第五章 原根与指标
2015年05月14日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

5.2 原根

问题:

1. 模p 原根存在吗?
2. 如何生成模p 原根g 吗?
3. 模p^α 原根存在吗?
4. 如何生成模p^α 原根g 吗?
5. 模$2\,p^\alpha$ 原根存在吗?
6. 模m 原根存在吗?
7. 如何构造模p 原根g 的指数表?

5.2.1 模p 原根

先给出模p 原根的存在性证明及原根个数:

定理5.2.1 设p 是奇素数, 则模p 的原根存在, 且有$\varphi(p-1)$ 个原根, 其中φ 为欧拉函数.

证一 (构造性) 在模p 的简化剩余系$1,\ \ldots,\ p-1$ 中, 记

$$e_r = \mathrm{ord}_p(r), \quad 1 \leq r \leq p-1, \quad e = [e_1, \ldots, e_{p-1}].$$

那么根据§5.1 定理5.1.8 , 存在整数g, 使得 $g^e \equiv 1 \pmod{p}$.

因此, $e \mid \varphi(p) = p-1$. 又因为 $e_r \mid e, \quad r = 1, \ldots, p-1,$

从而推出同余式 $x^e \equiv 1 \pmod{p}$

有$p-1$ 个解 $x \equiv 1,\ \ldots,\ p-1 \pmod{p}$.

根据§3.4 定理3.4.4 , 我们有$p-1 \leq e$. 故g 的指数为$p-1$, 即g 是模p 的原根.

最后, 根据定理5.1.4 之推论1, 当g 为原根时, $g^d,\ \ (d, p-1) = 1$ 也是原根, 共有$\varphi(p-1)$ 个.

证二 (存在性) 设$d \mid p-1$. 我们用$F(d)$ 表示模p 的简化剩余系中指数为d 的元素个数. 根据§5.1定理5.1.1 的推论, 模p 简化剩余系中每个元素的指数是$p-1$ 的因数, 所以我们有

$$\sum_{d|p-1} F(d) = p-1. \tag{1}$$

因为模p指数为d 的元素满足同余式:

$$x^d - 1 \equiv 0 \pmod{p}, \tag{2}$$

根据§3.4 定理3.4.5 的推论, 同余式(2)有d 个模p 不同的解.
现在, 若a 是模p 指数为d 的元素, 则同余式(2)的解可以表示成

$$x \equiv a^0,\ a,\ \ldots,\ a^{d-1}.$$

根据§5.1 定理5.1.4 , 这些数中有$\varphi(d)$ 个指数为d 的元素. 因此, $F(d) = \varphi(d)$. 而若没有模p 指数为d 的元素, 则$F(d) = 0$.
总之, 我们有 $F(d) \le \varphi(d)$.

但由§2.3 定理2.3.9 , 我们又有

$$\sum_{d|p-1} \varphi(d) = p - 1. \tag{3}$$

这样, 由(1)和(3)推出

$$\sum_{d|p-1} (\varphi(d) - F(d)) = 0. \tag{4}$$

因此, 对所有正整数$d \mid p-1$, 我们有

$$F(d) = \varphi(d). \tag{5}$$

特别, 我们有 $F(p-1) = \varphi(p-1)$.
这说明存在模p 指数为$p-1$的元素, 即模p 的原根存在. 证毕

推论 设p 是奇素数, $d \mid p-1$. 则模p 指数为d 的元素存在.
证 从定理5.2.1 证明的关系式(5), 即可推出结论. 证毕

再给出原根的构造方法:

定理5.2.2 设p 为奇素数, $p-1$ 的所有不同素因数是$q_1, \ldots, q_s$, 则g 是模p 原根的充要条件是

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{m}, \qquad i = 1, \ldots, s. \tag{6}$$

证 设g 是p 的一个原根, 则g 对模p 的指数是$p-1$. 但

$$0 < \frac{p-1}{q_i} < p-1, \qquad i = 1, \ldots, s.$$

根据§5.1 定理5.1.2 , 有(6), 即 $g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}, \qquad i = 1, \ldots, s.$

反过来, 若g 满足(6), 但对模p 的指数$e = \mathrm{ord}_p(g) < p-1$. 则根据§5.1定理5.1.1 , 有$e \mid p-1$. 因而存在一个素数$q$ 使得$q \mid \frac{p-1}{e}$. 即

$$\frac{p-1}{e} = u \cdot q, \quad \text{或} \quad \frac{p-1}{q} = u \cdot e.$$

进而 $g^{\frac{p-1}{q}} = (g^e)^u \equiv 1 \pmod{p}$.

