

定理得证.

□

**定理 4.1.6** 设 $a$ 对模 $m$ 的次数是 $\operatorname{ord}_m(a)$，存在非负整数 $n$，使得

$$\operatorname{ord}_m(a)=\operatorname{ord}_m(a^n)$$

的充要条件是$(\operatorname{ord}_m(a), n)=1$.

**证明** 略. 这个定理实际上就是定理 4.1.5 的推论. 后面讨论原根时需要用到该定理.

□

**例 4.1.5** 下表给出了整数 1 到 12 对 13 的次数，其中我们可以看到 $\operatorname{ord}_{13}(2)=12$, $\operatorname{ord}_{13}(4)=\operatorname{ord}_{13}(2^2)=6$，$\operatorname{ord}_{13}(8)=\operatorname{ord}_{13}(2^3)=4$，我们很容易验证 $6=12/\gcd(2, 12)$和 $4=12/\gcd(3, 12)$，这正是定理 4.1.5 给出的结论. 次数与 $\operatorname{ord}_{13}(2)=12$ 相同的整数是 $6 \equiv 2^5, 7 \equiv 2^{11}, 11 \equiv 2^7 \pmod{13}$，显然 5, 11, 7 都与 12 互素.

| 整数 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 次数 | 1 | 12 | 3 | 6 | 4 | 12 | 12 | 4 | 3 | 6 | 12 | 2 |

□

为了帮助读者更好地理解整数次数的概念并掌握其应用，下面给出了整数次数的几个性质及其证明，读者可以根据需要阅读.

**性质 1** 设 $m$ 和 $n$ 都是大于 1 的整数，$a$ 是与 $m$ 和 $n$ 都互素的正整数，则

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

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

**证明** (1) 由于

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

又 $n \mid m$，故可知

$$a^{\operatorname{ord}_m(a)} \equiv 1 \pmod n.$$

于是，我们有 $\operatorname{ord}_n(a) \mid \operatorname{ord}_m(a)$.

(2) 由(1)可知

$$\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a),$$
$$\mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a),$$

于是

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

又因为

$$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod m,$$

$$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod n,$$

所以

$$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod{mn}.$$

于是

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

因此，我们得到

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

□

由性质 1 的(2)可直接得到下面的性质.

**性质 2** 设 $m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的正整数，则当 $m$ 的标准分解式为

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, 2, \cdots, s$$

时，有

$$\mathrm{ord}_m(a) = [\mathrm{ord}_{p_1^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \cdots, \mathrm{ord}_{p_s^{\alpha_s}}(a)].$$

**性质 3** 设 $m$ 和 $n$ 都是大于 1 的整数，且$(m, n) = 1$，则对与 $mn$ 互素的任意正整数 $a, b$，存在正整数 $c$，使得

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

**证明** 考虑同余方程组

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

由孙子定理可知，此同余方程组有唯一解

$$x \equiv c \pmod{mn}.$$

由定理 4.1.2(2)可知

$$\mathrm{ord}_m(c) = \mathrm{ord}_m(a), \quad \mathrm{ord}_n(c) = \mathrm{ord}_n(b),$$

于是，根据性质 1 中(2)，我们有

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

□

## 习题 4.1

**A 组**

1. 34 对模 37 的次数是多少?

2. $2^{12}$ 对模 37 的次数是多少?

3. 2 是模 61 的一个原根， 利用这个事实， 在小于 61 的正整数中， 找到所有次数为 4 的整数.

4. 证明 $\mathrm{ord}_3(2)= 2$, $\mathrm{ord}_5(2)= 4$, $\mathrm{ord}_7(2)= 3$.

**B 组**

5. 设 $ab \equiv 1 \pmod m$， 求证 $\mathrm{ord}_m(a)= \mathrm{ord}_m(b)$.

6. 设 $m = a^n - 1$，其中 $a$ 和 $n$ 是正整数，证明 $\mathrm{ord}_m(a) = n$，且 $n \mid \varphi(m)$ .

7. 设 $m > 1$, $(a, m) = 1$，如果 $\mathrm{ord}_m(a) = st$，证明 $\mathrm{ord}_m(a^s) = t$.

8. 设 $a, b, m$ 是正整数，如果 $a, b$ 分别与 $m$ 互素，且满足$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，证明 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

9. 证明如果 $a^{-1}$ 是 $a$ 模 $n$ 的逆，则 $\mathrm{ord}_n(a) = \mathrm{ord}_n(a^{-1})$.

10. 证明$\mathrm{ord}_{F_n}(2) \le 2^{n+1}$，其中$F_n = 2^{2^n} + 1$是第 $n$ 个费马数.

11. 设 $p$ 是费马数$F_n = 2^{2^n} + 1$的一个素因子，证明：

    (1) $\mathrm{ord}_p(2) = 2^{n+1}$;

    (2) $p$ 一定形如$2^{n+1}k + 1$.

12. 编写程序求 $a$ 对模 $m$ 的次数，其中 $a$ 与 $m$ 是互素的正整数.

## 4.2 原根

**定义 4.2.1** 设 $m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的整数，若

$$\mathrm{ord}_m(a) = \varphi(m),$$

则 $a$ 叫作 $m$ 的**原根**.

在例 4.1.1 中，由于$\varphi(11) =10$，故 2, 6, 7, 8 是 11 的原根.

**例 4.2.1** 5 是否是 6 的原根?是否是 8 的原根?

**解** 由于 5 与 6 互素，$\varphi(6) =2$，又

$$5^1 \equiv 5, \quad 5^2 \equiv 1 \pmod 6,$$

故 $\mathrm{ord}_6(5) = \varphi(6)$，即 5 是 6 的原根.

