第五章 原根

1. 整数的阶

2. 原根

3. 一般既约剩余系的构造

4. 离散对数

前面的讨论都直接或间接与既约剩余系有关, 因此如果既约剩余系能够很简单的表出, 那么很多问题就可能得到简化.

前面的讨论都直接或间接与既约剩余系有关, 因此如果既约剩余系能够很简单的表出, 那么很多问题就可能得到简化.

为此, 在本章中我们介绍阶, 原根和离散对数等重要概念, 证明原根存在的充要条件, 并给出一般既约剩余系的构造方法.

在本节, 我们引进阶的概念, 并给出它的求法.

在本节, 我们引进阶的概念, 并给出它的求法.

由欧拉定理我们知道, 对任意正整数 m, 如果整数 a 满足 $(a,m)=1$, 那么必有 $a^{\phi(m)} \equiv 1 \pmod{m}$. 基于这一事实, 我们有下面的定义.

在本节, 我们引进阶的概念, 并给出它的求法.

由欧拉定理我们知道, 对任意正整数 m, 如果整数 a 满足 $(a,m)=1$, 那么必有 $a^{\phi(m)} \equiv 1 \pmod{m}$. 基于这一事实, 我们有下面的定义.

定义 1.1. 设 $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ 且 $(a,m)=1$, 如果 l 是使

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

成立的最小正整数, 则称 l 为 a 关于模 m 的**阶**(order), 记为 $\mathrm{ord}_m a$.

在本节, 我们引进阶的概念, 并给出它的求法.

由欧拉定理我们知道, 对任意正整数 m, 如果整数 a 满足 $(a, m) = 1$, 那么必有 $a^{\phi(m)} \equiv 1 \pmod{m}$. 基于这一事实, 我们有下面的定义.

定义 1.1. 设 $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ 且 $(a, m) = 1$, 如果 l 是使

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

成立的最小正整数, 则称 l 为 a 关于模 m 的**阶**(order), 记为 $\mathrm{ord}_m a$.

由定义, 如果 $a \equiv b \pmod{m}$, 那么显然有 $\mathrm{ord}_m a = \mathrm{ord}_m b$.

定理 1.1. 设 $\mathrm{ord}_m a = l$, 整数 $n \geq 0$, 则 $a^n \equiv 1 \pmod{m}$ 当且仅当 $l|n$. 特别地, $l|\phi(m)$.

定理 1.1. 设 $\mathrm{ord}_m a = l$, 整数 $n \geq 0$, 则 $a^n \equiv 1 \pmod{m}$ 当且仅当 $l|n$. 特别地, $l|\phi(m)$.

证明: 由 $\mathrm{ord}_m a = l$ 知, $a^l \equiv 1 \pmod{m}$.

定理 1.1. 设 $\mathrm{ord}_m a = l$, 整数 $n \geq 0$, 则 $a^n \equiv 1 \pmod{m}$ 当且仅当 $l|n$. 特别地, $l|\phi(m)$.

证明: 由 $\mathrm{ord}_m a = l$ 知, $a^l \equiv 1 \pmod{m}$.

下面证明定理的充分性. 假设 $l|n$, 不妨设 $n = lk$. 因为

$$a^n - 1 = a^{lk} - 1 = (a^l - 1)(a^{l(k-1)} + \cdots + a + 1),$$

又 $a^l \equiv 1 \pmod{m}$, 所以有 $a^n \equiv 1 \pmod{m}$.

定理 1.1. 设 $\mathrm{ord}_m a = l$, 整数 $n \geq 0$, 则 $a^n \equiv 1 \pmod{m}$ 当且仅当 $l|n$. 特别地, $l|\phi(m)$.

证明: 由 $\mathrm{ord}_m a = l$ 知, $a^l \equiv 1 \pmod{m}$.

下面证明定理的充分性. 假设 $l|n$, 不妨设 $n = lk$. 因为

$$a^n - 1 = a^{lk} - 1 = (a^l - 1)(a^{l(k-1)} + \cdots + a + 1),$$

又 $a^l \equiv 1 \pmod{m}$, 所以有 $a^n \equiv 1 \pmod{m}$.

下证必要性. 假设 $n = ql + r$, 其中 $0 \leq r < l$. 则由 $a^n \equiv a^l \equiv 1 \pmod{m}$ 有

$$1 \equiv a^n = a^{ql+r} = a^{ql} \cdot a^r = (a^l)^q \cdot a^r \equiv a^r \pmod{m},$$

即 $a^r \equiv 1 \pmod{m}$. 于是由阶的定义知, $r = 0$, 故 $l|n$. 由欧拉定理, $l|\phi(m)$ 是显然的, 因此定理成立. □

例 1.1. 求 $\mathrm{ord}_7 2$ 和 $\mathrm{ord}_7 3$.

例 1.1. 求 $\mathrm{ord}_7 2$ 和 $\mathrm{ord}_7 3$.

解: 直接计算知

$$2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 \equiv 1 \pmod 7,$$

所以 $\mathrm{ord}_7 2 = 3$.

例 1.1. 求 $\mathrm{ord}_7 2$ 和 $\mathrm{ord}_7 3$.

解: 直接计算知

$$2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 \equiv 1 \pmod 7,$$

所以 $\mathrm{ord}_7 2 = 3$.

同理, 因为

$$3^1 \equiv 3 \pmod 7, \quad 3^2 \equiv 2 \pmod 7, \quad 3^3 \equiv 6 \pmod 7,$$
$$3^4 \equiv 4 \pmod 7, \quad 3^5 \equiv 5 \pmod 7, \quad 3^6 \equiv 1 \pmod 7,$$

所以 $\mathrm{ord}_7 3 = 6$.

例 1.1. 求 $\mathrm{ord}_7 2$ 和 $\mathrm{ord}_7 3$.

解: 直接计算知

$$2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 \equiv 1 \pmod 7,$$

所以 $\mathrm{ord}_7 2 = 3$.

同理, 因为

$$3^1 \equiv 3 \pmod 7, \quad 3^2 \equiv 2 \pmod 7, \quad 3^3 \equiv 6 \pmod 7,$$

$$3^4 \equiv 4 \pmod 7, \quad 3^5 \equiv 5 \pmod 7, \quad 3^6 \equiv 1 \pmod 7,$$

所以 $\mathrm{ord}_7 3 = 6$.

事实上, 因为 $\phi(7) = 6$, 所以由定理1.1知
$\mathrm{ord}_7 2, \mathrm{ord}_7 3 \in \{1, 2, 3, 6\}$, 因此在求 $\mathrm{ord}_7 3$ 时可以不计算 3^4 和 3^5. □

利用阶, 我们有时可以判断一个数是否是一个指数方程的解.

利用阶, 我们有时可以判断一个数是否是一个指数方程的解.

例 1.2. 判断 $x_1 = 10$ 和 $x_2 = 15$ 是否是 $2^x \equiv 1 \pmod 7$ 的解.

利用阶, 我们有时可以判断一个数是否是一个指数方程的解.

例 1.2. 判断 $x_1 = 10$ 和 $x_2 = 15$ 是否是 $2^x \equiv 1 \pmod 7$ 的解.

解: 在例1.1中, 我们已经得到 $\mathrm{ord}_7 2 = 3$. 而由定理1.1知, 非负整数 n 是 $2^x \equiv 1 \pmod 7$ 的解当且仅当 $3|n$. 因此 $x_1 = 10$ 不是 $2^x \equiv 1 \pmod 7$ 的解, 而 $x_2 = 15$ 是 $2^x \equiv 1 \pmod 7$ 的解. □

定理 1.2. 设 $\mathrm{ord}_m a = l$, i 和 j 为非负整数, 则 $a^i \equiv a^j \pmod{m}$ 当且仅当 $i \equiv j \pmod{l}$.

定理 1.2. 设 $\mathrm{ord}_m a = l$, i 和 j 为非负整数, 则 $a^i \equiv a^j \pmod{m}$ 当且仅当 $i \equiv j \pmod{l}$.

证明: 我们先证充分性. 假设 $i \equiv j \pmod{l}$, $i \geq j \geq 0$, 则存在非负整数 k 使得 $i - j = kl$, 即 $i = kl + j$. 于是有

$$a^i = a^{kl+j} = (a^l)^k \cdot a^j \equiv a^j \pmod{m},$$

即 $a^i \equiv a^j \pmod{m}$.

定理 1.2. 设 $\mathrm{ord}_m a = l$, i 和 j 为非负整数, 则 $a^i \equiv a^j \pmod{m}$ 当且仅当 $i \equiv j \pmod{l}$.

证明: 我们先证充分性. 假设 $i \equiv j \pmod{l}$, $i \geq j \geq 0$, 则存在非负整数 k 使得 $i - j = kl$, 即 $i = kl + j$. 于是有

$$a^i = a^{kl+j} = (a^l)^k \cdot a^j \equiv a^j \pmod{m},$$

即 $a^i \equiv a^j \pmod{m}$.

下证必要性. 假设 $a^i \equiv a^j \pmod{m}$, $i \geq j \geq 0$, 则有

$$a^j(a^{i-j} - 1) \equiv 0 \pmod{m}.$$

因为 $(a, m) = 1$, 所以 $a^{i-j} - 1 \equiv 0 \pmod{m}$, 即 $a^{i-j} \equiv 1 \pmod{m}$. 因为 $i - j \geq 0$, 所以由定理1.1知, $l | i - j$, 即 $i \equiv j \pmod{l}$, 这就证明了定理. □

下面的推论是显然的.

推论 1.1. 设 $\mathrm{ord}_m a = l$, 则 $1, a, a^2, \ldots, a^{l-1}$ 关于模 m 两两互不同余.

定理 1.3. 如果 $\mathrm{ord}_m a = l$, $s \in \mathbb{Z}^+$, 那么

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

定理 1.3. 如果 $\mathrm{ord}_m a = l$, $s \in \mathbb{Z}^+$, 那么

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

证明: 设 $\mathrm{ord}_m a^s = t$, 则有 $a^{st} \equiv 1 \pmod m$. 因为 $\mathrm{ord}_m a = l$, 所以由定理1.1知, $l|st$, 于是 $\frac{l}{(s,l)} | \frac{st}{(s,l)}$. 由于 $\left(\frac{l}{(s,l)}, \frac{s}{(s,l)}\right) = 1$, 所以 $\frac{l}{(s,l)}|t$. 另一方面, 因为

$$(a^s)^{\frac{l}{(s,l)}} = (a^l)^{\frac{s}{(s,l)}} \equiv 1 \pmod m,$$

而 $\mathrm{ord}_m a^s = t$, 所以 $t|\frac{l}{(s,l)}$. 于是, 我们发现 $t = \frac{l}{(s,l)}$ 或 $t = -\frac{l}{(s,l)}$. 因为 t 和 $\frac{l}{(s,l)}$ 都是正数, 所以必然有 $t = \frac{l}{(s,l)}$. 故定理成立. □

由欧拉函数的定义和上面的定理, 下面的推论也是显然的.

推论 1.2. 设 $\mathrm{ord}_m a = l$, 令 $S = \{a^s | (s, l) = 1, 1 \le s \le l\}$, 则 $|S| = \phi(l)$, 且对任意 $b \in S$, 都有 $\mathrm{ord}_m b = l$.

由欧拉函数的定义和上面的定理, 下面的推论也是显然的.

推论 1.2. 设 $\mathrm{ord}_m a = l$, 令 $S = \{a^s | (s,l) = 1, 1 \le s \le l\}$, 则 $|S| = \phi(l)$, 且对任意 $b \in S$, 都有 $\mathrm{ord}_m b = l$.

值得注意的是, 上面推论里 S 中的 $\phi(l)$ 个数, 尽管它们的阶相同, 但是它们关于模 m 两两互不同余.

定理 1.4. 设 p 是素数, $a \in \mathbb{Z}$ 使得 $\mathrm{ord}_p a = l$, 那么有且仅有 $\phi(l)$ 个关于模 p 的阶为 l, 且两两互不同余的数.

定理 1.4. 设 p 是素数, $a \in \mathbb{Z}$ 使得 $\mathrm{ord}_p a = l$, 那么有且仅有 $\phi(l)$ 个关于模 p 的阶为 l, 且两两互不同余的数.

证明: 因为 $\mathrm{ord}_p a = l$, 所以由推论1.1知, $a, a^2, \ldots, a^l$ 关于模 p 两两互不同余. 令 $S = \{a^s | 1 \leq s \leq l, (s, l) = 1\}$, 则由定理1.3知, S 中每个元素的阶均为 l, 因此 S 中的元素给出 $\phi(l)$ 个关于模 p 的阶为 l, 且两两互不同余的数.

定理 1.4. 设 p 是素数, $a \in \mathbb{Z}$ 使得 $\mathrm{ord}_p a = l$, 那么有且仅有 $\phi(l)$ 个关于模 p 的阶为 l, 且两两互不同余的数.