与假设(6)矛盾. 证毕

例5.2.1 求模$p=41$的所有原根.

解 因为$p-1=40=2^3\cdot 5$,其素因数为$q_1=2,\ q_2=5$. 进而, $\dfrac{p-1}{q_1}=20$, $\dfrac{p-1}{q_2}=8$. 根据定理5.2.2, 只需验证(6), 即$g^{20},\ g^8$模m是否同余于1. 对$g=2,\ 3,\ 5,\ 6,\ldots$, 逐个验算:

$$\begin{aligned}
&2^2\equiv 4, \quad 2^4\equiv 16, \quad 2^8\equiv 10, \quad 2^{16}\equiv 18, \quad 2^{20}\equiv 1,\\
&3^2\equiv 9, \quad 3^4\equiv -1, \quad 3^8\equiv 1, \quad 3^{16}\equiv 1, \quad 3^{20}\equiv -1,\\
&5^2\equiv 25, \quad 5^4\equiv 10, \quad 5^8\equiv 18, \quad 5^{16}\equiv 37, \quad 5^{20}\equiv 1,\\
&6^2\equiv 36, \quad 6^4\equiv 25, \quad 6^8\equiv 10, \quad 6^{16}\equiv 18, \quad 6^{20}\equiv -1, \pmod{41},
\end{aligned}$$

故$g=6$是模$p=41$的原根.

进一步,当$(d,p-1)=1$时, d遍历模$p-1=40$的简化剩余系:

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

共$\varphi(p-1)=16$个数时, g^d遍历模41的所有原根:

$$\begin{aligned}
&g^1\equiv 6, \quad g^3\equiv 11, \quad g^7\equiv 29, \quad g^9\equiv 19, \quad g^{11}\equiv 28, \quad g^{13}\equiv 24,\\
&g^{17}\equiv 26, \quad g^{19}\equiv 34, \quad g^{21}\equiv 35, \quad g^{23}\equiv 30, \quad g^{27}\equiv 12, \quad g^{29}\equiv 22,\\
&g^{31}\equiv 13, \quad g^{33}\equiv 17, \quad g^{37}\equiv 15, \quad g^{39}\equiv 7 \pmod{41}.
\end{aligned}$$

例5.2.2 求模$p = 43$的原根.

解 因为$p - 1 = 42 = 2 \cdot 3 \cdot 7$, $q_1 = 2$, $q_2 = 3$, $q_3 = 7$, 因此, $\dfrac{p-1}{q_1} = 21$, $\dfrac{p-1}{q_2} = 14$, $\dfrac{p-1}{q_3} = 6$. 只需验证(6), 即g^{21}, g^{14}, g^6 模m 是否同余于1. 对$g = 2, 3, 5, \ldots$逐个验算:

$$
\begin{aligned}
&2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^6 \equiv 64 \equiv 21, \quad 2^7 \equiv 21 \cdot 2 \equiv -1,\\
&2^{14} \equiv 1, \quad 3^2 \equiv 9, \quad 3^4 \equiv 81 \equiv -5, \quad 3^6 \equiv 9 \cdot (-5) \equiv -2,\\
&3^7 \equiv -6, \quad 3^{14} \equiv (-6)^2 \equiv 36, \quad 3^{21} \equiv (-6) \cdot 36 \equiv -1 \pmod{43}.
\end{aligned}
$$

因此, $g = 3$ 是模$p = 43$ 的原根.