由于 5 与 8 互素，$\varphi(8) =4$，又

$$5^1 \equiv 5, \quad 5^2 \equiv 1 \pmod 8,$$

故 $\mathrm{ord}_8(5) = 2 \neq \varphi(8)$，即 5 不是 8 的原根.

□

在下面的讨论中，基于与上一节同样的道理，当我们谈到"$a$ 是否为 $m$ 的原根"的问题时，即使没有明确陈述定义中的条件"$m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的整数"，我们仍然暗含地假设这个条件成立，这样我们的陈述将变得简洁易记忆.

**定理 4.2.1** $a$ 是 $m$ 的原根的充要条件是

$$1, a, a^2, \dots, a^{\varphi(m)-1}$$

是模 $m$ 的一个缩系.

**证明** 先证必要性. 若 $a$ 是 $m$ 的原根，则

$$\mathrm{ord}_m(a) = \varphi(m),$$

根据定理 4.1.4，可知

$$1, a, a^2, \dots, a^{\varphi(m)-1}$$

两两模 $m$ 不同余. 又因为 $a$ 与 $m$ 互素，所以 $a$ 的任意非负整数次幂都与 $m$ 互素，因此这 $\varphi(m)$ 个数组成模 $m$ 的一个缩系.

再证充分性. 若

$$1, a, a^2, \dots, a^{\varphi(m)-1}$$

这 $\varphi(m)$ 个数是模 $m$ 的一个缩系，则 $a$ 与 $m$ 互素，而且这 $\varphi(m)$ 个数之间两两不同余. 所以这 $\varphi(m)$ 个数中，除了 1 以外, 其他 $\varphi(m)-1$ 个数都与 1 不同余，即对任一整数 $s$，$1\leqslant s\leqslant \varphi(m)-1$，$a^s$ 与 1 模 $m$ 不同余. 根据欧拉定理,

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

所以由次数的定义可知

$$\mathrm{ord}_m(a) = \varphi(m),$$

即 $a$ 是 $m$ 的原根. 定理得证.

□

**定理 4.2.2** 设 $a$ 是 $m$ 的一个原根，$t$ 是非负整数，则 $a^t$ 也是 $m$ 的原根的充要条件是$(t, \varphi(m)) = 1$.

**证明** 因为 $\mathrm{ord}_m(a) = \varphi(m)$，所以由定理 4.1.6 可知，$\mathrm{ord}_m(a^t) = \mathrm{ord}_m(a) = \varphi(m)$ 的充要条件是$(t, \mathrm{ord}_m(a)) = (t, \varphi(m)) = 1$. 即 $a^t$ 是 $m$ 的原根的充要条件是$(t, \varphi(m)) = 1$. 定理得证.

□

**定理 4.2.3** 设 $a$ 是 $m$ 的一个原根，则 $m$ 恰有 $\varphi(\varphi(m))$ 个模 $m$ 不同余的原根.

**证明** 由于 $a$ 是 $m$ 的原根，故 $\varphi(m)$ 个整数

$$1, a, a^2, \dots, a^{\varphi(m)-1}$$

构成模 $m$ 的一个缩系. 根据定理 4.2.2，$a^t$ 是 $m$ 的原根当且仅当$(t, \varphi(m)) = 1$. 因为这样的 $t$ 共有 $\varphi(\varphi(m))$ 个，所以 $m$ 恰有 $\varphi(\varphi(m))$ 个模 $m$ 不同余的原根. 定理得证.

□

**例 4.2.2**　在例 4.1.5 中, 模 13 的原根是 2, 6, 7, 11，共 4 个原根，易验证

$$\varphi(\varphi(13)) = \varphi(12) = \varphi(3\times 2^2) = 2\times 2 = 4.$$

□

**例 4.2.3**　试求 8 的原根.

**解**　先求出 $\varphi(8)=4$．易知

$$\mathrm{ord}_8(1) = 1，\ \mathrm{ord}_8(3) = 2，\ \mathrm{ord}_8(5) = 2，\mathrm{ord}_8(7) = 2,$$

因此不存在 8 的原根.

□

由这个例子看出，对任意模数 $m$ 来说，不一定存在原根. 下面我们重点讨论原根的存在性问题．正式讨论之前，作为预备内容，我们先来证明两个定理.

**定理 4.2.4**　设 $a$ 和 $b$ 对模 $m$ 的次数分别是 $\mathrm{ord}_m(a)$和 $\mathrm{ord}_m(b)$，则

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

的充要条件是

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

**证明**　由于$(a, m) = 1$，$(b, m) = 1$，故$(ab, m) = 1$，且存在 $\mathrm{ord}_m(ab)$.

先证必要性．由

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

可知 $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)\mathrm{ord}_m(ab)$, 又$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，所以 $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(ab)$.

同理可证 $\mathrm{ord}_m(b)\mid\mathrm{ord}_m(ab)$．由于$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，所以 $\mathrm{ord}_m(a)\mathrm{ord}_m(b)\mid\mathrm{ord}_m(ab)$.

另一方面，由

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

可知 $\mathrm{ord}_m(ab)\mid\mathrm{ord}_m(a)\mathrm{ord}_m(b)$．所以

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

再证充分性．由

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

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

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

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

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

定理得证.

□

**定理 4.2.5**　设 $a$ 和 $b$ 对模 $m$ 的次数分别是 $\mathrm{ord}_m(a)$和 $\mathrm{ord}_m(b)$，则存在整数 $c$，使得

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

**证明**　因为对于整数 $\mathrm{ord}_m(a)$和 $\mathrm{ord}_m(b)$，存在整数 $u, v$ 满足

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

并使得

$$(u, v) = 1, \qquad uv = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

令

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

则

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

又由定理 4.2.4 可知

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

于是，取 $c \equiv a^s b^t \pmod m$即可．定理得证.