证明: 因为 $\mathrm{ord}_p a = l$, 所以由推论1.1知, $a, a^2, \ldots, a^l$ 关于模 p 两两互不同余. 令 $S = \{a^s | 1 \le s \le l, (s, l) = 1\}$, 则由定理1.3知, S 中每个元素的阶均为 l, 因此 S 中的元素给出 $\phi(l)$ 个关于模 p 的阶为 l, 且两两互不同余的数.

下证不存在其他阶为 l 且与 S 中元素关于模 p 不同余的数. 如前所述, $a, a^2, \ldots, a^l$ 关于模 p 两两互不同余, 所以它们是同余方程 $x^l \equiv 1 \pmod{p}$ 的全部解. 由此可见对 $\forall b \in \mathbb{Z}$, 如果 $\mathrm{ord}_p b = l$, 那么 b 是 $x^l \equiv 1 \pmod{p}$ 的解, 因此 b 必与 $a, a^2, \ldots, a^l$ 中某个数关于模 p 同余. 不妨设 $1 \le k \le l$ 使得 $b \equiv a^k \pmod{p}$. 由定理1.3知, $\mathrm{ord}_p b = \mathrm{ord}_p a^k = l$ 意味着 $(k, l) = 1$, 从而 $a^k \in S$, 即不存在其他阶为 l 且与 S 中元素关于模 p 不同余的数. 故定理成立. □

例如, 当 $p = 7$ 时, 在例1.1中我们已经得到 $\mathrm{ord}_7 3 = 6$, 那么由上面的定理知, 应该存在 $\phi(6) = 2$ 个关于模 7 的阶为 6 且互不同余的数. 由定理1.4的证明知, 当 $(s, 6) = 1$, 即 $s = 1$ 或 5 时, 3 和 3^5 的阶均为 6.

例如, 当 $p=7$ 时, 在例1.1中我们已经得到 $\mathrm{ord}_7 3=6$, 那么由上面的定理知, 应该存在 $\phi(6)=2$ 个关于模 7 的阶为 6 且互不同余的数. 由定理1.4的证明知, 当 $(s,6)=1$, 即 $s=1$ 或 5 时, 3 和 3^5 的阶均为 6.

设 p 是素数, 则由定理1.1知, $\mathrm{ord}_p a|\phi(p)=p-1$, 即一个数关于模 p 的阶一定是 $p-1$ 的因数.

例如, 当 $p=7$ 时, 在例1.1中我们已经得到 $\mathrm{ord}_7 3=6$, 那么由上面的定理知, 应该存在 $\phi(6)=2$ 个关于模 7 的阶为 6 且互不同余的数. 由定理1.4的证明知, 当 $(s,6)=1$, 即 $s=1$ 或 5 时, 3 和 3^5 的阶均为 6.

设 p 是素数, 则由定理1.1知, $\mathrm{ord}_p a|\phi(p)=p-1$, 即一个数关于模 p 的阶一定是 $p-1$ 的因数.

反过来, 对 $p-1$ 的任意正因数 l, 即 $l|p-1$, 存在整数 a 满足 $\mathrm{ord}_p a=l$ 吗?

下面的定理肯定地回答了这个问题.

定理 1.5. 设 p 是素数, $l|p-1$, 则存在 $\phi(l)$ 个关于模 p 的阶为 l 且两两互不同余的数.

定理 1.5. 设 p 是素数, $l|p-1$, 则存在 $\phi(l)$ 个关于模 p 的阶为 l 且两两互不同余的数.

证明: 对任意 $l|p-1$, 用 $f(l)$ 记 $\{1,2,\ldots,p-1\}$ 中关于模 p 阶为 l 的元素个数. 显然, $f(l)\geq 0$. 因为 $\{1,2,\ldots,p-1\}$ 中任一元素的阶都等于 $p-1$ 的某个因数, 所以

$$\sum_{l|p-1} f(l) = p-1. \tag{1}$$

定理 1.5. 设 p 是素数, $l|p-1$, 则存在 $\phi(l)$ 个关于模 p 的阶为 l 且两两互不同余的数.

证明: 对任意 $l|p-1$, 用 $f(l)$ 记 $\{1,2,\ldots,p-1\}$ 中关于模 p 阶为 l 的元素个数. 显然, $f(l)\geq 0$. 因为 $\{1,2,\ldots,p-1\}$ 中任一元素的阶都等于 $p-1$ 的某个因数, 所以

$$\sum_{l|p-1} f(l)=p-1. \tag{1}$$

另一方面, 由欧拉函数有

$$\sum_{l|p-1} \phi(l)=p-1. \tag{2}$$

定理 1.5. 设 p 是素数, $l|p-1$, 则存在 $\phi(l)$ 个关于模 p 的阶为 l 且两两互不同余的数.

证明: 对任意 $l|p-1$, 用 $f(l)$ 记 $\{1,2,\ldots,p-1\}$ 中关于模 p 阶为 l 的元素个数. 显然, $f(l)\geq 0$. 因为 $\{1,2,\ldots,p-1\}$ 中任一元素的阶都等于 $p-1$ 的某个因数, 所以

$$\sum_{l|p-1} f(l) = p-1. \tag{1}$$

另一方面, 由欧拉函数有

$$\sum_{l|p-1} \phi(l) = p-1. \tag{2}$$

而由定理1.4知, 对任意 $l|p-1$, $f(l)=0$ 或 $\phi(l)$, 因此总有 $f(l)\leq\phi(l)$. 于是由 (1) 和 (2) 式得 $\sum_{l|p-1}(\phi(l)-f(l))=0$, 所以有 $f(l)=\phi(l)$. 故定理成立. □

接下来我们讨论阶的求法. 设 $\mathrm{ord}_m a = l$, $d_1, d_2, \ldots, d_s$ 是 $\phi(m)$ 的所有因数. 由于 $l|\phi(m)$, 所以阶 l 可以通过计算 a^{d_1}, a^{d_2}, ···, a^{d_s} 关于模 m 的值求出. 下面的事实可以简化计算.

接下来我们讨论阶的求法. 设 $\mathrm{ord}_m a = l$, $d_1, d_2, \ldots, d_s$ 是 $\phi(m)$ 的所有因数. 由于 $l|\phi(m)$, 所以阶 l 可以通过计算 a^{d_1}, a^{d_2}, ⋯, a^{d_s} 关于模 m 的值求出. 下面的事实可以简化计算.

定理 1.6. 如果 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 m 的标准分解, 那么 $\mathrm{ord}_m a = [\mathrm{ord}_{p_1^{\alpha_1}} a, \mathrm{ord}_{p_2^{\alpha_2}} a, \ldots, \mathrm{ord}_{p_k^{\alpha_k}} a]$.

接下来我们讨论阶的求法. 设 $\mathrm{ord}_m a = l$, $d_1, d_2, \ldots, d_s$ 是 $\phi(m)$ 的所有因数. 由于 $l|\phi(m)$, 所以阶 l 可以通过计算 a^{d_1}, a^{d_2}, ⋯, a^{d_s} 关于模 m 的值求出. 下面的事实可以简化计算.

定理 1.6. 如果 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 m 的标准分解, 那么 $\mathrm{ord}_m a = [\mathrm{ord}_{p_1^{\alpha_1}} a, \mathrm{ord}_{p_2^{\alpha_2}} a, \ldots, \mathrm{ord}_{p_k^{\alpha_k}} a]$.

证明: 设 $l_i = \mathrm{ord}_{p_i^{\alpha_i}} a$, 其中 $i = 1, 2, \ldots, k$, 令 $l = [l_1, l_2, \ldots, l_k]$. 因为对任意 $1 \le i \le k$, 都有 $a^{l_i} \equiv 1 \pmod{p_i^{\alpha_i}}$, 所以对任意 $1 \le i \le k$, 都有 $a^l \equiv 1 \pmod{p_i^{\alpha_i}}$, 于是有 $a^l \equiv 1 \pmod{m}$. 如果 $l \ne \mathrm{ord}_m a$, 则将 $\mathrm{ord}_m a$ 记作 t. 显然, $0 < t < l$. 由 $a^t \equiv 1 \pmod{m}$ 可得 $a^t \equiv 1 \pmod{p_i^{\alpha_i}}$ 对任意 $1 \le i \le k$ 均成立. 因此, 对任意 $1 \le i \le k$, 都有 $l_i | t$, 于是 $[l_1, l_2, \ldots, l_k] | t$, 即 $l | t$, 这与 $0 < t < l$ 矛盾! 故 $l = \mathrm{ord}_m a$. □

例 1.3. 计算 $\mathrm{ord}_{45}2$.

例 1.3. 计算 $\mathrm{ord}_{45}2$.

解: 这里 $m = 45 = 5 \cdot 3^2$, $a = 2$, $\phi(5) = 4$, $\phi(3^2) = 6$. 直接计算知, $\mathrm{ord}_5 2 = 4$, $\mathrm{ord}_{3^2} 2 = 6$, 故由上面的定理得, $\mathrm{ord}_{45}2 = [4, 6] = 12$. □

例 1.3. 计算 $\mathrm{ord}_{45}2$.

解: 这里 $m = 45 = 5 \cdot 3^2$, $a = 2$, $\phi(5) = 4$, $\phi(3^2) = 6$. 直接计算知, $\mathrm{ord}_5 2 = 4$, $\mathrm{ord}_{3^2} 2 = 6$, 故由上面的定理得,
$\mathrm{ord}_{45}2 = [4, 6] = 12$. □

由定理1.6知, 计算 $\mathrm{ord}_m a$ 的关键是计算 a 关于模素数幂的阶. 下面的定理将解决这个问题. 为了定理叙述的方便, 我们需要一个符号 "$\|$": 如果 $p^s | a$, 但是 $p^{s+1} \nmid a$, 那么我们写 $p^s \parallel a$.

定理 1.7. 设 p 是素数, 对任意正整数 i, 记 $\mathrm{ord}_{p^i} a = l_i$, 则 $l_{i+1} = l_i$ 或 $l_{i+1} = pl_i$. 进一步, 设 $p^{i_0} \parallel a^{l_2} - 1$, 则有

$$l_i = \begin{cases} l_2 & \text{若 } 2 \le i \le i_0 \\ p^{i-i_0} l_2 & \text{若 } i > i_0. \end{cases}$$

定理 1.7. 设 p 是素数, 对任意正整数 i, 记 $\mathrm{ord}_{p^i} a = l_i$, 则 $l_{i+1} = l_i$ 或 $l_{i+1} = pl_i$. 进一步, 设 $p^{i_0} \parallel a^{l_2} - 1$, 则有

$$l_i = \begin{cases} l_2 & \text{若 } 2 \le i \le i_0 \\ p^{i-i_0} l_2 & \text{若 } i > i_0. \end{cases}$$

证明: 因为 $\mathrm{ord}_{p^i} a = l_i$, 所以 $a^{l_i} \equiv 1 \pmod{p^i}$. 于是 $(a^{l_i})^k \equiv 1 \pmod{p^i}$ 且

$$\sum_{k=0}^{p-1} (a^{l_i})^k \equiv \sum_{k=0}^{p-1} 1 \equiv p \pmod{p^i},$$

所以 $\sum_{k=0}^{p-1} (a^{l_i})^k \equiv 0 \pmod{p}$. 这样我们得到

$$a^{pl_i} - 1 = (a^{l_i} - 1) \cdot \sum_{k=0}^{p-1} (a^{l_i})^k \equiv 0 \pmod{p^{i+1}},$$

即 $a^{pl_i} \equiv 1 \pmod{p^{i+1}}$, 所以 $l_{i+1} | pl_i$.

另外, 因为 $a^{l_{i+1}} \equiv 1 \pmod{p^{i+1}}$, 所以 $a^{l_{i+1}} \equiv 1 \pmod{p^i}$, 从而有 $l_i | l_{i+1}$. 由 $l_i | l_{i+1}$ 及前面得到的 $l_{i+1} | pl_i$, 不难推出 $l_{i+1} = l_i$ 或 pl_i.

下面证明定理后半部分. 设 $p^{i_0} \parallel a^{l_2} - 1$, 则当 $i = 2, 3, \ldots, i_0$ 时, $p^i | a^{l_2} - 1$, 所以 $l_i | l_2$, 这里 $2 \le i \le i_0$. 另一方面, 当 $2 \le i \le i_0$ 时, 由 $a^{l_i} \equiv 1 \pmod{p^i}$ 知, $a^{l_i} \equiv 1 \pmod{p^2}$, 故 $l_2 | l_i$. 由它及前面证明得到的 $l_i | l_2$ 知, 当 $2 \le i \le i_0$ 时, $l_i = l_2$.