进一步,当$(d, p-1) = 1$时, d 遍历模$p - 1 = 42$ 的简化剩余系:

$$1,\ 5,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 37,\ 41$$

共$\varphi(p-1) = 12$个数时, g^d 遍历模43 的所有原根:

$$
\begin{aligned}
&g^1 \equiv 3, \quad g^5 \equiv 28, \quad g^{11} \equiv 30, \quad g^{13} \equiv 12, \quad g^{17} \equiv 26, \quad g^{19} \equiv 19, \quad g^{23} \equiv 34,\\
&g^{25} \equiv 5, \quad g^{29} \equiv 18, \quad g^{31} \equiv 33, \quad g^{37} \equiv 20, \quad g^{41} \equiv 29 \pmod{43}.
\end{aligned}
$$

例5.2.3 求模$p = 191$ 的原根.

解 因为$p - 1 = 190 = 2 \cdot 5 \cdot 19, \quad q_1 = 2,\ q_2 = 5,\ q_3 = 19$, 因此, $\dfrac{p-1}{q_1} = 95,\ \dfrac{p-1}{q_2} = 38,\ \dfrac{p-1}{q_3} = 10.$ 只需验证(6), 即$g^{\frac{p-1}{q_1}},\ g^{\frac{p-1}{q_2}},\ g^{\frac{p-1}{q_3}}$ 模m 是否同余于1. 对$g = 2,\ 3,\ 5,\ \ldots$ 逐个验算:

g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$	g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$	g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$
2	1	49	69	10	1	49	180	15	1	39	153
3	1	39	30	11	190	1	107	17	1	109	32
5	1	1	177	12	1	49	153	18	1	39	25
6	1	1	160	13	1	184	121	19	190	39	52
7	190	39	1	14	190	1	69				

因此, $g = 19$ 是模$p = 191$ 的原根.

5.2.2 模p^α 原根

本节讨论模p^α 原根的存在性. 先给出如下的引理:

引理5.2.1 设p 是一个奇素数. 如果整数g 是模p 原根, 则有

$$g^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{或} \quad (g+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

证 因为

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} \cdot g^{p-2} \cdot p + \binom{p-1}{2} \cdot g^{p-3} \cdot p^2 + \cdots + p^{p-1} \\ &= g^{p-1} + (p-1) \cdot g^{p-2} \cdot p + A \cdot p^2,\end{aligned}$$

其中A 为整数, 所以有

$$(g+p)^{p-1} - 1 \equiv (g^{p-1} - 1) + (p-1) \cdot g^{p-2} \cdot p \pmod{p^2}$$

因此, 结论成立. 证毕

引理5.2.2 设p 是一个奇素数. 如果整数g 满足

$$g^{p-1} = 1 + u_0 \cdot p, \quad (u_0, p) = 1 \tag{7}$$

则对任意整数$k \geq 2$, 存在整数u_{k-2} 使得

$$g^{p^{k-2}(p-1)} = 1 + u_{k-2} \cdot p^{k-1}, \quad (u_{k-2}, p) = 1. \tag{8}$$

证 我们对$k \geq 2$ 作数学归纳法, 来证明关系式(8), 即

$$g^{p^{k-2}(p-1)} = 1 + u_{k-2} \cdot p^{k-1}, \quad (u_{k-2}, p) = 1.$$

$k = 2$时, 关系式(8)就是关系式((7)), 命题成立.

假设$k-1$时, 命题成立, 即存在整数u_{k-3}使得

$$g^{p^{k-3}(p-1)} = 1 + u_{k-3} \cdot p^{k-2}, \quad (u_{k-3}, p) = 1.$$

两端作p次方, 我们有

$$\begin{aligned} g^{p^{k-2}(p-1)} &= (1 + u_{k-3} \cdot p^{k-2})^p \\ &= 1 + \binom{p}{1}(u_{k-3} \cdot p^{k-2}) + \binom{p}{2}(u_{k-3} \cdot p^{k-2})^2 + \cdots + (u_{k-3} \cdot p^{k-2})^p \\ &= 1 + (u_{k-3} + A_{k-3} \cdot p) \cdot p^{k-1} \end{aligned} \tag{9}$$

其中A_{k-3}为整数. 取$u_{k-2} = u_{k-3} + A_{k-3} \cdot p$, 有$(u_{k-2}, p) = (u_{k-3}, p) = 1$. 命题成立.