□

到这里，我们就可以得到第一个原根存在性定理如下.

**定理 4.2.6** 设 $p$ 是奇素数，则 $p$ 的原根存在.

**证明** 在模 $p$ 的缩系 $1, 2, \cdots, p-1$ 中，记

$$u_r = \mathrm{ord}_p(r), \quad 1 \leqslant r \leqslant p-1,$$

令 $u = [u_1, u_2, \cdots, u_{p-1}]$．反复应用定理 4.2.5 可知，存在整数 $g$，使得

$$\mathrm{ord}_p(g) = u.$$

根据定理 4.1.2(1)，可知 $u \mid \varphi(p)$，即 $u \mid p-1$，所以 $u \leqslant p-1$.

由于

$$r^{u_r} \equiv 1 \pmod p, \quad 1 \leqslant r \leqslant p-1,$$

又 $u_r \mid u$，故

$$r^u \equiv 1 \pmod p, \quad 1 \leqslant r \leqslant p-1,$$

即同余方程

$$x^u \equiv 1 \pmod p,$$

至少有 $p-1$ 个解

$$x \equiv 1, 2, \cdots, p-1 \pmod p.$$

又根据拉格朗日关于同余方程解的数量的定理 3.7.4 可知，该方程至多有 $u$ 个解，所以 $p-1 \leqslant u$.

因此，我们有 $u = p-1$，即 $\mathrm{ord}_p(g) = u = p-1 = \varphi(p)$．所以 $g$ 是 $p$ 的原根．定理得证.

□

**定理 4.2.7** 设 $g$ 是奇素数 $p$ 的一个原根，且满足

$$g^{p-1} \not\equiv 1 \pmod{p^2},$$

则对每一个 $l \geqslant 2$，有

$$g^{\varphi(p^{l-1})} \not\equiv 1 \pmod{p^l}.$$

**证明** 对 $l$ 用数学归纳法．当 $l = 2$ 时，即为题设 $g^{p-1} \not\equiv 1 \pmod{p^2}$，显然成立．

假设定理对 $l$（$l \geqslant 2$）成立，即

$$g^{\varphi(p^{l-1})} \not\equiv 1 \pmod{p^l}.$$

由欧拉定理可知

$$g^{\varphi(p^{l-1})} \equiv 1 \pmod{p^{l-1}}.$$

所以存在整数 $k$ 使得

$$g^{\varphi(p^{l-1})} = 1 + kp^{l-1},$$

由归纳假设可知，其中 $k$ 不能被 $p$ 整除(否则，如果 $k=k_1p$，那么 $g^{\varphi(p^{l-1})}=1+k_1pp^{l-1}=1+k_1p^l$，即 $g^{\varphi(p^{l-1})} \equiv 1 \pmod{p^l}$，这与归纳假设矛盾)．将上式两端分别取 $p$ 次方，可得

$$\begin{aligned}(g^{\varphi(p^{l-1})})^p &= (g^{p^{l-1}-p^{l-2}})^p = g^{p^l-p^{l-1}} \\ &= g^{\varphi(p^l)} = (1+kp^{l-1})^p = 1+kp^l + k^2\frac{p(p-1)}{2}p^{2(l-1)} + rp^{3(l-1)},\end{aligned}$$

其中 $r$ 是一个整数．由于 $2(l-1) \geqslant l+1$，$3(l-1) \geqslant l+1$，所以上式最右端从第三项起，都能够被 $p^{l+1}$ 整除，因此

$$g^{\varphi(p^l)} \equiv 1 + kp^l \pmod{p^{l+1}}.$$

因为 $k$ 不能被 $p$ 整除，所以有

$$g^{\varphi(p^l)} \not\equiv 1 \pmod{p^{l+1}},$$

于是，定理对 $l+1$ 成立．定理得证．

□

**定理 4.2.8** 设 $p$ 是一个奇素数，则对任意正整数 $l$，存在 $p^l$ 的原根．

**证明** 当 $l = 1$ 时，定理成立，可设 $g$ 为 $p$ 的原根，则有

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

若

$$g^{p-1} - 1 \not\equiv 0 \pmod{p^2},$$

我们取 $r = g$．反之，若

$$g^{p-1} - 1 \equiv 0 \pmod{p^2},$$

我们取 $r = g + p$，由于 $r \equiv g \pmod{p}$，所以 $r$ 也是 $p$ 的原根，且

$$r^{p-1}-1=(g+p)^{p-1}-1=g^{p-1}+(p-1)pg^{p-2}+p^2\text{ 的倍数项}-1 \equiv -pg^{p-2} \not\equiv 0 \pmod{p^2}.$$

即我们总能够找到模 $p$ 的原根 $r$，满足 $r^{p-1} \not\equiv 1 \pmod{p^2}$.

下面我们开始证明 $r$ 即为 $p^l$ ($l \geqslant 2$)的原根．设

$$t = \mathrm{ord}_{p^l}(r),$$

则有

$$r^t \equiv 1 \pmod{p^l},$$

显然也有

$$r^t \equiv 1 \pmod{p}.$$

因为 $r$ 是 $p$ 的原根，所以有 $\varphi(p) \mid t$，于是可记

$$t = \varphi(p)q.$$

由于 $t \mid \varphi(p^l)$，即 $\varphi(p)q \mid \varphi(p^l)$，又

$$\varphi(p^l) = p^{l-1}(p-1), \qquad \varphi(p) = p-1,$$

故有 $q \mid p^{l-1}$.