另外, 因为 $a^{l_{i+1}} \equiv 1 \pmod{p^{i+1}}$, 所以 $a^{l_{i+1}} \equiv 1 \pmod{p^i}$, 从而有 $l_i | l_{i+1}$. 由 $l_i | l_{i+1}$ 及前面得到的 $l_{i+1} | pl_i$, 不难推出 $l_{i+1} = l_i$ 或 pl_i.

下面证明定理后半部分. 设 $p^{i_0} \parallel a^{l_2} - 1$, 则当 $i = 2, 3, \ldots, i_0$ 时, $p^i | a^{l_2} - 1$, 所以 $l_i | l_2$, 这里 $2 \le i \le i_0$. 另一方面, 当 $2 \le i \le i_0$ 时, 由 $a^{l_i} \equiv 1 \pmod{p^i}$ 知, $a^{l_i} \equiv 1 \pmod{p^2}$, 故 $l_2 | l_i$. 由它及前面证明得到的 $l_i | l_2$ 知, 当 $2 \le i \le i_0$ 时, $l_i = l_2$.

下面考虑 $i > i_0$ 的情形, 此时 $p^i \nmid a^{l_2} - 1$. 由 $l_{i_0+1} = l_{i_0}$ 或 pl_{i_0} 知, 必须是 $l_{i_0+1} = pl_{i_0}$; 否则有 $l_{i_0+1} = l_{i_0} = l_2$, 从而有 $p^{i_0+1} | a^{l_{i_0+1}} - 1 = a^{l_2} - 1$, 这与 $p^{i_0+1} \nmid a^{l_2} - 1$ 矛盾!

又由 $l_{i_0+2} = l_{i_0+1}$ 或 pl_{i_0+1} 知, 必须是 $l_{i_0+2} = pl_{i_0+1}$; 否则由

$$a^{l_{i_0+2}} - 1 = a^{l_{i_0+1}} - 1 = (a^{l_{i_0}} - 1) \cdot \sum_{k=0}^{p-1} (a^{l_{i_0}})^k \equiv 0 \pmod{p^{i_0+2}} \tag{3}$$

和前面已证的结论

$$\sum_{k=0}^{p-1} (a^{l_{i_0}})^k \equiv p \pmod{p^{i_0}} \tag{4}$$

得

$$a^{l_{i_0}} - 1 \equiv 0 \pmod{p^{i_0+1}}, \tag{5}$$

所以 $l_{i_0+1} | l_{i_0}$, 这与前面得到的 $l_{i_0+1} = pl_{i_0}$ 矛盾!

又由 $l_{i_0+2}=l_{i_0+1}$ 或 pl_{i_0+1} 知, 必须是 $l_{i_0+2}=pl_{i_0+1}$; 否则由

$$a^{l_{i_0+2}}-1=a^{l_{i_0+1}}-1=(a^{l_{i_0}}-1)\cdot\sum_{k=0}^{p-1}(a^{l_{i_0}})^k\equiv 0 \pmod{p^{i_0+2}} \tag{3}$$

和前面已证的结论

$$\sum_{k=0}^{p-1}(a^{l_{i_0}})^k\equiv p \pmod{p^{i_0}} \tag{4}$$

得

$$a^{l_{i_0}}-1\equiv 0 \pmod{p^{i_0+1}}, \tag{5}$$

所以 $l_{i_0+1}|l_{i_0}$, 这与前面得到的 $l_{i_0+1}=pl_{i_0}$ 矛盾!

同理可证, $l_{i_0+3}=pl_{i_0+2}$, $l_{i_0+4}=pl_{i_0+3}$, $\ldots$, 因此

$l_{i_0+1}=pl_{i_0}=pl_2$, $l_{i_0+2}=pl_{i_0+1}=p^2l_2$, $l_{i_0+3}=pl_{i_0+2}=p^3l_2$,

$\ldots$, $l_i=p^{i-i_0}l_2$, 这里 $i>i_0$. 这就完成了定理的证明. □

上面定理的证明中, 多次使用了定理1.1. 在给出例子之前, 我们考察一下定理1.7中的条件. 首先值得注意的是, 定理中假设的是 $p^{i_0} \parallel a^{l_2} - 1$. 一个自然的问题是, 为什么不假设 $p^{i_0} \parallel a^{l_1} - 1$ 呢?

上面定理的证明中, 多次使用了定理1.1. 在给出例子之前, 我们考察一下定理1.7中的条件. 首先值得注意的是, 定理中假设的是 $p^{i_0} \parallel a^{l_2} - 1$. 一个自然的问题是, 为什么不假设 $p^{i_0} \parallel a^{l_1} - 1$ 呢?

事实上, 这是不可行的, 因为在从 (3) 和 (4) 推出 (5) 时, 需要用到 $i \geq 2$ 这一事实. 也可以使用随后的例子验证假设 $p^{i_0} \parallel a^{l_1} - 1$ 时定理结论将是错误的. 另外, 因为我们假设的是 $p^{i_0} \parallel a^{l_2} - 1$, 又因为显然有 $p^{i_2} | a^{l_2} - 1$, 所以 $i_0 \geq 2$. 因此在定理中考虑 $2 \leq i \leq i_0$ 不会有矛盾和遗漏.

上面定理的证明中, 多次使用了定理1.1. 在给出例子之前, 我们考察一下定理1.7中的条件. 首先值得注意的是, 定理中假设的是 $p^{i_0} \parallel a^{l_2} - 1$. 一个自然的问题是, 为什么不假设 $p^{i_0} \parallel a^{l_1} - 1$ 呢?

事实上, 这是不可行的, 因为在从 (3) 和 (4) 推出 (5) 时, 需要用到 $i \geq 2$ 这一事实. 也可以使用随后的例子验证假设 $p^{i_0} \parallel a^{l_1} - 1$ 时定理结论将是错误的. 另外, 因为我们假设的是 $p^{i_0} \parallel a^{l_2} - 1$, 又因为显然有 $p^{i_2} | a^{l_2} - 1$, 所以 $i_0 \geq 2$. 因此在定理中考虑 $2 \leq i \leq i_0$ 不会有矛盾和遗漏.

例 1.4. 设 $a = 7$, $p = 2$, 计算 $\mathrm{ord}_{2^{10}} 7$.

上面定理的证明中, 多次使用了定理1.1. 在给出例子之前, 我们考察一下定理1.7中的条件. 首先值得注意的是, 定理中假设的是 $p^{i_0} \parallel a^{l_2} - 1$. 一个自然的问题是, 为什么不假设 $p^{i_0} \parallel a^{l_1} - 1$ 呢?

事实上, 这是不可行的, 因为在从 (3) 和 (4) 推出 (5) 时, 需要用到 $i \geq 2$ 这一事实. 也可以使用随后的例子验证假设 $p^{i_0} \parallel a^{l_1} - 1$ 时定理结论将是错误的. 另外, 因为我们假设的是 $p^{i_0} \parallel a^{l_2} - 1$, 又因为显然有 $p^{i_2} | a^{l_2} - 1$, 所以 $i_0 \geq 2$. 因此在定理中考虑 $2 \leq i \leq i_0$ 不会有矛盾和遗漏.

例 1.4. 设 $a = 7$, $p = 2$, 计算 $\mathrm{ord}_{2^{10}} 7$.

解: 计算知, $l_1 = \mathrm{ord}_2 7 = 1$, $l_2 = \mathrm{ord}_{2^2} 7 = 2$. 因为 $7^2 - 1 = 48$, $2^4 \parallel 48$, 所以 $i_0 = 4 < 10$, 故 $l_{10} = 2^{10-4} l_2 = 2^6 \cdot 2 = 128$, 即 $\mathrm{ord}_{2^{10}} 7 = 128$. □

1. 整数的阶

2. 原根

3. 一般既约剩余系的构造

4. 离散对数

在前一节我们已经看到, 当 $(a, m) = 1$ 时, 有 $\mathrm{ord}_m a | \phi(m)$, 即 a 关于模 m 的阶一定是 $\phi(m)$ 的因数, 并且由定理1.5知, 当 m 是素数时, 存在 $\phi(m-1)$ 个使得 $\mathrm{ord}_m a = \phi(m)$ 的 a.

在前一节我们已经看到, 当 $(a, m) = 1$ 时, 有 $\mathrm{ord}_m a | \phi(m)$, 即 a 关于模 m 的阶一定是 $\phi(m)$ 的因数, 并且由定理1.5知, 当 m 是素数时, 存在 $\phi(m-1)$ 个使得 $\mathrm{ord}_m a = \phi(m)$ 的 a.

正如我们后面要看到的, 满足 $\mathrm{ord}_m a = \phi(m)$ 的 a 具有一些好的性质, 例如, $\{a, a^2, \ldots, a^{\phi(m)}\}$ 构成模 m 的一个既约剩余系.

在前一节我们已经看到, 当 $(a,m)=1$ 时, 有 $\mathrm{ord}_m a|\phi(m)$, 即 a 关于模 m 的阶一定是 $\phi(m)$ 的因数, 并且由定理1.5知, 当 m 是素数时, 存在 $\phi(m-1)$ 个使得 $\mathrm{ord}_m a=\phi(m)$ 的 a.

正如我们后面要看到的, 满足 $\mathrm{ord}_m a=\phi(m)$ 的 a 具有一些好的性质, 例如, $\{a,a^2,\ldots,a^{\phi(m)}\}$ 构成模 m 的一个既约剩余系.

因此在本节中, 我们研究什么样的 m 会使得存在 a 满足 $\mathrm{ord}_m a=\phi(m)$ 以及如何求相应的 a.

定义 2.1. 设 m 是正整数, $(g,m)=1$. 如果 $\mathrm{ord}_m g=\phi(m)$, 那么称 g 为 m 的一个**原根**.

定义 2.1. 设 m 是正整数, $(g, m) = 1$. 如果 $\mathrm{ord}_m g = \phi(m)$, 那么称 g 为 m 的一个**原根**.

如前所述, 定理1.5已经表明, 对某些 m, 原根的确是存在的.

定义 2.1. 设 m 是正整数, $(g,m)=1$. 如果 $\mathrm{ord}_m g=\phi(m)$, 那么称 g 为 m 的一个**原根**.

如前所述, 定理1.5已经表明, 对某些 m, 原根的确是存在的.

例如, $\mathrm{ord}_7 3=\mathrm{ord}_7 5=6=\phi(7)$, 因此 3 和 5 都是 7 的原根. 而由定理1.4知, 仅有 $\phi(6)=2$ 个关于模 7 的阶为 6 且两两互不同余的整数, 所以 3 和 5 是 7 的全部原根.

定义 2.1. 设 m 是正整数, $(g, m) = 1$. 如果 $\mathrm{ord}_m g = \phi(m)$, 那么称 g 为 m 的一个**原根**.

如前所述, 定理1.5已经表明, 对某些 m, 原根的确是存在的.

例如, $\mathrm{ord}_7 3 = \mathrm{ord}_7 5 = 6 = \phi(7)$, 因此 3 和 5 都是 7 的原根. 而由定理1.4知, 仅有 $\phi(6) = 2$ 个关于模 7 的阶为 6 且两两互不同余的整数, 所以 3 和 5 是 7 的全部原根.

然而, 也并非所有的整数都有原根, 例如 8 就没有原根. 事实上, 小于 8 且与之互素的正整数只有 $1, 3, 5, 7$, 而简单计算则知 $\mathrm{ord}_8 1 = 1$, $\mathrm{ord}_8 3 = \mathrm{ord}_8 5 = \mathrm{ord}_8 7 = 2$, 又因为 $\phi(8) = 2^3 - 2^2 = 4$, 所以 8 没有原根.

定理 2.1. 设 m 是正整数, 则 g 是 m 的原根当且仅当 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 组成模 m 的一个既约剩余系.

定理 2.1. 设 m 是正整数, 则 g 是 m 的原根当且仅当 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 组成模 m 的一个既约剩余系.

证明: $(\Rightarrow)$ 设 g 是 m 的原根, 则由定理1.2知, $g, g^2, \ldots, g^{\phi(m)}$ 中任意两个数关于模 m 两两互不同余. 又因为 g 是 m 的原根, 所以 $(g, m) = 1$. 于是对任意 $1 \leq i \leq \phi(m)$, 都有 $(g^i, m) = 1$, 所以 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 组成模 m 的一个既约剩余系.

定理 2.1. 设 m 是正整数, 则 g 是 m 的原根当且仅当 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 组成模 m 的一个既约剩余系.

证明: $(\Rightarrow)$ 设 g 是 m 的原根, 则由定理1.2知, $g, g^2, \ldots, g^{\phi(m)}$ 中任意两个数关于模 m 两两互不同余. 又因为 g 是 m 的原根, 所以 $(g, m) = 1$. 于是对任意 $1 \leq i \leq \phi(m)$, 都有 $(g^i, m) = 1$, 所以 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 组成模 m 的一个既约剩余系.