根据数学归纳法原理, 关系式(8)对所有整数$k \geq 2$成立. 证毕

引理5.2.3 设p 是一个奇素数. 设$k \geq 2$. 如果模p 原根g 满足

$$g^{p^{k-2}(p-1)} = 1 + u_{k-2} \cdot p^{k-1}, \quad (u_{k-2}, p) = 1. \tag{10}$$

则g 也是模p^k 原根.

证 令$e_k = \mathrm{ord}_{p^k}(g)$. 则我们有 $g^{e_k} \equiv 1 \pmod{p^k}$.

进而, $g^{e_k} \equiv 1 \pmod{p}$. 因为$g$ 是模p 原根, 所以$p-1 \mid e_k$. 故e_k 具有形式$e_k = p^t(p-1)$. 下面确定$t = k-1$.

一方面, 根据引理5.2.2 之证明(9), 由假设条件(10), 可得到

$$g^{p^{k-1}(p-1)} = 1 + (u_{k-2} + A_{k-2} \cdot p) \cdot p^k$$

其中A_{k-2} 为整数, 从而$e_k \mid p^{k-1}(p-1), \ t \leq k-1$.

另一方面, 仍由假设条件(10), 知 $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$,

得到$e_k \not\mid p^{k-2}(p-1), \ t > k-2$.

故$t = k-1$, $e_k = p^{k-1}(p-1) = \varphi(p^k)$. g 也是模p^k 原根. 证毕

其次, 构造模p^2 的原根.

定理5.2.3 设g 是模p的一个原根, 则g 或者$g+p$ 是模p^2 原根.

证 根据引理5.2.1 , 有(7)

$$g^{p-1} = 1 + u_0 \cdot p, \quad (u_0, p) = 1$$

或

$$(g+p)^{p-1} = 1 + u_0 \cdot p, \quad (u_0, p) = 1$$

再由引理5.2.3 , 前者推出g 是模p^2 原根, 而后者推出$g+p$ 是模p^2 原根. 证毕

再次, 构造模p^α 的原根.

定理5.2.4 设p 是一个奇素数, 则对任意正整数α, 模p^α 的原根存在. 更确切地说, 如果g 是模p^2的一个原根, 则对任意正整数α, g 是模p^α 的原根.

证 根据定理5.2.1 , 知模p 原根存在, 再由定理5.2.3 及其证明知道模p^2 的原根g 也存在, 且满足(7), 即

$$g^{p-1} = 1 + u_0 \cdot p.$$

根据引理5.2.2 , 对任意整数$\alpha \geq 2$, 存在整数$u_{\alpha-2}$ 使得(8) 成立, 即

$$g^{p^{\alpha-2}(p-1)} = 1 + u_{\alpha-2} \cdot p^{\alpha-1}, \quad (u_{\alpha-2}, p) = 1.$$

因此, 根据引理5.2.3 , g 是模p^α 原根. 证毕

定理5.2.5 设$\alpha \geq 1$, g 是模p^α 的一个原根, 则g 与$g + p^\alpha$ 中的奇数是模$2\,p^\alpha$ 的一个原根.

证 (i) 设奇数a 满足同余式 $a^d \equiv 1 \pmod{p^\alpha}$,

又显然有 $a^d \equiv 1 \pmod 2$,

根据§2.1 定理2.1.12 ,

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

反之显然.

(ii) 若g 是奇数, 令$d = \varphi(p^\alpha)$, 则 $\varphi(2p^\alpha) = \varphi(p^\alpha) = d$.

又当 $g^d \equiv 1 \pmod{p^\alpha}$, $g^r \not\equiv 1 \pmod{p^\alpha}$, $0 < r < d$ 时, 有

$$g^d \equiv 1 \pmod{2p^\alpha}, \quad g^r \not\equiv 1 \pmod{2p^\alpha}, \quad 0 < r < d.$$

故g 是模$2p^\alpha$ 的一个原根.

(iii) 若g 是偶数, 则$g + p^\alpha$ 是奇数, 类似(ii)可得结论. 证毕

例5.2.4 设$m = 41^2 = 1681$, 求模m 的原根.

解 由例5.2.1 , 有$g = 6$ 是模$p = 41$ 的原根. 作计算

$$g^{p-1} = 6^{40} \equiv 143 \equiv 1+3\cdot 41, \qquad (g+p)^{p-1} = 47^{40} \equiv 1518 \equiv 1+37\cdot 41 \pmod{41^2}.$$

因此, $g = 6$ 和$g + p = 47$ 都是模$m = p^2$ 的原根.