不妨设 $q = p^k$，其中 $k \leqslant l-1$．若这个不等式严格成立 $k < l-1$，则 $k+1 \leqslant l-1$，即

$$l-k-2 \geqslant 0$$

由

$$t = \varphi(p)p^k = (p-1)p^k = p^{k+1} - p^k, \qquad \varphi(p^{l-1}) = p^{l-1} - p^{l-2} = (p^{k+1} - p^k)p^{l-k-2} = t\,p^{l-k-2},$$

可知

$$t \mid \varphi(p^{l-1}),$$

因此

$$r^{\varphi(p^{l-1})} \equiv 1 \pmod{p^l}.$$

但这个结果显然与定理 4.2.7 矛盾，于是只能 $k = l-1$，即 $t = \varphi(p^l)$．所以 $r$ 是 $p^l$ 的一个原根，定理得证.

□

从该定理看出，素数 $p$ 的原根不一定是 $p^2$ 的原根.

**例 4.2.4**　8 是 3 的原根，但不是 $3^2$ 的原根，因为 $8^2 \equiv 1 \pmod{3^2}$.

□

**定理 4.2.9**　设 $p$ 是一个奇素数，则对任意正整数 $l$，存在 $2p^l$ 的原根.

**证明**　设 $g$ 是 $p^l$ 的一个原根，我们先证当 $g$ 是奇数时，$g$ 也是 $2p^l$ 的一个原根.

因为$(g, p^l) = 1$ 且$(g, 2) = 1$，所以$(g, 2p^l) = 1$, 因此由欧拉定理可知

$$g^{\varphi(2p^l)} \equiv 1 \pmod{2p^l}.$$

设 $t = \mathrm{ord}_{2p^l}(g)$，又因为 $\varphi(2p^l) = \varphi(2)\,\varphi(p^l) = \varphi(p^l)$，故有 $t \mid \varphi(p^l)$.

由

$$g^t \equiv 1 \pmod{2p^l},$$

可知

$$g^t \equiv 1 \pmod{p^l}.$$

又因为 $g$ 是 $p^l$ 的一个原根，所以 $\varphi(p^l) \mid t$.

于是，我们有 $t = \varphi(p^l) = \varphi(2p^l)$，即 $g$ 是 $2p^l$ 的一个原根.

当 $g$ 是偶数时，则 $g + p^l$ 是奇数且为 $p^l$ 的一个原根(因为 $g \equiv g + p^l \pmod{p^l}$)，可类似地按以上证明得出结论. 定理得证.

□

上面讨论了具有原根的一些整数的特征，为了完整地给出具有原根的所有整数的特征，我们还需要排除那些没有原根的整数. 首先下面的定理将说明例 4. 2. 3 中的整数 8 为什么没有原根.

**定理 4.2.10** 设 $a$ 是一个奇数，则对任意整数 $k \geqslant 3$，有

$$a^{\frac{1}{2}\varphi(2^k)} \equiv a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

即 $2^k(k \geqslant 3)$ 没有原根.

**证明** 用数学归纳法. 不妨设 $a = 2b + 1$，则有

$$a^2 = 4b(b+1) + 1 \equiv 1 \pmod{2^3},$$

注意其中 $2 \mid b(b+1)$，而 $\varphi(2^3) = 4$，所以结论对 $k = 3$ 成立.

假设结论对 $k-1\ (k > 3)$成立，则有

$$a^{2^{(k-1)-2}} \equiv 1 \pmod{2^{k-1}},$$

即存在整数 $q$ 使得

$$a^{2^{(k-1)-2}} = 1 + q2^{k-1}.$$

将等式两端分别平方，可得

$$a^{2^{k-2}} = (1 + q2^{k-1})^2 = 1 + (q + 2^{k-2}q^2)2^k,$$

故

$$a^{2^{k-2}} \equiv 1 \pmod{2^k},$$

即结论对 $k$ 成立. 于是定理得证.

□

有了前面的这些定理，我们就不难推出原根存在的充要条件了.

**定理 4.2.11** 设 $m$ 是大于 1 的整数，则 $m$ 的原根存在的充要条件是 $m$ 为 $2, 4, p^l, 2p^l$ 之一，其中 $l \geqslant 1$，$p$ 是奇素数.

**证明** 先证必要性. 设 $m$ 的标准分解式为

$$m = {p_1}^{l_1} \cdot {p_2}^{l_2} \cdot \cdots \cdot {p_s}^{l_s},$$

其中 $p_i < p_j\,(i < j)$. 又设 $a$ 为一与 $m$ 互素的正整数，则必满足

$$(a, {p_i}^{l_i}) = 1,\ \ i = 1,2,\ldots,s.$$

由欧拉定理，可知

$$a^{\varphi(p_i^{l_i})} \equiv 1 \pmod{p_i^{l_i}},\ i = 1,2,\ldots,s.$$

令 $h = [\varphi(p_1^{l_1}), \varphi(p_2^{l_2}), \ldots, \varphi(p_s^{l_s})]$，则

$$a^h \equiv 1 \pmod{p_i^{l_i}},\ \ i = 1,2,\ldots,s.$$

由于 $p_i^{l_i}\,(i = 1,2,\ldots,s)$两两互素，于是$[p_1^{l_1}, p_2^{l_2}, \ldots, p_s^{l_s}] = m$，故有

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

因为 $h \leqslant \varphi(m)$，而当 $h < \varphi(m)$ 时，$m$ 无原根存在，所以，若 $m$ 有原根，则必须

$$h = \varphi(m),$$

即 $\varphi(p_i^{l_i})\,(i = 1,2,\ldots,s)$两两互素.