$(\Leftarrow)$ 设 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 是模 m 的一个既约剩余系, 则有 $(g, m) = 1$. 因此由欧拉定理知, $g^{\phi(m)} \equiv 1 \pmod{m}$. 因为 m 的既约剩余系中的任意两个数关于模 m 都是互不同余的, 所以对任意 $1 \leq i < \phi(m)$, 都有 $g^i \not\equiv 1 \pmod{m}$. 因此 $\mathrm{ord}_m g = \phi(m)$, 即 g 是 m 的原根. □

例如, 因为 $\phi(9) = 6$ 且 $\{2, 2^2, \ldots, 2^6\}$ 是模 9 的一个既约剩余系, 所以由定理2.1知, 2 是 9 的一个原根.

例如, 因为 $\phi(9)=6$ 且 $\{2,2^2,\ldots,2^6\}$ 是模 9 的一个既约剩余系, 所以由定理2.1知, 2 是 9 的一个原根.

在给出下一个定理之前, 我们考察一下前 30 个正整数中哪些数存在原根, 看看它们是否有规律可循.

例如, 因为 $\phi(9)=6$ 且 $\{2,2^2,\ldots,2^6\}$ 是模 9 的一个既约剩余系, 所以由定理2.1知, 2 是 9 的一个原根.

在给出下一个定理之前, 我们考察一下前 30 个正整数中哪些数存在原根, 看看它们是否有规律可循.

因为 1 太特殊, 所以我们不予考虑. 剩下的 29 个数中, $2,3,4,5,6,7,9,10,11,\ 13,14,17,18,19,22,23,25,26,27,29$ 都有原根, 而其他数没有原根.
除了每个素数都有原根外, 每个奇素数的幂 $(9,25,27)$ 也都有原根, 但偶素数 2 的方幂中只有 4 有原根; 其他有原根的数是 $6,10,14,18,22,26$, 这些数的共同特点是它们都是奇素数幂的 2 倍的形式.

例如, 因为 $\phi(9)=6$ 且 $\{2,2^2,\ldots,2^6\}$ 是模 9 的一个既约剩余系, 所以由定理2.1知, 2 是 9 的一个原根.

在给出下一个定理之前, 我们考察一下前 30 个正整数中哪些数存在原根, 看看它们是否有规律可循.

因为 1 太特殊, 所以我们不予考虑. 剩下的 29 个数中, $2,3,4,5,6,7,9,10,11,\ 13,14,17,18,19,22,23,25,26,27,29$ 都有原根, 而其他数没有原根.
除了每个素数都有原根外, 每个奇素数的幂 $(9,25,27)$ 也都有原根, 但偶素数 2 的方幂中只有 4 有原根; 其他有原根的数是 $6,10,14,18,22,26$, 这些数的共同特点是它们都是奇素数幂的 2 倍的形式.

因此, 我们可以猜测当 $m=2,4,p^\alpha$ 或 $2p^\alpha$ 时, m 有原根.

定理 2.2. 设整数 $m > 1$, 如果 m 有原根, 那么 m 必为下列诸数之一:

$$2,\ 4,\ p^{\alpha},\ 2p^{\alpha},$$

这里 p 为奇素数, α 为正整数.

定理 2.2. 设整数 $m > 1$, 如果 m 有原根, 那么 m 必为下列诸数之一:

$$2,\ 4,\ p^{\alpha},\ 2p^{\alpha},$$

这里 p 为奇素数, α 为正整数.

证明: 设 m 的标准分解式为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. 对任意正整数 a, 如果 $(a, m) = 1$, 那么 $(a,\ p_i^{\alpha_i}) = 1$. 因此由欧拉定理得, $a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$, 这里 $1 \le i \le k$. 令 $\alpha = [\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}), \ldots, \phi(p_k^{\alpha_k})]$, 则有 $a^{\alpha} \equiv 1 \pmod{p_i^{\alpha_i}}$, 其中 $1 \le i \le k$, 于是 $a^{\alpha} \equiv 1 \pmod{m}$, 故 $\mathrm{ord}_m a \le \alpha$.

另一方面, $\phi(m) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\cdots\phi(p_k^{\alpha_k}) \geq \alpha$. 因为当 $\phi(m) > \alpha$ 时, 我们有 $\mathrm{ord}_m a < \phi(m)$, 所以此时 m 没有原根. 因此 m 若有原根, 则必须满足 $\phi(m) = \alpha$, 这等价于 $\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}), \ldots, \phi(p_k^{\alpha_k})$ 两两互素. 由于对任意奇素数 p, $\phi(p^\alpha)$ 均为偶数, 所以当 m 有两个不同的奇素因数时, m 没有原根. 这意味着 m 若有原根, 则必为 2^s, p^α 或 $2^t p^\alpha$ $(s > 0, \alpha > 0, t > 0)$ 三种形式之一.

另一方面, $\phi(m) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\cdots\phi(p_k^{\alpha_k}) \geq \alpha$. 因为当 $\phi(m) > \alpha$ 时, 我们有 $\mathrm{ord}_m a < \phi(m)$, 所以此时 m 没有原根. 因此 m 若有原根, 则必须满足 $\phi(m) = \alpha$, 这等价于 $\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}), \ldots, \phi(p_k^{\alpha_k})$ 两两互素. 由于对任意奇素数 p, $\phi(p^\alpha)$ 均为偶数, 所以当 m 有两个不同的奇素因数时, m 没有原根. 这意味着 m 若有原根, 则必为 2^s, p^α 或 $2^t p^\alpha$ $(s > 0, \alpha > 0, t > 0)$ 三种形式之一.

如果 $t > 1$, 那么 $\phi(2^t) = 2^t - 2^{t-1} = 2^{t-1}$ 与 $\phi(p^\alpha)$ 将不互素, 因此 $t = 1$.

下证 $s \geq 3$ 时, $m = 2^s$ 没有原根. 首先, 我们归纳证明: 对任意奇数 a, 当 $s \geq 3$ 时,

$$a^{2^{s-2}} \equiv 1 \pmod{2^s}. \tag{6}$$

下证 $s \geq 3$ 时, $m = 2^s$ 没有原根. 首先, 我们归纳证明: 对任意奇数 a, 当 $s \geq 3$ 时,

$$a^{2^{s-2}} \equiv 1 \pmod{2^s}. \tag{6}$$

事实上, 当 a 为奇数时, 显然有 $a^2 \equiv 1 \pmod{2^3}$, 所以 $s = 3$ 时 (6) 成立. 归纳假设 $a^{2^{s-3}} \equiv 1 \pmod{2^{s-1}}$ 成立, 则存在 $l \in \mathbb{Z}$ 使得 $a^{2^{s-3}} = 1 + 2^{s-1}l$. 于是有

$$a^{2^{s-2}} = \left(a^{2^{s-3}}\right)^2 = (1+2^{s-1}l)^2 = 1+2^sl+2^{2(s-1)}l^2 \equiv 1 \pmod{2^s}.$$

因此, 对任意奇数 a, 当 $s \geq 3$ 时, (6) 成立. 另一方面, 因为 $\phi(2^s) = 2^s - 2^{s-1} = 2^{s-1} > 2^{s-2}$, 所以当 $s \geq 3$ 时, $m = 2^s$ 没有原根.

下证 $s \geq 3$ 时, $m = 2^s$ 没有原根. 首先, 我们归纳证明: 对任意奇数 a, 当 $s \geq 3$ 时,

$$a^{2^{s-2}} \equiv 1 \pmod{2^s}. \tag{6}$$

事实上, 当 a 为奇数时, 显然有 $a^2 \equiv 1 \pmod{2^3}$, 所以 $s = 3$ 时 (6) 成立. 归纳假设 $a^{2^{s-3}} \equiv 1 \pmod{2^{s-1}}$ 成立, 则存在 $l \in \mathbb{Z}$ 使得 $a^{2^{s-3}} = 1 + 2^{s-1}l$. 于是有

$$a^{2^{s-2}} = \left(a^{2^{s-3}}\right)^2 = (1+2^{s-1}l)^2 = 1+2^s l+2^{2(s-1)}l^2 \equiv 1 \pmod{2^s}.$$

因此, 对任意奇数 a, 当 $s \geq 3$ 时, (6) 成立. 另一方面, 因为 $\phi(2^s) = 2^s - 2^{s-1} = 2^{s-1} > 2^{s-2}$, 所以当 $s \geq 3$ 时, $m = 2^s$ 没有原根.

综上, 我们证明了 $m \neq 2, 4, p^\alpha, 2p^\alpha$ 时, m 没有原根. 因此定理成立. $\square$

更重要的是, 上面定理的逆定理也是成立的.

定理 2.3. 当 $m = 2, 4, p^\alpha, 2p^\alpha$ (其中 p 为奇素数, α 为正整数) 时, m 有原根.

更重要的是, 上面定理的逆定理也是成立的.

定理 2.3. 当 $m=2,4,p^{\alpha},2p^{\alpha}$ (其中 p 为奇素数, α 为正整数) 时, m 有原根.

因此, 由定理2.2和定理2.3, 我们有下面的推论.

推论 2.1. 设整数 $m>1$, 则 m 有原根当且仅当 $m=2,4,p^{\alpha}$, 或 $2p^{\alpha}$, 这里 p 为奇素数, α 为正整数.

为证明定理2.3, 我们需要下面的引理.

引理 2.1. 设 g 是奇素数 p 的原根且满足

$$g^{\phi(p)} \not\equiv 1 \pmod{p^2}, \tag{7}$$

则对任意整数 $\alpha \geq 2$, 有

$$g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}. \tag{8}$$

为证明定理2.3, 我们需要下面的引理.

引理 2.1. 设 g 是奇素数 p 的原根且满足

$$g^{\phi(p)} \not\equiv 1 \pmod{p^2}, \tag{7}$$

则对任意整数 $\alpha \geq 2$, 有

$$g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}. \tag{8}$$

证明: 对 α 进行归纳证明. 当 $\alpha = 2$ 时, (8) 即 (7), 故引理成立.

为证明定理2.3, 我们需要下面的引理.

引理 2.1. 设 g 是奇素数 p 的原根且满足

$$g^{\phi(p)} \not\equiv 1 \pmod{p^2}, \tag{7}$$

则对任意整数 $\alpha \geq 2$, 有

$$g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}. \tag{8}$$

证明: 对 α 进行归纳证明. 当 $\alpha = 2$ 时, (8) 即 (7), 故引理成立.

假设引理对 α (≥ 2) 成立, 即 $g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}$. 因为 g 是 p 的原根, 所以 $(g, p^{\alpha-1}) = 1$. 于是由欧拉定理得,
$g^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}$, 因此存在 $k \in \mathbb{Z}$ 使得
$g^{\phi(p^{\alpha-1})} = 1 + kp^{\alpha-1}$.

由归纳假设 $g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}$ 知, $p \nmid k$, 从而有

$$\begin{aligned} g^{\phi(p^\alpha)} &= g^{p^\alpha - p^{\alpha-1}} = g^{p\phi(p^{\alpha-1})} = (g^{\phi(p^{\alpha-1})})^p \\ &= (1 + kp^{\alpha-1})^p \\ &= 1 + kp^\alpha + k^2 \cdot \frac{p(p-1)}{2} \cdot p^{2(\alpha-1)} + rp^{3(\alpha-1)}, \quad (9) \end{aligned}$$

这里 $r \in \mathbb{Z}$.

由归纳假设 $g^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}$ 知, $p \nmid k$, 从而有

$$\begin{aligned} g^{\phi(p^\alpha)} &= g^{p^\alpha - p^{\alpha-1}} = g^{p\phi(p^{\alpha-1})} = (g^{\phi(p^{\alpha-1})})^p \\ &= (1+kp^{\alpha-1})^p \\ &= 1 + kp^\alpha + k^2 \cdot \frac{p(p-1)}{2} \cdot p^{2(\alpha-1)} + rp^{3(\alpha-1)}, \quad (9) \end{aligned}$$

这里 $r \in \mathbb{Z}$.

因为 $2(\alpha-1) \geq \alpha+1$, $3(\alpha-1) \geq \alpha+1$, 所以由 (9) 式得

$$g^{\phi(p^\alpha)} \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}}.$$

由前面的论证 $p \nmid k$ 知, $g^{\phi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$, 故 (8) 对 $\alpha+1$ 成立. 这就证明了定理. □

定理2.3的证明：分情况讨论:

(1) $m = 2$ 时, 1 即为 m 的原根.

定理2.3的证明： 分情况讨论:

(1) $m=2$ 时, 1 即为 m 的原根.

(2) $m=4$ 时, 3 即为 m 的原根.

定理2.3的证明：分情况讨论:

(1) $m=2$ 时, 1 即为 m 的原根.