根据§5.1 定理5.2.5 和定理5.2.6 , $(d, \varphi(m)) = 1$时, $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, 因此, 当$d$ 遍历模$\varphi(41^2) = 1640$ 的简化剩余系时, 6^d遍历模41^2的所有原根.

例5.2.5 设$m = 2 \cdot 41^2 = 3362$, 求模m 的原根.

解 这里应用定理5.2.4 及例5.2.4 , 即可得到$6 + 41^2 = 1687$ 和47 是模$2 \cdot 41^2 = 3362$ 的原根.

例5.2.6 设$m = 43^2 = 1849$, 求模m 的原根.

解 由例5.2.2 , 有$g = 3$ 是模$p = 43$ 的原根. 根据定理5.2.3, 可知$g = 3$ 或者$g + p = 3 + 43 = 46$ 是模$43^2 = 1849$ 的原根. 事实上, 我们有

$$g^{p-1} = 3^{42} \equiv 87 \equiv 1 + 2 \cdot 43 \pmod{43^2},$$

$$(g + p)^{p-1} = 46^{40} \equiv 689 \equiv 1 + 16 \cdot 43 \pmod{43^2}.$$

因此, $g = 3$ 和$g + p = 46$ 都是模$m = p^2$ 的原根, 也都是模$m = p^\alpha$ 的原根.

例5.2.7 设$m = 191^2 = 36481$, 求模m 的原根.

解 由例5.2.3, 有$g = 19$ 是模$p = 191$ 的原根, 所以根据定理5.2.3, 可知$g = 19$ 或者$g + p = 19 + 191 = 210$ 是模$191^2 = 1849$ 的原根. 事实上, 我们有

$$g^{p-1} = 19^{190} \equiv 15854 \equiv 1 + 83 \cdot 191 \pmod{191^2},$$

$$(g + p)^{p-1} = 210^{190} \equiv 17764 \equiv 1 + 93 \cdot 191 \pmod{191^2}.$$

因此, $g = 19$ 和$g + p = 210$ 都是模$m = p^2$ 的原根, 也都是模$m = p^\alpha$ 的原根.

5.2.3 模2^α 指数

先给出两个引理:

引理5.2.4 设a 是一个奇整数. 如果

$$a^2 = 1 + u_1 \cdot 2^t, \quad (u_1, 2) = 1,\ t \geq 3, \tag{11}$$

则对任意整数$k > t$, 存在整数u_{k-t} 使得

$$a^{2^{k-t}} = 1 + u_{k-t} \cdot 2^{k-1}, \quad (u_{k-t}, 2) = 1. \tag{12}$$

证 我们对$k > t$ 作数学归纳法, 来证明关系式(12)

$k = t + 1$时, 关系式(12)就是关系式((11)), 命题成立.

假设$k - 1 > t$ 时, 命题成立, 即存在整数u_{k-1-t} 使得

$$a^{2^{k-1-t}} = 1 + u_{k-1-t} \cdot 2^{k-2}, \quad (u_{k-1-t}, 2) = 1.$$

两端作2 次方, 我们有

$$a^{2^{k-t}} = 1 + (u_{k-1-t} + u_{k-1-t}^2 \cdot 2^{k-3}) \cdot 2^{k-1} = 1 + u_{k-t} \cdot 2^{k-1} \tag{13}$$

其中$u_{k-t} = u_{k-1-t} + u_{k-1-t}^2 \cdot 2^{k-3}$ 满足$(u_{k-t}, 2) = (u_{k-1-t}, 2) = 1$. 命题成立.

引理5.2.5 设整数$t \geq 3$. 对于整数$k > t$, 如果奇整数a 满足关系式(12), 即

$$a^{2^{k-t}} = 1 + u_{k-t} \cdot 2^{k-1}, \quad (u_{k-t}, 2) = 1,$$

则 a 模2^k 的指数为2^{k-t+1}.

证 令$e_k = \mathrm{ord}_{2^k}(a)$. 则我们有 $a^{e_k} \equiv 1 \pmod{2^k}$.