因为$\varphi(p^l) = p^{l-1}(p-1)$，当 $p$ 为奇素数时，$\varphi(p^l)$ 必为偶数，所以当 $m$ 有两个或两个以上的奇素数因子时，$m$ 无原根. 于是，若使 $m$ 有原根，$m$ 只能具有 $2^k, p^l, 2^t p^l$ 三种形式之一，其中 $k, t, l$ 均为正整数.

若 $t > 1$，则 $\varphi(2^t) = 2^{t-1}$ 与 $\varphi(p^l)$ 不互素，故只能 $t = 1$.

若 $k \geqslant 3$，由定理 4.2.10 显然可知 $2^k$ 无原根存在，故只能 $k = 1$ 或 $k = 2$.

综上所述，若 $m$ 有原根，则 $m$ 只能是 $2, 4, p^l, 2p^l$ 之一，必要性成立.

再证充分性.

当 $m = 2$ 时，$\varphi(2) = 1$，1 即为 2 的原根.

当 $m = 4$ 时，$\varphi(4) = 2$，3 即为 4 的原根.

当 $m = p^l$ 时，由定理 4.2.8 可知 $m$ 的原根存在.

当 $m = 2p^l$ 时，由定理 4.2.9 可知 $m$ 的原根存在.

于是充分性也成立，定理得证.

□

下面我们再给出一种寻找原根的方法.

**定理 4.2.12** 设 $m$ 是大于 2 的整数，$\varphi(m)$ 的所有不同的素因子是 $q_1, q_2, \cdots, q_s$，则与 $m$ 互素的正整数 $g$ 是 $m$ 的一个原根的充要条件是

$$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod{m},\ \ i = 1, 2, \cdots, s.$$

**证明** 先证必要性. 若 $g$ 是 $m$ 的一个原根，则有

$$\mathrm{ord}_m(g) = \varphi(m).$$

而

$$0 < \frac{\varphi(m)}{q_i} < \varphi(m), \ i = 1, 2, \cdots, s,$$

所以

$$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod{m}, \quad i = 1, 2, \cdots, s.$$

再证充分性．用反证法，设

$$\mathrm{ord}_m(g) = v,$$

假定 $g$ 不是 $m$ 的一个原根，则 $v < \varphi(m)$，从而 $v \mid \varphi(m)$．于是存在一个素数 $q$，使得

$$q \mid \frac{\varphi(m)}{v},$$

故又存在一个整数 $u$，使得

$$\frac{\varphi(m)}{v} = qu,$$

即

$$\frac{\varphi(m)}{q} = uv.$$

于是，我们有

$$g^{\frac{\varphi(m)}{q}} = (g^v)^u \equiv 1 \pmod{m},$$

这与所给条件是矛盾的．所以假设不成立，充分性得证．定理得证．

□

当 $m$ 数值比较小的时候，我们可以利用这个定理很快找到 $m$ 的原根．但是，当 $m$ 数值比较大的时候，我们可能很难找到 $\varphi(m)$ 的所有素数因子，这个时候就很难应用该定理了．到目前为止，即使知道 $m$ 有原根，人们也没有找到一个具有普遍性的容易的方法来发现 $m$ 的原根．然而，如果我们已知一个原根，那么其他的所有原根就可以比较容易地计算出来，该方法的根据就是定理 4.2.2.

**例 4.2.5** 求 41 的原根.

**解** 因为 $\varphi(m) = \varphi(41) = 40 = 2^3 \times 5$，所以 $\varphi(m)$ 的素因子是 $q_1 = 5$，$q_2 = 2$，进而

$$\frac{\varphi(m)}{q_1} = 8, \qquad \frac{\varphi(m)}{q_2} = 20.$$

对 $g = 2, 3, \cdots$ 逐个验算 $g^8$ 和 $g^{20}$ 是否与 1 模 $m$ 同余，得

$2^8 \equiv 10 \pmod{41}$，$2^{20} \equiv 1 \pmod{41}$，失败；

$3^8 \equiv 1 \pmod{41}$，失败；

$4^8 \equiv 18 \pmod{41}$，$4^{20} \equiv 1 \pmod{41}$，失败；

$5^8 \equiv 18 \pmod{41}$，$5^{20} \equiv 1 \pmod{41}$，失败；

$6^8 \equiv 10 \pmod{41}$，$6^{20} \equiv 40 \pmod{41}$，成功.

可知 6 是 41 的最小原根.

根据定理 4.2.2，可知当 $t$ 遍历 $\varphi(m)=40$ 的缩系

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

时，$6^t$ 遍历 41 的原根，即

$6^1 \equiv 6 \pmod{41}$, $6^{17} \equiv 26 \pmod{41}$, $6^{31} \equiv 13 \pmod{41}$,

$6^3 \equiv 11 \pmod{41}$, $6^{19} \equiv 34 \pmod{41}$, $6^{33} \equiv 17 \pmod{41}$,

$6^7 \equiv 29 \pmod{41}$, $6^{21} \equiv 35 \pmod{41}$, $6^{37} \equiv 15 \pmod{41}$,

$6^9 \equiv 19 \pmod{41}$, $6^{23} \equiv 30 \pmod{41}$, $6^{39} \equiv 7 \pmod{41}$

$6^{11} \equiv 28 \pmod{41}$, $6^{27} \equiv 12 \pmod{41}$,

$6^{13} \equiv 24 \pmod{41}$, $6^{29} \equiv 22 \pmod{41}$,

所以, 41 的所有原根为：6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

□

## 习题 4.2

**A 组**

1. 求以下素数原根的个数：

(1) 7;　(2) 19;　(3) 29;　(4) 47.