(2) $m=4$ 时, 3 即为 m 的原根.

(3) 设 $m=p^\alpha$, 其中 p 是奇素数, α 是正整数. 当 $\alpha=1$ 时, 由定理1.5我们已经知道 p 存在原根. 设 g 是 p 的一个原根. 下面利用 g 构造 p^α 的原根.

定理2.3的证明: 分情况讨论:

(1) $m=2$ 时, 1 即为 m 的原根.

(2) $m=4$ 时, 3 即为 m 的原根.

(3) 设 $m=p^\alpha$, 其中 p 是奇素数, α 是正整数. 当 $\alpha=1$ 时, 由定理1.5我们已经知道 p 存在原根. 设 g 是 p 的一个原根. 下面利用 g 构造 p^α 的原根. 如果 $g^{\phi(p)} \not\equiv 1 \pmod{p^2}$, 取 $h=g$, 则有 $h^{\phi(p)} \not\equiv 1 \pmod{p^2}$. 如果 $g^{\phi(p)} \equiv 1 \pmod{p^2}$, 取 $h=g+p$, 此时 h 也是 p 的一个原根, 且

$$
\begin{aligned}
h^{\phi(p)}-1 &= h^{p-1}-1=(g+p)^{p-1}-1 \\
&\equiv g^{p-1}+(p-1)pg^{p-2}-1 \\
&\equiv -pg^{p-2} \not\equiv 0 \pmod{p^2},
\end{aligned}
$$

即 $h^{\phi(p)} \not\equiv 1 \pmod{p^2}$. 下证 h 是 p^α $(\alpha \geq 2)$ 的原根.

设 $\mathrm{ord}_{p^\alpha} h = l$, 则有 $h^l \equiv 1 \pmod{p^\alpha}$, 所以 $h^l \equiv 1 \pmod{p}$. 因为 h 是 p 的原根, 所以 $\phi(p)|l$. 设 $l = \phi(p)q$. 因为 $\mathrm{ord}_{p^\alpha} h = l$, 所以 $l|\phi(p^\alpha)$, 即 $\phi(p)q|\phi(p^\alpha)$, 亦即 $(p-1)q|p^{\alpha-1}(p-1)$, 故 $q|p^{\alpha-1}$.

设 $\mathrm{ord}_{p^\alpha} h = l$, 则有 $h^l \equiv 1 \pmod{p^\alpha}$, 所以 $h^l \equiv 1 \pmod{p}$. 因为 h 是 p 的原根, 所以 $\phi(p)|l$. 设 $l = \phi(p)q$. 因为 $\mathrm{ord}_{p^\alpha} h = l$, 所以 $l|\phi(p^\alpha)$, 即 $\phi(p)q|\phi(p^\alpha)$, 亦即 $(p-1)q|p^{\alpha-1}(p-1)$, 故 $q|p^{\alpha-1}$.

设 $q = p^\beta$, 这里 $0 \le \beta \le \alpha - 1$. 若 $\beta < \alpha - 1$, 则由 $l = \phi(p)q$ 知,

$$l = \phi(p)p^\beta = (p-1)p^\beta | p^{\alpha-2}(p-1),$$

因此 $l|\phi(p^{\alpha-1})$. 于是我们有 $h^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$, 这与引理2.1矛盾! 故 $\beta = \alpha - 1$, 从而

$$l = \phi(p)q = \phi(p)p^\beta = (p-1)p^{\alpha-1} = \phi(p^\alpha),$$

因此 h 是 p^α 的原根.

(4) 设 $m = 2p^\alpha$, 其中 p 是奇素数, α 是正整数. 由 3) 知, p^α 有原根. 设 g 是 p^α 的一个原根, 下证当 g 是奇数时, g 也是 $2p^\alpha$ 的原根.

(4) 设 $m = 2p^\alpha$, 其中 p 是奇素数, α 是正整数. 由 3) 知, p^α 有原根. 设 g 是 p^α 的一个原根, 下证当 g 是奇数时, g 也是 $2p^\alpha$ 的原根.

因为 $(g, 2p^\alpha) = 1$, 所以由欧拉定理得 $g^{\phi(2p^\alpha)} \equiv 1 \pmod{2p^\alpha}$. 设 $\mathrm{ord}_{2p^\alpha} g = l$, 则有 $l | \phi(2p^\alpha) = \phi(p^\alpha)$, 即 $l | \phi(p^\alpha)$.

(4) 设 $m = 2p^\alpha$, 其中 p 是奇素数, α 是正整数. 由 3) 知, p^α 有原根. 设 g 是 p^α 的一个原根, 下证当 g 是奇数时, g 也是 $2p^\alpha$ 的原根.

因为 $(g, 2p^\alpha) = 1$, 所以由欧拉定理得 $g^{\phi(2p^\alpha)} \equiv 1 \pmod{2p^\alpha}$. 设 $\mathrm{ord}_{2p^\alpha} g = l$, 则有 $l | \phi(2p^\alpha) = \phi(p^\alpha)$, 即 $l | \phi(p^\alpha)$.

另一方面, 由 $\mathrm{ord}_{2p^\alpha} g = l$ 知, $g^l \equiv 1 \pmod{2p^\alpha}$, 所以 $g^l \equiv 1 \pmod{p^\alpha}$, 从而 $\phi(p^\alpha) | l$.

(4) 设 $m=2p^\alpha$, 其中 p 是奇素数, α 是正整数. 由 3) 知, p^α 有原根. 设 g 是 p^α 的一个原根, 下证当 g 是奇数时, g 也是 $2p^\alpha$ 的原根.

因为 $(g,2p^\alpha)=1$, 所以由欧拉定理得 $g^{\phi(2p^\alpha)}\equiv 1 \pmod{2p^\alpha}$. 设 $\mathrm{ord}_{2p^\alpha}g=l$, 则有 $l|\phi(2p^\alpha)=\phi(p^\alpha)$, 即 $l|\phi(p^\alpha)$.

另一方面, 由 $\mathrm{ord}_{2p^\alpha}g=l$ 知, $g^l\equiv 1 \pmod{2p^\alpha}$, 所以 $g^l\equiv 1 \pmod{p^\alpha}$, 从而 $\phi(p^\alpha)|l$.

因此我们有 $l=\phi(p^\alpha)=\phi(2p^\alpha)$, 故 g 是 $2p^\alpha$ 的原根. 若 g 是偶数, 则考虑 $g+p^\alpha$, 它是 p^α 的一个原根, 且为奇数.

在定理2.3的证明中我们发现, 求 $p^\alpha, 2p^\alpha$ 的原根可以归结为求 p 的原根, 下面的推论明确给出了归结方法.

推论 2.2. 设 p 是一个奇素数.

(1) 如果 g 是 p 的原根, 那么当 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 时, g 是 p^2 的原根; 当 $g^{p-1} \equiv 1 \pmod{p^2}$ 时, $g+p$ 是 p^2 的原根.

在定理2.3的证明中我们发现, 求 $p^\alpha, 2p^\alpha$ 的原根可以归结为求 p 的原根, 下面的推论明确给出了归结方法.

推论 2.2. 设 p 是一个奇素数.

(1) 如果 g 是 p 的原根, 那么当 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 时, g 是 p^2 的原根; 当 $g^{p-1} \equiv 1 \pmod{p^2}$ 时, $g+p$ 是 p^2 的原根.

(2) 如果 g 是 p^2 的原根, 那么 g 也是 p^α $(\alpha \geq 3)$ 的原根.

在定理2.3的证明中我们发现, 求 $p^\alpha, 2p^\alpha$ 的原根可以归结为求 p 的原根, 下面的推论明确给出了归结方法.

推论 2.2. 设 p 是一个奇素数.

(1) 如果 g 是 p 的原根, 那么当 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 时, g 是 p^2 的原根; 当 $g^{p-1} \equiv 1 \pmod{p^2}$ 时, $g+p$ 是 p^2 的原根.

(2) 如果 g 是 p^2 的原根, 那么 g 也是 p^α $(\alpha \geq 3)$ 的原根.

(3) 如果 g 是 p^α $(\alpha \geq 1)$ 的原根, 那么当 g 为奇数时, g 是 $2p^\alpha$ 的原根; 当 g 为偶数时, $g+p^\alpha$ 是 $2p^\alpha$ 的原根.

在定理2.3的证明中我们发现, 求 $p^\alpha, 2p^\alpha$ 的原根可以归结为求 p 的原根, 下面的推论明确给出了归结方法.

推论 2.2. 设 p 是一个奇素数.

(1) 如果 g 是 p 的原根, 那么当 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 时, g 是 p^2 的原根; 当 $g^{p-1} \equiv 1 \pmod{p^2}$ 时, $g+p$ 是 p^2 的原根.

(2) 如果 g 是 p^2 的原根, 那么 g 也是 p^α $(\alpha \geq 3)$ 的原根.

(3) 如果 g 是 p^α $(\alpha \geq 1)$ 的原根, 那么当 g 为奇数时, g 是 $2p^\alpha$ 的原根; 当 g 为偶数时, $g+p^\alpha$ 是 $2p^\alpha$ 的原根.

在定理2.3的证明中我们发现, 求 $p^\alpha, 2p^\alpha$ 的原根可以归结为求 p 的原根, 下面的推论明确给出了归结方法.

推论 2.2. 设 p 是一个奇素数.

(1) 如果 g 是 p 的原根, 那么当 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 时, g 是 p^2 的原根; 当 $g^{p-1} \equiv 1 \pmod{p^2}$ 时, $g+p$ 是 p^2 的原根.

(2) 如果 g 是 p^2 的原根, 那么 g 也是 p^α $(\alpha \geq 3)$ 的原根.

(3) 如果 g 是 p^α $(\alpha \geq 1)$ 的原根, 那么当 g 为奇数时, g 是 $2p^\alpha$ 的原根; 当 g 为偶数时, $g+p^\alpha$ 是 $2p^\alpha$ 的原根.

证明: 直接由定理2.3的证明过程可得. $\square$

下面的定理描述了如何从一个原根构造所有的原根.

定理 2.4. 设 g 是 m 的原根, 则集合

$$S = \{g^s | 1 \leq s \leq \phi(m), (s, \phi(m)) = 1\}$$

中的元素给出 m 的全部原根. 因此, 若 m 有原根, 则 m 恰有 $\phi(\phi(m))$ 个关于模 m 两两互不同余的原根.

下面的定理描述了如何从一个原根构造所有的原根.

定理 2.4. 设 g 是 m 的原根, 则集合

$$S = \{g^s | 1 \leq s \leq \phi(m), (s, \phi(m)) = 1\}$$

中的元素给出 m 的全部原根. 因此, 若 m 有原根, 则 m 恰有 $\phi(\phi(m))$ 个关于模 m 两两互不同余的原根.

证明: 由定理1.3知, 任意 $g^s \in S$, 有

$$\mathrm{ord}_m g^s = \frac{\phi(m)}{(s, \phi(m))} = \phi(m),$$

所以 g^s 是 m 的原根.

下面的定理描述了如何从一个原根构造所有的原根.

定理 2.4. 设 g 是 m 的原根, 则集合

$$S = \{g^s | 1 \le s \le \phi(m), (s, \phi(m)) = 1\}$$

中的元素给出 m 的全部原根. 因此, 若 m 有原根, 则 m 恰有 $\phi(\phi(m))$ 个关于模 m 两两互不同余的原根.

证明: 由定理1.3知, 任意 $g^s \in S$, 有

$$\mathrm{ord}_m g^s = \frac{\phi(m)}{(s, \phi(m))} = \phi(m),$$

所以 g^s 是 m 的原根.

反过来, 设 h 是 m 的任一原根, 则由定理2.1知, $\{h, h^2, \ldots, h^{\phi(m)}\}$ 构成 m 的一个既约剩余系.

因为 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 也是 m 的一个既约剩余系, 所以存在整数 k, $1 \leq k \leq \phi(m)$, 使得 $g^k \equiv h \pmod{m}$, 因此 $\mathrm{ord}_m g^k = \mathrm{ord}_m h = \phi(m)$.

因为 $\{g, g^2, \ldots, g^{\phi(m)}\}$ 也是 m 的一个既约剩余系, 所以存在整数 k, $1 \le k \le \phi(m)$, 使得 $g^k \equiv h \pmod{m}$, 因此 $\mathrm{ord}_m g^k = \mathrm{ord}_m h = \phi(m)$.

另一方面, 由定理1.3, 有

$$\mathrm{ord}_m g^k = \frac{\phi(m)}{(k, \phi(m))},$$

所以 $(k, \phi(m)) = 1$. 因此 h 与 S 中的某个数关于模 m 同余, 又因为 S 中的数关于模 m 两两互不同余, 故 S 给出了 m 的全部互不同余的原根, 它们共 $\phi(\phi(m))$ 个. $\square$

在定理2.1之后, 我们看到 2 是 9 的一个原根, 因此由前面的定理知, 9 恰有 $\phi(\phi(9)) = 2$ 个原根, 相应的

$$S = \{2^s | 1 \leq s \leq \phi(9) = 6, (s, 6) = 1\} = \{2^s | s = 1, 5\} = \{2, 5\},$$

即 $2, 5$ 是 9 的全部原根.