根据欧拉定理(定理2.4.1), 有$e_k \mid \varphi(2^k) = 2^{k-1}$. 所以$e_k$ 具有形式$e_k = 2^s$. 下面确定$s = k - t + 1$.

一方面, 根据引理5.2.4 之证明(14), 由假设条件(12), 可得到

$$a^{2^{k-t+1}} = 1 + (u_{k-t} + u_{k-t}^2 \cdot 2^{k-2}) \cdot 2^k = 1 + u_{k-t+1} \cdot 2^k \tag{14}$$

其中$u_{k-t+1} = u_{k-t} + u_{k-t}^2 \cdot 2^{k-2}$ 满足$(u_{k-t+1}, 2) = (u_{k-t}, 2) = 1$, 从而$e_k \mid 2^{k-t+1}$, $s \leq k - t + 1$.

另一方面, 仍由假设条件(12), 知

$$a^{2^{k-t}} \not\equiv 1 \pmod{2^k},$$

得到$e_k \nmid 2^{k-t}$, $s > k - t$.

故$s = k - t + 1$, $e_k = 2^{k-t+1} = \varphi(p^k)/2^{t-2}$. 证毕

再讨论奇整数的指数的上界.

定理5.2.6 设a是一个奇整数. 则对任意整数$\alpha \geq 3$, 有a 模2^α 的指数不大于$\varphi(2^\alpha)/2 = 2^{\alpha-2}$, 即

$$a^{\varphi(2^\alpha)/2} \equiv a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \tag{15}$$

证 将奇整数a写成$a = 1 + b \cdot 2$, 因为$2 \mid b(b+1)$, 所以有

$$a^2 = 1 + b(b+1) \cdot 2^2 = 1 + u_1 \cdot 2^t, \quad (u_1, 2) = 1,\ t \geq 3.$$

对于整数$\alpha \geq 3$, 当$\alpha \leq t$ 时, 有

$$a^2 \equiv 1 \pmod{2^\alpha},$$

所以a 模2^α 的指数为$2 \leq \varphi(2^\alpha)/2 = 2^{\alpha-2}$.

而当$\alpha > t$ 时, 由引理5.2.4, 知有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, a 模2^α 的指数为$2^{\alpha-t+1} \leq \varphi(2^\alpha)/2 = 2^{\alpha-2}$.

证毕

定理5.2.7 设$\alpha \geq 3$是一个整数. 则

$$\mathrm{ord}_{2^\alpha}(5) = \varphi(2^\alpha)/2 = 2^{\alpha-2}.$$

证 因为$a = 5$ 具有形式

$$a^2 = 1 + 3 \cdot 2^3 = 1 + u_1 \cdot 2^t, \quad u_1 = 3,\ t = 3,$$

对于整数$\alpha \geq 3$, 由引理5.2.4, 知有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 5$ 模2^α 的指数为$2^{\alpha-t+1} = \varphi(2^\alpha)/2$.
证毕

例5.2.8 设$\alpha \geq 3$是一个整数. 则对于整数$a = 8k + 3$,

$$\mathrm{ord}_{2^\alpha}(a) = \varphi(2^\alpha)/2.$$

证 因为$a = 8k + 3$具有形式

$$a^2 = 1+(1+2(3k+4k^2))\cdot 2^3 = 1+u_1\cdot 2^t, \quad u_1 = 1+2(3k+4k^2),\ t = 3,$$

对于整数$\alpha \geq 3$, 由引理5.2.4, 知有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 8k + 3$模2^α的指数为$2^{\alpha-t+1} = \varphi(2^\alpha)/2$. 证毕

例5.2.9 设$\alpha \geq 3$ 是一个整数. 则对于整数$a = 2^s - 1,\ \ 3 \leq s < \alpha$, 有

$$\mathrm{ord}_{2^\alpha}(a) = 2^{\alpha - s}.$$

证 因为$a = 2^s - 1$ 具有形式

$$a^2 = 2^{2s} - 2^{s+1} + 1 = 1 + (2^{s-1} - 1) \cdot 2^{s+1} = 1 + u_1 \cdot 2^t, \quad u_1 = 2^{s-1} - 1,\ t = s + 1,$$

对于整数$\alpha \geq 3$, 由引理5.2.4 , 知有关系式

$$a^{2^{\alpha - t}} = 1 + u_{\alpha - t} \cdot 2^{\alpha - 1}, \quad (u_{\alpha - t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 2^s - 1$ 模2^α 的指数为$2^{\alpha - t + 1} = 2^{\alpha - s}$. 证毕

5.2.4 模m 原根

本节给出模m 原根存在的充要条件.