2. 求以下整数的一个原根：

(1) $5^2$;　(2) $13^2$;　(3) 6;　(4) 338.

3. 求以下整数的一个原根，其中 $k$ 是任意的一个正整数：

(1) $11^k$;　(2) $23^k$;　(3) $31^k$;　(4) $37^k$.

4. 求证 3 是 17 的一个原根，找出 17 的最小正剩余系中的所有原根.

5. 28, 47, 55, 59 的原根是否存在？若存在则求出其所有的原根.

6. 求 113 的最小原根.

7. 求 $113^2$ 的最小原根.

8. 证明整数 12 没有原根.

**B 组**

8. 求证如果 $g^k$ 是 $m$ 的原根，那么 $g$ 也是 $m$ 的原根.

9. 设 $a$ 与 $m$ 是互素的正整数，证明如果 $a \not\equiv 1, a^2 \not\equiv 1$, $a^{\frac{p-1}{2}} \not\equiv 1 \bmod m$，则 $a$ 是 $m$ 的原根.

10. 证明整数 $m$ 有一个原根，当且仅当同余方程 $x^2 \equiv 1 \pmod{m}$的唯一解是 $x \equiv \pm 1 \pmod{m}$.

11. 编写程序求解奇素数的原根.

12. 编写程序求解奇素数幂的原根.

## 4.3 指数与高次剩余

如果 $m$ 有一个原根 $g$，则根据定理 4.2.1 可知，

$$1,\ g,\ g^2,\ \dots,\ g^{\varphi(m)-1}$$

是模 $m$ 的一个缩系．因此，对任何一个与 $m$ 互素的整数 $a$，存在唯一的非负整数 $r$，$0\leqslant r<\varphi(m)$，使得

$$g^r \equiv a \pmod m.$$

由于原根具有上述性质，我们可以给出下面的定义.

**定义 4.3.1** 设 $m$ 是大于 1 的整数，$g$ 是 $m$ 的一个原根，$a$ 是与 $m$ 互素的整数，则存在唯一的非负整数 $r$，$0\leqslant r<\varphi(m)$，满足

$$a \equiv g^r \pmod m,$$

于是，我们把 $r$ 叫作以 $g$ 为底 $a$ 对模 $m$ 的**指数**，记作 $\mathrm{ind}_g a$．在不易引起混淆的情况下，可把 $\mathrm{ind}_g a$ 简写成 $\mathrm{ind}\, a$.

显然，根据定义我们有

$$a \equiv g^{\mathrm{ind}_g a} \pmod m.$$

有时，也把指数叫作**离散对数**，记作 $\log_g a$，于是

$$a \equiv g^{\log_g a} \pmod m.$$

**定理 4.3.1** $g$ 是 $m$ 的一个原根，$a$ 是与 $m$ 互素的整数，如果非负整数 $k$ 使得同余式

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

成立，则 $k$ 满足

$$k \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

**证明** 因为

$$g^k \equiv a \equiv g^{\mathrm{ind}_g a} \pmod m,$$

根据定理 4.1.3 可知

$$k \equiv \mathrm{ind}_g a \pmod{\mathrm{ord}_m(g)}.$$

又因为 $g$ 是 $m$ 的一个原根，所以

$$\mathrm{ord}_m(g) = \varphi(m),$$

所以

$$k \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

定理得证.

□

**定理 4.3.2** $g$ 是 $m$ 的一个原根，则

$$g^x \equiv g^y \pmod m$$

成立的充要条件是

$$x \equiv y \pmod{\varphi(m)}$$

成立.

**证明** 直接应用定理 4.1.3 和 $\mathrm{ord}_m(g) = \varphi(m)$，即得证.

□

下面的两个定理给出关于指数的最重要的几个性质.

**定理 4.3.3** $g$ 是 $m$ 的一个原根，整数 $a$ 和 $b$ 均与 $m$ 互素，则

(1) $\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$；$\mathrm{ind}_g g \equiv 1 \pmod{\varphi(m)}$；

(2) $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g a + \mathrm{ind}_g b \pmod{\varphi(m)}$；

(3) $\mathrm{ind}_g a^k \equiv k\mathrm{ind}_g a \pmod{\varphi(m)}$，其中 $k$ 为非负整数.

**证明** (1) 因为

$$g^0 \equiv 1 \pmod{m},$$

根据定理 4.3.1，可知

$$\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}.$$

因为

$$g^1 \equiv g \pmod{m},$$

根据定理 4.3.1，可知

$$\mathrm{ind}_g\, g \equiv 1 \pmod{\varphi(m)}.$$

(2) 因为

$$ab \equiv g^{\mathrm{ind}_g(ab)} \pmod{m}, \quad a \equiv g^{\mathrm{ind}_g a} \pmod{m}, \quad b \equiv g^{\mathrm{ind}_g b} \pmod{m},$$

所以

$$g^{\mathrm{ind}_g(ab)} \equiv g^{\mathrm{ind}_g a + \mathrm{ind}_g b} \pmod{m}.$$

根据定理 4.3.2，可知

$$\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g a + \mathrm{ind}_g b \pmod{\varphi(m)}.$$

(3) 因为

$$a^k \equiv g^{\mathrm{ind}_g a^k} \pmod{m}, \quad a \equiv g^{\mathrm{ind}_g a} \pmod{m},$$

所以

$$g^{\mathrm{ind}_g a^k} \equiv a^k \equiv (g^{\mathrm{ind}_g a})^k \equiv g^{k\mathrm{ind}_g a} \pmod{m}.$$

根据定理 4.3.2，可知

$$\mathrm{ind}_g a^k \equiv k\mathrm{ind}_g a \pmod{\varphi(m)}.$$

定理得证.