在定理2.1之后, 我们看到 2 是 9 的一个原根, 因此由前面的定理知, 9 恰有 $\phi(\phi(9)) = 2$ 个原根, 相应的

$$S = \{2^s | 1 \leq s \leq \phi(9) = 6, (s, 6) = 1\} = \{2^s | s = 1, 5\} = \{2, 5\},$$

即 $2, 5$ 是 9 的全部原根.

接下来我们讨论如何计算原根. 当 $m = 2$ 或 4 时, m 的原根在前面已经知道了.

在定理2.1之后, 我们看到 2 是 9 的一个原根, 因此由前面的定理知, 9 恰有 $\phi(\phi(9)) = 2$ 个原根, 相应的

$$S = \{2^s | 1 \le s \le \phi(9) = 6, (s, 6) = 1\} = \{2^s | s = 1, 5\} = \{2, 5\},$$

即 $2, 5$ 是 9 的全部原根.

接下来我们讨论如何计算原根. 当 $m = 2$ 或 4 时, m 的原根在前面已经知道了.

下面考虑 $m = p^\alpha, 2p^\alpha$ (其中 p 为奇素数, α 为正整数) 时原根的计算问题. 设 $(g, m) = 1$, 那么判断 g 是否是 m 的原根, 由定理1.1知不必逐一计算 $g, g^2, \ldots, g^{\phi(m)-1}$, 而只需计算 $g^l \bmod m$, 这里 l 是 $\phi(m)$ 的真因数. 基于这样的思想, 我们有下面的定理.

定理 2.5. 设整数 $m > 2$, $(g, m) = 1$, 且设 $p_1, p_2, \ldots, p_k$ 是 $\phi(m)$ 的所有不同的素因数. 则 g 是 m 的原根当且仅当对任意 $1 \leq i \leq k$,

$$g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}. \tag{10}$$

定理 2.5. 设整数 $m > 2$, $(g, m) = 1$, 且设 $p_1, p_2, \ldots, p_k$ 是 $\phi(m)$ 的所有不同的素因数. 则 g 是 m 的原根当且仅当对任意 $1 \le i \le k$,

$$g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}. \tag{10}$$

证明: (必要性) 若 g 是 m 的原根, 则有 $\mathrm{ord}_m g = \phi(m)$. 但是对任意 $1 \le i \le k$, 我们有 $0 < \frac{\phi(m)}{p_i} < \phi(m) < m$, 所以对任意 $1 \le i \le k$, 都有 $g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}$.

定理 2.5. 设整数 $m > 2$, $(g, m) = 1$, 且设 $p_1, p_2, \ldots, p_k$ 是 $\phi(m)$ 的所有不同的素因数. 则 g 是 m 的原根当且仅当对任意 $1 \le i \le k$,

$$g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}. \tag{10}$$

证明: (必要性) 若 g 是 m 的原根, 则有 $\mathrm{ord}_m g = \phi(m)$. 但是对任意 $1 \le i \le k$, 我们有 $0 < \frac{\phi(m)}{p_i} < \phi(m) < m$, 所以对任意 $1 \le i \le k$, 都有 $g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}$.

(充分性) 假设对任意 $1 \le i \le k$, (10) 均成立. 设 $\mathrm{ord}_m g = l$. 若 $l < \phi(m)$, 则因为 $l | \phi(m)$, 所以 $\frac{\phi(m)}{l}$ 是大于 1 的整数. 于是存在 $\phi(m)$ 的素因数 $p_i | \frac{\phi(m)}{l}$, 即存在 $q \in \mathbb{Z}$ 使得 $\frac{\phi(m)}{l} = p_i q$, 亦即 $\frac{\phi(m)}{p_i} = lq$. 因此 $g^{\frac{\phi(m)}{p_i}} = g^{lq} \equiv 1 \pmod{m}$, 这与 (10) 矛盾! 故 $l = \phi(m)$, 即 g 是 m 的一个原根. □

例 2.1. 验证 12 是 41 的原根.

例 2.1. 验证 12 是 41 的原根.

解: 令 $m=41$, 则 $\phi(m)=2^3\cdot 5$, 所以 $p_1=2, p_2=5$. 因为

$$12^{\frac{\phi(m)}{p_1}}=12^{20}\equiv 40\not\equiv 1 \pmod{41},$$
$$12^{\frac{\phi(m)}{p_2}}=12^{8}\equiv 18\not\equiv 1 \pmod{41},$$

故由定理2.5知, 12 的确是 41 的原根. □

如前所述, 求 $m = p^\alpha, 2p^\alpha$ 的原根可以归结为求奇素数 p 的原根. 下面介绍一种求 p 的原根的方法.

如前所述, 求 $m = p^\alpha, 2p^\alpha$ 的原根可以归结为求奇素数 p 的原根. 下面介绍一种求 p 的原根的方法.

定理 2.6. 设 p 是奇素数, 如果 $\operatorname{ord}_p a = l < p-1$, 那么 $a, a^2, \ldots, a^l$ 都不是 p 的原根.

如前所述, 求 $m = p^\alpha, 2p^\alpha$ 的原根可以归结为求奇素数 p 的原根. 下面介绍一种求 p 的原根的方法.

定理 2.6. 设 p 是奇素数, 如果 $\mathrm{ord}_p a = l < p - 1$, 那么 $a, a^2, \ldots, a^l$ 都不是 p 的原根.

证明: 对任意 $1 \le s \le l$, 因为

$$\mathrm{ord}_p a^s = \frac{l}{(s, l)} \le l < p - 1 = \phi(p),$$

所以 $a, a^2, \ldots, a^l$ 都不是 p 的原根. 故定理成立. □

基于定理2.6, 我们可以如下求奇素数 p 的原根:

(1) 先列出小于 p 的所有正整数:

$$1, 2, \ldots, p-1. \tag{11}$$

基于定理2.6, 我们可以如下求奇素数 p 的原根:

(1) 先列出小于 p 的所有正整数:

$$1, 2, \ldots, p-1. \tag{11}$$

(2) 取 $a = 2$, 计算 $\mathrm{ord}_p 2$. 如果 $\mathrm{ord}_p 2 = p - 1$, 则 2 就是 p 的原根; 否则在 (11) 中去掉以下各数: $2 \bmod p$, $2^2 \bmod p$, ⋯, $2^{\mathrm{ord}_p 2} \bmod p$.

基于定理2.6, 我们可以如下求奇素数 p 的原根:

(1) 先列出小于 p 的所有正整数:

$$1, 2, \ldots, p-1. \tag{11}$$

(2) 取 $a=2$, 计算 $\mathrm{ord}_p 2$. 如果 $\mathrm{ord}_p 2 = p-1$, 则 2 就是 p 的原根; 否则在 (11) 中去掉以下各数: $2 \bmod p$, $2^2 \bmod p$, $\cdots$, $2^{\mathrm{ord}_p 2} \bmod p$.

(3) 在 (11) 中剩下的数中再取一数, 重复第 (2) 步, 直到 (11) 中仅剩下 $\phi(p-1)$ 个数. 因为对奇素数 p, 它恰有 $\phi(p-1)$ 个原根, 所以这剩下的 $\phi(p-1)$ 个数便是 p 的全部原根.

例 2.2. 求 41 的全部原根.

例 2.2. 求 41 的全部原根.

解: 小于 41 的全部正整数为: 1, 2, $\ldots$, 40. 因为 $\mathrm{ord}_{41}2 = 20 < 41-1$, 所以在这些数中去掉以下各数:
$2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1.$
剩下的数为:

$$3, 6, 7, 11, 12, 13, 14, 15, 17, 19, 22, 24, 26, 27, 28, 29, 30, 34, 35, 38. \tag{12}$$

又因为 $\mathrm{ord}_{41}3 = 8 < 41-1$, 所以在 (12) 中去掉以下各数:
$3, 9, 27, 40, 38, 32, 14, 1$, 其中 $1, 9, 32, 40$ 在此前已经去除.
(12) 中尚剩下 $\phi(40) = 16$ 个数:

$$6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35,$$

因此它们便是 41 的全部原根. $\square$

1. 整数的阶

2. 原根

3. 一般既约剩余系的构造

4. 离散对数

当 m 有原根时, 由定理2.1知 m 的既约剩余系可经其原根的方幂表出.

当 m 有原根时, 由定理2.1知 m 的既约剩余系可经其原根的方幂表出.

而当 m 没有原根, 例如 $m = 2^\alpha$ $(\alpha \geq 3)$, 如何构造它的既约剩余系呢? 这节我们来讨论这个问题.

当 m 有原根时, 由定理2.1知 m 的既约剩余系可经其原根的方幂表出.

而当 m 没有原根, 例如 $m = 2^\alpha$ $(\alpha \geq 3)$, 如何构造它的既约剩余系呢? 这节我们来讨论这个问题.

我们先考虑 $m = 2^\alpha$ $(\alpha \geq 3)$ 的情形. 在定理2.2的证明中, 我们证明了对任意奇数 a, 当 $\alpha \geq 3$ 时,

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

这表明, 关于模 2^α, 任意奇数的阶都不大于 $2^{\alpha-2}$.

当 m 有原根时, 由定理2.1知 m 的既约剩余系可经其原根的方幂表出.

而当 m 没有原根, 例如 $m = 2^\alpha$ $(\alpha \geq 3)$, 如何构造它的既约剩余系呢? 这节我们来讨论这个问题.

我们先考虑 $m = 2^\alpha$ $(\alpha \geq 3)$ 的情形. 在定理2.2的证明中, 我们证明了对任意奇数 a, 当 $\alpha \geq 3$ 时,

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

这表明, 关于模 2^α, 任意奇数的阶都不大于 $2^{\alpha-2}$.
那么有没有阶恰好等于 $2^{\alpha-2}$ 的数呢? 若有的话, 那么我们就可以用它的方幂表出模 2^α 的既约剩余系中的一半元素, 至于另外一半, 如果能够用它们的负数来补足, 那么模 2^α 的既约剩余系的形式与有原根的情形相似, 仍然比较简单.

定理 3.1. 设整数 $\alpha \geq 3$, 则 $\operatorname{ord}_{2^\alpha} 5 = 2^{\alpha-2}$.

定理 3.1. 设整数 $\alpha \geq 3$, 则 $\mathrm{ord}_{2^\alpha} 5 = 2^{\alpha-2}$.

证明: 如果我们能够证明当 $\alpha \geq 3$ 时,

$$5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}, \tag{13}$$

则有 $5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$, 而 $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$, 因此 5 关于模 2^α 的阶为 $2^{\alpha-2}$, 这样就证明了定理.

定理 3.1. 设整数 $\alpha \geq 3$, 则 $\mathrm{ord}_{2^\alpha} 5 = 2^{\alpha-2}$.

证明: 如果我们能够证明当 $\alpha \geq 3$ 时,

$$5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}, \tag{13}$$

则有 $5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$, 而 $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$, 因此 5 关于模 2^α 的阶为 $2^{\alpha-2}$, 这样就证明了定理.

下面归纳证明 (13). 当 $\alpha = 3$ 时, (13) 显然成立. 假定 α 时成立, 于是存在 $k \in \mathbb{Z}$ 使得 $5^{2^{\alpha-2}} = 1 + 2^{\alpha-1} + 2^\alpha k$, 从而有

$$5^{2^{\alpha-2}} = \left(5^{2^{\alpha-3}}\right)^2 = \left(1 + 2^{\alpha-1} + 2^\alpha k\right)^2 \equiv 1 + 2^\alpha \pmod{2^{\alpha+1}}.$$

这就证明了当 $\alpha \geq 3$ 时, (13) 成立, 因此定理得证. □

定理 3.2. 设整数 $\alpha \geq 3$, 令

$$S = \{\pm 5^1, \pm 5^2, \ldots, \pm 5^{2^{\alpha-2}}\},$$

则 S 是模 2^α 的一个既约剩余系.

定理 3.2. 设整数 $\alpha \geq 3$, 令

$$S = \{\pm 5^1, \pm 5^2, \ldots, \pm 5^{2^{\alpha-2}}\},$$

则 S 是模 2^α 的一个既约剩余系.

证明: 因为 $5 \equiv 1 \pmod 4$, 所以对任意非负整数 i, 我们有 $5^i \equiv 1 \pmod 4$, 因此也有 $-5^i \equiv -1 \pmod 4$. 于是对任意非负整数 i, j, 当 $i \neq j$ 时, 我们有 $5^i \not\equiv -5^j \pmod{2^2}$. 这表明, S 中任意两个数关于模 2^α 互不同余. 显然, S 中每个数均与 2^α 互素. 又因为 $|S| = 2^{\alpha-1} = \phi(2^\alpha)$, 故 S 是模 2^α 的一个既约剩余系. $\square$

定理 3.2. 设整数 $\alpha \geq 3$, 令

$$S = \{\pm 5^1, \pm 5^2, \dots, \pm 5^{2^{\alpha-2}}\},$$

则 S 是模 2^α 的一个既约剩余系.

证明: 因为 $5 \equiv 1 \pmod 4$, 所以对任意非负整数 i, 我们有 $5^i \equiv 1 \pmod 4$, 因此也有 $-5^i \equiv -1 \pmod 4$. 于是对任意非负整数 i, j, 当 $i \neq j$ 时, 我们有 $5^i \not\equiv -5^j \pmod{2^2}$. 这表明, S 中任意两个数关于模 2^α 互不同余. 显然, S 中每个数均与 2^α 互素. 又因为 $|S| = 2^{\alpha-1} = \phi(2^\alpha)$, 故 S 是模 2^α 的一个既约剩余系. □

基于上面的定理, 可以使用下面的命题对任意正整数 m 构造既约剩余系.

命题 3.1. 设 $m = m_1 m_2$, $(m_1, m_2) = 1$, m_1 和 m_2 的既约剩余系分别为 $S_1 = \{a_1, a_2, \ldots, a_{\phi(m_1)}\}$ 和 $S_2 = \{b_1, b_2, \ldots, b_{\phi(m_2)}\}$. 若对任意 $a_i \in S_1$ 和 $b_j \in S_2$, 有 $a_i \equiv 1 \pmod{m_2}$ 和 $b_j \equiv 1 \pmod{m_1}$, 则 $S = \{a_i b_j | 1 \leq i \leq \phi(m_1), 1 \leq j \leq \phi(m_2)\}$ 是模 m 的一个既约剩余系.

命题 3.1. 设 $m = m_1 m_2$, $(m_1, m_2) = 1$, m_1 和 m_2 的既约剩余系分别为 $S_1 = \{a_1, a_2, \ldots, a_{\phi(m_1)}\}$ 和 $S_2 = \{b_1, b_2, \ldots, b_{\phi(m_2)}\}$. 若对任意 $a_i \in S_1$ 和 $b_j \in S_2$, 有 $a_i \equiv 1 \pmod{m_2}$ 和 $b_j \equiv 1 \pmod{m_1}$, 则 $S = \{a_i b_j | 1 \le i \le \phi(m_1), 1 \le j \le \phi(m_2)\}$ 是模 m 的一个既约剩余系.

证明: 因为 $(a_i, m_1) = (a_i, m_2) = 1$, 所以 $(a_i, m) = 1$, 同理, $(b_j, m) = 1$, 因此 $(a_i b_j, m) = 1$, 这说明 S 中的每个数均与 m 互素. 假设 $a_i b_j \equiv a_{i'} b_{j'} \pmod{m}$, 则有 $a_i b_j \equiv a_{i'} b_{j'} \pmod{m_1}$. 由于 $b_j \equiv b_{j'} \equiv 1 \pmod{m_1}$, 所以 $a_i \equiv a_{i'} \pmod{m_1}$, 因此 $a_i = a_{i'}$. 同理, $b_j = b_{j'}$. 这就是说 S 中任意两个数关于模 m 两两互不同余. 又因为 $|S| = \phi(m_1)\phi(m_2) = \phi(m)$, 所以 S 是模 m 的既约剩余系. $\square$

命题3.1给出了由 m 彼此互素的因数的既约剩余系构造模 m 的既约剩余系的方法, 这事实上提供了对任意正整数 m 构造模 m 的既约剩余系的途径, 惟一有待解释的是如何满足条件: 对任意 $a_i \in S_1$ 和 $b_j \in S_2$, 有 $a_i \equiv 1 \pmod{m_2}$ 和 $b_j \equiv 1 \pmod{m_1}$.

命题3.1给出了由 m 彼此互素的因数的既约剩余系构造模 m 的既约剩余系的方法, 这事实上提供了对任意正整数 m 构造模 m 的既约剩余系的途径, 惟一有待解释的是如何满足条件: 对任意 $a_i \in S_1$ 和 $b_j \in S_2$, 有 $a_i \equiv 1 \pmod{m_2}$ 和 $b_j \equiv 1 \pmod{m_1}$.

我们考虑如何满足条件 $a_i \equiv 1 \pmod{m_2}$; $b_j \equiv 1 \pmod{m_1}$ 的情形类似.

命题3.1给出了由 m 彼此互素的因数的既约剩余系构造模 m 的既约剩余系的方法, 这事实上提供了对任意正整数 m 构造模 m 的既约剩余系的途径, 惟一有待解释的是如何满足条件: 对任意 $a_i \in S_1$ 和 $b_j \in S_2$, 有 $a_i \equiv 1 \pmod{m_2}$ 和 $b_j \equiv 1 \pmod{m_1}$.

我们考虑如何满足条件 $a_i \equiv 1 \pmod{m_2}$; $b_j \equiv 1 \pmod{m_1}$ 的情形类似.

事实上, 只要适当挑选 m_1 的既约剩余系, $a_i \equiv 1 \pmod{m_2}$ 都是可以满足的, 这是因为如果 $\{x_1, x_2, \ldots, x_{\phi(m_1)}\}$ 是模 m_1 的既约剩余系, 那么同余方程 $m_1 y \equiv 1 - x_i \pmod{m_2}$ 有惟一解 $y \equiv y_i \pmod{m_2}$. 令 $a_i = m_1 y_i + x_i$, 则有 $a_i \equiv 1 \pmod{m_2}$, 并且 $a_i \equiv x_i \pmod{m_1}$, 所以 $\{a_1, a_2, \ldots, a_{\phi(m_1)}\}$ 是模 m_1 的既约剩余系.

下面通过一个例子阐明上述方法.

例 3.1. 使用命题 3.1 求模 $m=40$ 的既约剩余系.

下面通过一个例子阐明上述方法.

例 3.1. 使用命题 3.1 求模 $m = 40$ 的既约剩余系.

解: 因为 $m = 40 = 5 \cdot 2^3$, 我们分别选取 5 和 2^3 的既约剩余系 $\{1, 9, 17, 33\}$ 和 $\{1, 11, 21, 31\}$. 显然, 这样的既约剩余系满足命题3.1的条件, 于是模 40 的既约剩余系中的元素为:

$$1 \cdot 1, 1 \cdot 11, 1 \cdot 21, 1 \cdot 31, 9 \cdot 1, 9 \cdot 11, 9 \cdot 21, 9 \cdot 31,$$
$$17 \cdot 1, 17 \cdot 11, 17 \cdot 21, 17 \cdot 31, 33 \cdot 1, 33 \cdot 11, 33 \cdot 21, 33 \cdot 31,$$

即 $\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$ 是模 40 的既约剩余系. □

在 5.2 节我们看到, 若 m 有原根 g, 则 $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ 构成 m 的一个既约剩余系.

在 5.2 节我们看到, 若 m 有原根 g, 则 $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ 构成 m 的一个既约剩余系.

因此, 对任意整数 a, 如果 $(a, m) = 1$, 那么必存在 $0 \le k < \phi(m)$ 使得 $a \equiv g^k \pmod{m}$, 并且这样的 k 是惟一的.

在 5.2 节我们看到, 若 m 有原根 g, 则 $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ 构成 m 的一个既约剩余系.

因此, 对任意整数 a, 如果 $(a, m) = 1$, 那么必存在 $0 \leq k < \phi(m)$ 使得 $a \equiv g^k \pmod{m}$, 并且这样的 k 是惟一的.

为了描述原根的上述重要性质, 我们给出下面的定义.

定义 4.1. 设正整数 m 有原根 g, 则对任意满足 $(a,m)=1$ 的整数 a, 必存在惟一的整数 x, $0 \le x < \phi(m)$, 使得

$$g^x \equiv a \pmod{m},$$

称 x 为模 m 以 g 为底 a 的**离散对数**, 记作 $x=\log_g a$. 有时, 也称离散对数为**指标**.

定义 4.1. 设正整数 m 有原根 g, 则对任意满足 $(a, m) = 1$ 的整数 a, 必存在惟一的整数 x, $0 \le x < \phi(m)$, 使得

$$g^x \equiv a \pmod{m},$$

称 x 为模 m 以 g 为底 a 的**离散对数**, 记作 $x = \log_g a$. 有时, 也称离散对数为**指标**.

注 4.1.

(1) 由定义, 有 $g^{\log_g a} \equiv a \pmod{m}$.

定义 4.1. 设正整数 m 有原根 g, 则对任意满足 $(a,m)=1$ 的整数 a, 必存在惟一的整数 x, $0 \le x < \phi(m)$, 使得

$$g^x \equiv a \pmod{m},$$

称 x 为模 m 以 g 为底 a 的**离散对数**, 记作 $x = \log_g a$. 有时, 也称离散对数为**指标**.

注 4.1.

(1) 由定义, 有 $g^{\log_g a} \equiv a \pmod{m}$.

(2) 若 $(a,m)=(b,m)=1$, 则 $a \equiv b \pmod{m}$ 当且仅当 $\log_g a = \log_g b$.

下面例子给出模 7 分别以 3 和 5 为底 $1, 2, \ldots, 6$ 的离散对数.

下面例子给出模 7 分别以 3 和 5 为底 $1, 2, \ldots, 6$ 的离散对数.

例 4.1. 当 $m = 7$ 时, m 有原根 3. 因为

$$3^0 \equiv 1 \pmod 7, \quad 3^1 \equiv 3 \pmod 7, \quad 3^2 \equiv 2 \pmod 7,$$
$$3^3 \equiv 6 \pmod 7, \quad 3^4 \equiv 4 \pmod 7, \quad 3^5 \equiv 5 \pmod 7,$$

所以

$$\log_3 1 = 0, \quad \log_3 2 = 2, \quad \log_3 3 = 1,$$
$$\log_3 4 = 4, \quad \log_3 5 = 5, \quad \log_3 6 = 3.$$

下面例子给出模 7 分别以 3 和 5 为底 $1, 2, \ldots, 6$ 的离散对数.

例 4.1. 当 $m = 7$ 时, m 有原根 3. 因为

$$3^0 \equiv 1 \pmod 7, \quad 3^1 \equiv 3 \pmod 7, \quad 3^2 \equiv 2 \pmod 7,$$
$$3^3 \equiv 6 \pmod 7, \quad 3^4 \equiv 4 \pmod 7, \quad 3^5 \equiv 5 \pmod 7,$$

所以

$$\log_3 1 = 0, \quad \log_3 2 = 2, \quad \log_3 3 = 1,$$
$$\log_3 4 = 4, \quad \log_3 5 = 5, \quad \log_3 6 = 3.$$

另外, 5 也是 7 的原根, 类似计算得

$$\log_5 1 = 0, \quad \log_5 2 = 4, \quad \log_5 3 = 5,$$
$$\log_5 4 = 2, \quad \log_5 5 = 1, \quad \log_5 6 = 3.$$

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

(3) $\log_g 1 = 0$, $\log_g g = 1$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

(3) $\log_g 1 = 0$, $\log_g g = 1$.

(4) 如果 $m > 2$, 则 $\log_g(-1) = \phi(m)/2$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

(3) $\log_g 1 = 0$, $\log_g g = 1$.

(4) 如果 $m > 2$, 则 $\log_g(-1) = \phi(m)/2$.

(5) 如果 h 也是 m 的原根, 则 $\log_g a \equiv \log_h a \cdot \log_g h \pmod{\phi(m)}$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

(3) $\log_g 1 = 0$, $\log_g g = 1$.

(4) 如果 $m > 2$, 则 $\log_g(-1) = \phi(m)/2$.

(5) 如果 h 也是 m 的原根, 则 $\log_g a \equiv \log_h a \cdot \log_g h \pmod{\phi(m)}$.

离散对数具有如下类似于对数的性质.

定理 4.1. 设 g 是 m 的原根, $(a,m)=(b,m)=1$, 则有:

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$, 这里 $n \in \mathbb{Z}^+$.

(3) $\log_g 1 = 0$, $\log_g g = 1$.

(4) 如果 $m > 2$, 则 $\log_g(-1) = \phi(m)/2$.

(5) 如果 h 也是 m 的原根, 则 $\log_g a \equiv \log_h a \cdot \log_g h \pmod{\phi(m)}$.