□

**定理 4.3.4** $g$ 是 $m$ 的一个原根，整数 $a$ 和 $b$ 均与 $m$ 互素，则 $a \equiv b(\mathrm{mod}\ m)$的充要条件是 $\mathrm{ind}_g a \equiv \mathrm{ind}_g b\ (\mathrm{mod}\ \varphi(m))$.

**证明** 先证必要性. 因为 $a \equiv b(\mathrm{mod}\ m)$，所以

$$g^{\mathrm{ind}_g a} \equiv g^{\mathrm{ind}_g b} (\mathrm{mod}\ m),$$

所以由定理 4.3.2 可知

$$\mathrm{ind}_g a \equiv \mathrm{ind}_g b\ (\mathrm{mod}\ \varphi(m)).$$

再证充分性. 因为 $\mathrm{ind}_g a \equiv \mathrm{ind}_g b\ (\mathrm{mod}\ \varphi(m))$，所以存在整数 $k$ 使得

$$\mathrm{ind}_g a = \mathrm{ind}_g b + k\varphi(m),$$

所以

$$g^{\mathrm{ind}_g a} = g^{\mathrm{ind}_g b + k\varphi(m)} = g^{\mathrm{ind}_g b}(g^{\varphi(m)})^k \equiv g^{\mathrm{ind}_g b}(1)^k = g^{\mathrm{ind}_g b} (\mathrm{mod}\ m)$$

即

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

定理得证.

□

上面两个定理表明指数的性质和实数中的对数的性质非常相似，因此我们可以利用原根做出指数表.

**例 4.3.1** 做模 41 的指数表.

**解** 已知 $g = 6$ 是 41 的原根，且 $\varphi(41) = 40$，直接计算 $g^r\ (\mathrm{mod}\ m)$，$0 \leqslant r \leqslant 39$，即

| | | | | | |
|---|---|---|---|---|---|
| $6^0 \equiv 1$, | $6^1 \equiv 6$, | $6^2 \equiv 36$, | $6^3 \equiv 11$, | $6^4 \equiv 25$, | $6^5 \equiv 27$, |
| $6^6 \equiv 39$, | $6^7 \equiv 29$, | $6^8 \equiv 10$, | $6^9 \equiv 19$, | $6^{10} \equiv 32$, | $6^{11} \equiv 28$, |
| $6^{12} \equiv 4$, | $6^{13} \equiv 24$, | $6^{14} \equiv 21$, | $6^{15} \equiv 3$, | $6^{16} \equiv 18$, | $6^{17} \equiv 26$, |
| $6^{18} \equiv 33$, | $6^{19} \equiv 34$, | $6^{20} \equiv 40$, | $6^{21} \equiv 35$, | $6^{22} \equiv 5$, | $6^{23} \equiv 30$, |
| $6^{24} \equiv 16$, | $6^{25} \equiv 14$, | $6^{26} \equiv 2$, | $6^{27} \equiv 12$, | $6^{28} \equiv 31$, | $6^{29} \equiv 22$, |
| $6^{30} \equiv 9$, | $6^{31} \equiv 13$, | $6^{32} \equiv 37$, | $6^{33} \equiv 17$, | $6^{34} \equiv 20$, | $6^{35} \equiv 38$, |
| $6^{36} \equiv 23$, | $6^{37} \equiv 15$, | $6^{38} \equiv 8$, | $6^{39} \equiv 7$ | $(\mathrm{mod}\ 41)$. | |

下面做出模 41 的指数表，第一行表示 $g^r\ (\mathrm{mod}\ m)$的个位数，第一列表示 $g^r\ (\mathrm{mod}\ m)$的十位数，交叉位置即为 $r$.

| | **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 | | | | | | | | | |

□

我们知道，如果从已知整数 $r$ 来计算 $a \equiv g^r \pmod{m}$很容易，而从已知整数 $a$ 求整数 $r$ 使得 $g^r \equiv a \pmod{m}$有时是很困难的．指数表对我们解决此类问题有一定的帮助．例如，通过查表，我们可以很快地知道以 6 为底 28 对模 41 的指数是 11.

指数表可以用来解一些特殊类型的(高次)同余方程，下面我们就开始讨论这个问题.

**定义 4.3.2** 设 $m$ 是大于 1 的整数，$a$ 是与 $m$ 互素的整数，若 $n$ ($n \geqslant 2$)次同余方程

$$x^n \equiv a \pmod{m}$$

有解，则 $a$ 叫作模 $m$ 的 ***n* 次剩余**．否则，$a$ 叫作模 $m$ 的 ***n* 次非剩余**.

**注意：**当 $n = 2$ 时，我们就可以得到二次剩余的定义．二次剩余在公钥密码中有非常重要的应用价值．其相关理论我们在 3.3~3.5 节已经进行了详细讨论，在此不再赘述.

**定理 4.3.5** $g$ 是 $m$ 的一个原根，$a$ 是与 $m$ 互素的整数，则同余方程

$$x^n \equiv a \pmod{m} \tag{4.3.1}$$

有解的充要条件是$(n, \varphi(m)) \mid \mathrm{ind}_g a$．并且，若此同余方程有解，则解数恰为$(n, \varphi(m))$.