证明: (1) 由 $g^{\log_g a} \equiv a \pmod{m}$, $g^{\log_g b} \equiv b \pmod{m}$, $g^{\log_g(ab)} \equiv ab \pmod{m}$ 得
$g^{\log_g(ab)} \equiv ab \equiv g^{\log_g a} \cdot g^{\log_g b} = g^{\log_g a + \log_g b} \pmod{m}$, 因此由定理1.2知 $\log_g(ab) \equiv \log_g a + \log_g b \pmod{\phi(m)}$.

(2) 由

$$g^{\log_g a^n} \equiv a^n \pmod{m}, \quad g^{\log_g a} \equiv a \pmod{m}$$

得

$$g^{\log_g a^n} \equiv a^n \equiv \left(g^{\log_g a}\right)^n = g^{n\log_g a} \pmod{m},$$

所以由定理1.2知 $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$.

(2) 由

$$g^{\log_g a^n} \equiv a^n \pmod m, \quad g^{\log_g a} \equiv a \pmod m$$

得

$$g^{\log_g a^n} \equiv a^n \equiv \left(g^{\log_g a}\right)^n = g^{n\log_g a} \pmod m,$$

所以由定理1.2知 $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$.

(3) 由定义, 显然成立.

(2) 由

$$g^{\log_g a^n} \equiv a^n \pmod{m}, \quad g^{\log_g a} \equiv a \pmod{m}$$

得

$$g^{\log_g a^n} \equiv a^n \equiv \left(g^{\log_g a}\right)^n = g^{n\log_g a} \pmod{m},$$

所以由定理1.2知 $\log_g a^n \equiv n\log_g a \pmod{\phi(m)}$.

(3) 由定义, 显然成立.

(4) 当 $m > 2$ 时, m 只可能是 $4, p^\alpha, 2p^\alpha$(其中 p 是奇素数, α 是正整数), 此时均有 $\phi(m) \equiv 0 \pmod{2}$. 当 $m = 4$ 时, 结论显然. 当 $m = p^\alpha$ 时, 因为 $(g, m) = 1$, 所以由欧拉定理有 $g^{\phi(m)} \equiv 1 \pmod{p^\alpha}$, 于是有

$$\left(g^{\frac{\phi(m)}{2}} - 1\right)\left(g^{\frac{\phi(m)}{2}} + 1\right) \equiv 0 \pmod{p^\alpha}.$$

因为 $\left(g^{\frac{\phi(m)}{2}}-1, g^{\frac{\phi(m)}{2}}+1\right) \leq 2$, 所以 $p^\alpha | g^{\frac{\phi(m)}{2}}-1$ 或 $p^\alpha | g^{\frac{\phi(m)}{2}}+1$. 又因为 g 是 p^α 的原根, 所以 $\mathrm{ord}_{p^\alpha} g = \phi(m)$, 因此 $g^{\frac{\phi(m)}{2}} \not\equiv 1 \pmod{p^\alpha}$, 故 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{p^\alpha}$.

因为 $\left(g^{\frac{\phi(m)}{2}}-1, g^{\frac{\phi(m)}{2}}+1\right) \leq 2$, 所以 $p^{\alpha} | g^{\frac{\phi(m)}{2}}-1$ 或 $p^{\alpha} | g^{\frac{\phi(m)}{2}}+1$. 又因为 g 是 p^{α} 的原根, 所以 $\mathrm{ord}_{p^{\alpha}} g=\phi(m)$, 因此 $g^{\frac{\phi(m)}{2}} \not\equiv 1 \pmod{p^{\alpha}}$, 故 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{p^{\alpha}}$.

当 $m=2p^{\alpha}$ 时, 此时 g 必为奇数. 因为 $(g, m)=1$, 所以由欧拉定理有 $g^{\phi(m)} \equiv 1 \pmod{2p^{\alpha}}$, 于是有 $\left(g^{\frac{\phi(m)}{2}}-1\right)\left(g^{\frac{\phi(m)}{2}}+1\right) \equiv 0 \pmod{2p^{\alpha}}$, 因此 $\left(g^{\frac{\phi(m)}{2}}-1\right)\left(g^{\frac{\phi(m)}{2}}+1\right) \equiv 0 \pmod{p^{\alpha}}$. 因为 $\left(g^{\frac{\phi(m)}{2}}-1, g^{\frac{\phi(m)}{2}}+1\right) \leq 2$, 所以 $p^{\alpha} | g^{\frac{\phi(m)}{2}}-1$ 或 $p^{\alpha} | g^{\frac{\phi(m)}{2}}+1$.

因为 $\left(g^{\frac{\phi(m)}{2}}-1, g^{\frac{\phi(m)}{2}}+1\right) \leq 2$, 所以 $p^\alpha | g^{\frac{\phi(m)}{2}}-1$ 或 $p^\alpha | g^{\frac{\phi(m)}{2}}+1$. 又因为 g 是 p^α 的原根, 所以 $\mathrm{ord}_{p^\alpha} g = \phi(m)$, 因此 $g^{\frac{\phi(m)}{2}} \not\equiv 1 \pmod{p^\alpha}$, 故 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{p^\alpha}$.

当 $m = 2p^\alpha$ 时, 此时 g 必为奇数. 因为 $(g, m) = 1$, 所以由欧拉定理有 $g^{\phi(m)} \equiv 1 \pmod{2p^\alpha}$, 于是有 $\left(g^{\frac{\phi(m)}{2}}-1\right)\left(g^{\frac{\phi(m)}{2}}+1\right) \equiv 0 \pmod{2p^\alpha}$, 因此 $\left(g^{\frac{\phi(m)}{2}}-1\right)\left(g^{\frac{\phi(m)}{2}}+1\right) \equiv 0 \pmod{p^\alpha}$. 因为 $\left(g^{\frac{\phi(m)}{2}}-1, g^{\frac{\phi(m)}{2}}+1\right) \leq 2$, 所以 $p^\alpha | g^{\frac{\phi(m)}{2}}-1$ 或 $p^\alpha | g^{\frac{\phi(m)}{2}}+1$.

又因为 g 是 $2p^\alpha$ 的原根, 所以 $\mathrm{ord}_{2p^\alpha} g = \phi(m)$, 因此 $g^{\frac{\phi(m)}{2}} \not\equiv 1 \pmod{p^\alpha}$; 否则由 g 是奇数知, $g^{\frac{\phi(m)}{2}} \equiv 1 \pmod{2p^\alpha}$, 矛盾! 故 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{p^\alpha}$. 再次由 g 是奇数, 可得 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{2}$. 于是 $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod{2p^\alpha}$. 这就证明了 (4).

(5) 由定理2.4知, 存在整数 k 满足 $1 \le k \le \phi(m)$ 和 $(k, \phi(m)) = 1$, 且使得 $h \equiv g^k \pmod{m}$. 于是有

$$g^{\log_g a} \equiv a \equiv h^{\log_h a} \equiv g^{k \log_h a} \pmod{m},$$

所以由定理1.2知 $\log_g a \equiv k \log_h a = \log_g h \cdot \log_h a \pmod{\phi(m)}$, 故 (5) 成立. $\square$

可以利用原根造出离散对数表来解同余方程.

例 4.2. 解同余方程 $6x^{12} \equiv 11 \pmod{17}$.

可以利用原根造出离散对数表来解同余方程.

例 4.2. 解同余方程 $6x^{12} \equiv 11 \pmod{17}$.

解: 通过计算 (可使用例2.2的方法), 3 是 17 的一个原根.

可以利用原根造出离散对数表来解同余方程.

例 4.2. 解同余方程 $6x^{12} \equiv 11 \pmod{17}$.

解: 通过计算 (可使用例2.2的方法), 3 是 17 的一个原根.

进一步, 计算

$$3^0 \equiv 1 \pmod{17},\ 3^1 \equiv 3 \pmod{17},\ \ldots,\ 3^{15} \equiv 6 \pmod{17}$$

得离散对数表如下:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\log_3 a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

显然, 由定理1.2知,

$$6x^{12} \equiv 11 \pmod{17} \tag{14}$$

与 $\log_3(6x^{12}) \equiv \log_3 11 \pmod{16}$ 等价, 后者即为

$$\log_3 6 + 12\log_3 x \equiv \log_3 11 \pmod{16}. \tag{15}$$

显然, 由定理1.2知,

$$6x^{12} \equiv 11 \pmod{17} \tag{14}$$

与 $\log_3(6x^{12}) \equiv \log_3 11 \pmod{16}$ 等价, 后者即为

$$\log_3 6 + 12\log_3 x \equiv \log_3 11 \pmod{16}. \tag{15}$$

查上面的离散对数表知, (15) 即为

$$12\log_3 x \equiv 8 \pmod{16}. \tag{16}$$

显然, 由定理1.2知,

$$6x^{12} \equiv 11 \pmod{17} \tag{14}$$

与 $\log_3(6x^{12}) \equiv \log_3 11 \pmod{16}$ 等价, 后者即为

$$\log_3 6 + 12\log_3 x \equiv \log_3 11 \pmod{16}. \tag{15}$$

查上面的离散对数表知, (15) 即为

$$12\log_3 x \equiv 8 \pmod{16}. \tag{16}$$

因此, 求解 (14) 等价于求解 (16). 而 (16) 是关于 $\log_3 x$ 的一次同余方程, 解之得 $\log_3 x \equiv 2, 6, 10, 14 \pmod{16}$. 再次使用上面的离散对数表, 反查即得 $x \equiv 9, 15, 8, 2 \pmod{17}$, 这些即为原同余方程的全部解. □

例 4.3. 解同余方程 $7^x \equiv 6 \pmod{17}$.

例 4.3. 解同余方程 $7^x \equiv 6 \pmod{17}$.

解: 因为 3 是 17 的一个原根, 所以同余方程 $7^x \equiv 6 \pmod{17}$ 等价于

$$\log_3(7^x) \equiv \log_3 6 \pmod{16},$$

后者即为

$$x\log_3 7 \equiv \log_3 6 \pmod{16}.$$

查例4.2中离散对数表知, 上面同余方程即为 $11x \equiv 15 \pmod{16}$, 解之得 $x \equiv 13 \pmod{16}$. 故原同余方程的解为 $x \equiv 13 \pmod{16}$. □

一般地, 我们有下面的定理.

定理 4.2. 设 m 有原根 g, $(b,m)=1$, $n\in\mathbb{Z}^+$, 那么同余方程

$$x^n \equiv b \pmod{m} \tag{17}$$

有解的充要条件是 $d=(n,\phi(m))|\log_g b$. 若 (17) 有解, 则恰有 d 个解.

一般地, 我们有下面的定理.

定理 4.2. 设 m 有原根 g, $(b,m)=1$, $n\in\mathbb{Z}^+$, 那么同余方程

$$x^n \equiv b \pmod{m} \tag{17}$$

有解的充要条件是 $d=(n,\phi(m))|\log_g b$. 若 (17) 有解, 则恰有 d 个解.

证明: 先证必要性. 假设 (17) 有解 x_0, 即 $x_0^n \equiv b \pmod{m}$, 于是有

$$n\log_g x_0 \equiv \log_g b \pmod{\phi(m)}.$$

因此关于 y 的一次同余方程 $ny \equiv \log_g b \pmod{\phi(m)}$ 有解 $y \equiv \log_g x_0 \pmod{\phi(m)}$, 从而由一次同余方程有解的条件知 $d=(n,\phi(m))|\log_g b$.

下证充分性. 假设 $d = (n, \phi(m)) | \log_g b$, 那么关于 y 的一次同余方程

$$ny \equiv \log_g b \pmod{\phi(m)}$$

有 d 个解, 设为 $y_1, y_2, \ldots, y_d$. 令 $x_i = g^{y_i} \bmod m$, $1 \le i \le d$.

下证充分性. 假设 $d=(n,\phi(m))|\log_g b$, 那么关于 y 的一次同余方程

$$ny \equiv \log_g b \pmod{\phi(m)}$$

有 d 个解, 设为 $y_1, y_2, \ldots, y_d$. 令 $x_i = g^{y_i} \bmod m$, $1 \le i \le d$.

当 $i \ne j$ 时, $x_i \not\equiv x_j \pmod{m}$; 否则有 $g^{y_i} \equiv g^{y_j} \pmod{m}$, 从而 $y_i \equiv y_j \pmod{\phi(m)}$, 矛盾! 计算知

$$x_i^n \equiv (g^{y_i})^n \equiv g^{ny_i} \equiv g^{\log_g b} \equiv b \pmod{m},$$

所以由此我们可以得到 (17) 的 d 个关于模 m 互不同余的解. 易证, (17) 没有更多的解, 因此 (17) 恰有 d 个解. □

定理 4.3. 设 m 有原根 g, $(a,m)=(b,m)=1$, 则同余方程 $a^x \equiv b \pmod{m}$ 有解的充要条件是 $d=(\log_g a, \phi(m)) | \log_g b$. 若该方程有解, 则恰有 d 个解.

证明: 与定理4.2的证明类似, 在此省略. □