**证明** 我们先来证明同余方程(4.3.1)与同余方程

$$n\,\mathrm{ind}_g x \equiv \mathrm{ind}_g a \pmod{\varphi(m)} \tag{4.3.2}$$

等价．若同余方程(4.3.1)有解，设为

$$x \equiv x_0 \pmod{m},$$

则

$$x_0^n \equiv a \pmod{m},$$

即

$$g^{\mathrm{ind}_g x_0^n} \equiv g^{n\,\mathrm{ind}_g x_0} \equiv g^{\mathrm{ind}_g a} \pmod{m}.$$

由定理 4.3.2 可知

$$n\,\mathrm{ind}_g x_0 \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

反过来，若同余方程(4.3.2)有解，设为

$$x \equiv x_0 \pmod{\varphi(m)},$$

使得

$$n\,\mathrm{ind}_g x_0 \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

由定理 4.3.2 可知

$$g^{n\,\mathrm{ind}_g x_0} \equiv g^{\mathrm{ind}_g x_0^n} \equiv g^{\mathrm{ind}_g a} \pmod{m},$$

即

$$x_0^n \equiv a \pmod{m}.$$

因此，同余方程(4.3.1)与同余方程(4.3.2)等价.

由于对任一给定整数 $X$，同余方程

$$X \equiv \mathrm{ind}_g x \pmod{\varphi(m)}$$

总有解，故(4.3.2)有解的充要条件是

$$nX \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$$

有解．又根据定理 3.5.2，可知同余方程(4.3.1)有解的充要条件是$(n, \varphi(m)) \mid \mathrm{ind}_g a$．并且，若此同余方程有解，则解数恰为$(n, \varphi(m))$．定理得证.

□

**定理 4.3.6** $g$ 是 $m$ 的一个原根，$a$ 是与 $m$ 互素的整数，则 $a$ 是模 $m$ 的 $n$ 次剩余的充要条件是

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

**证明** 根据定理 4.3.5 可知

$$x^n \equiv a \pmod{m}$$

有解的充要条件是 $d \mid \mathrm{ind}_g a$，即

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

而这个式子的一个等价式(充要条件)为

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

由定理 4.3.2，可得其充要条件为

$$g^{\frac{\phi(m)}{d}\mathrm{ind}_g a} \equiv a^{\frac{\phi(m)}{d}} \equiv g^0 \equiv 1 \pmod{m},$$

于是定理得证.

□

**定理 4.3.7** $a$ 是与素数 $p$ 互素的整数，则 $a$ 是模 $p$ 的 2 次剩余的充要条件是

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

**证明** 略．这个定理就是上面定理 4.3.6 的推论.

□

**例 4.3.2** 求解同余方程

$$x^{12} \equiv 37 \pmod{41}.$$

**解** 因为$\varphi(41) = 40$，$d = (12, 40) = 4$，查模 41 的指数表得到 $\mathrm{ind}_g 37 = 32$，所以根据 $4 \mid 32$ 可知同余方程有解．由于原同余方程与

$$12\mathrm{ind}_g x \equiv \mathrm{ind}_g 37 = 32 \pmod{40}$$

等价，即

$$3\mathrm{ind}_g x \equiv 8 \pmod{10},$$

由于 3 模 10 的逆元是 7，所以两边同时乘以 7 得到

$$\mathrm{ind}_g x \equiv 56 \equiv 6 \pmod{10},$$

可解得

$$\mathrm{ind}_g x \equiv 6, 16, 26, 36 \pmod{40},$$

故通过查模 41 的指数表可得到原同余方程的解为 $x\equiv 39, 18, 2, 23 \pmod{41}$.

□

## 习题 4.3

**A 组**

1. 已知 2 是 19 的原根，构造 19 的指数表，并求出如下各方程的最小正剩余解:

（1）$8x^4\equiv 3 \pmod{19}$;

（2）$5x^3\equiv 2 \pmod{19}$;

（3）$x^7\equiv 1 \pmod{19}$.

2. 已知 3 是 17 的原根， 构造 17 的指数表， 并求出满足如下各方程的整数 $x$:

（1）$3^x\equiv 7 \pmod{17}$;

（2）$3^x\equiv x \pmod{17}$.

3. 求以下同余方程的所有解：

(1) $3^x \equiv 2 \pmod{23}$　　(2) $13^x \equiv 5 \pmod{23}$

4. 求出使同余方程 $8x^7=a \pmod{29}$有解的 $a$ 值.

**B 组**

5. 求解同余方程 $x^{22}\equiv 5 \pmod{41}$.

6. 求同余方程 $x^x \equiv x \pmod{23}$ 的所有解.

7. 证明如果 $p$ 是一个以 $g$ 为原根的奇素数，则 $\mathrm{ind}_g(p-1)=\dfrac{p-1}{2}$.

8. 设 $p$ 为奇素数，证明同余方程 $x^4 \equiv -1 \pmod{p}$ 有解当且仅当 $p$ 的形式为 $8k+1$.

9. 设 $e\geqslant 2$ 是一个正整数，证明如果 $k$ 是一个正奇数，则每个奇数 $a$ 都是 $2e$ 的一个 $k$ 次剩余.

10. 设 $p$ 为奇素数，编写程序构造 $p$ 的指数表，并由此求解 $n$ 次同余方程 $x^n \equiv a \pmod{p}$ .

11. 设 $p$ 为奇素数，编写程序构造 $p$ 的指数表，并由此快速计算 $ab \bmod p$ .

12. 编写程序求解形式为 $ax^b \equiv c \pmod{m}$ 的同余方程，其中 $a$ 和 $b$ 是整数, $c$ 和 $m$ 是正整数且 $m$ 有原根.

13. 编写程序求具有原根的正整数 $m$ 的 $k$ 次剩余，其中 $k$ 是正整数.