定理5.2.8 模m 的原根存在的充要条件是$m = 2,\ 4,\ p^{\alpha},\ 2p^{\alpha}$, 其中$p$是奇素数.

证 必要性. 设m 的标准分解式为 $m = 2^{\alpha}p_1^{\alpha_1}\cdots 2p_k^{\alpha_k}$.

若$(a,m) = 1$, 则 $(a,2^{\alpha}) = 1,\quad (a,p_i^{\alpha_i}) = 1,\quad i = 1,\ldots,k.$

根据定理2.4.1 (欧拉定理)及定理5.2.6, 我们有

$$\begin{cases} a^{\tau} \equiv 1 \pmod{2^{\alpha}} \\ a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}} \\ \vdots \\ a^{\varphi(p_k^{\alpha_k})} \equiv 1 \pmod{p_k^{\alpha_k}}, \end{cases}$$

其中$\tau = \begin{cases} \varphi(2^{\alpha}), & \alpha \le 2, \\ \frac{1}{2}\varphi(2^{\alpha}), & \alpha \ge 3. \end{cases}$

令 $h = [\tau,\ \varphi(p_1^{\alpha_1}),\ \ldots,\ \varphi(p_k^{\alpha_k})]$.

根据定理5.1.6之推论, 对所有整数$a,\ (a,m) = 1$, 我们有

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

因此, 若$h < \varphi(m)$, 则模m 的原根不存在.

现在讨论何时 $h = \varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.

(1) 当$\alpha \geq 3$ 时, $\tau = \dfrac{\varphi(2^\alpha)}{2}$. 因此, $h \leq \dfrac{\varphi(m)}{2} < \varphi(m)$.

(2) 当$k \geq 2$ 时, $2 \mid \varphi(p_1^{\alpha_1})$, $2 \mid \varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2})] \leq \frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) < \varphi(p_1^{\alpha_1}p_2^{\alpha_2}).$$

因此, $h < \varphi(m)$.

(3) 当$\alpha = 2,\ k = 1$时, $\varphi(2^\alpha) = 2$, $2 \mid \varphi(p_1^{\alpha_1})$.

因此, $h = \varphi(p_1^{\alpha_1}) < \varphi(2^n)\varphi(p_1^{\alpha_1}) = \varphi(m)$.

故只有在(α, k) 是

$$(1,0),\ (2,0),\ (0,1),\ (1,1)$$

四种情形之一, 即只有在m是

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

四数之一时, 才有可能$h = \varphi(m)$. 因此必要性成立.

充分性. 当$m=2$ 时, $\varphi(2)=1$, 整数1 是模2 的原根;
当$m=4$ 时, $\varphi(4)=2$, 整数3 是模4 的原根;
当$m=p^{\alpha}$ 时, 根据定理5.2.4, 模m 的原根存在;
当$m=2p^{\alpha}$ 时, 根据定理5.2.5, 模m 的原根存在.
因此,条件的充分性是成立的. 证毕

例5.2.10 设$m = 41$, 求模m 的所有整数的指数表.

解 模$m = 41$ 的指数表为:

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

例5.2.11 设$m = 43$, 求模m 的所有整数的指数表.

解 模$m = 43$ 的指数表为:

a	order	a	order	a	order	a	order	a	order
1	1	11	7	21	7	31	21	41	7
2	14	12	42	22	14	32	14	42	2
3	42	13	21	23	21	33	42		
4	7	14	21	24	21	34	42		
5	42	15	21	25	21	35	7		
6	3	16	7	26	42	36	3		
7	6	17	21	27	14	37	6		
8	14	18	42	28	42	38	21		
9	21	19	42	29	42	39	14		
10	21	20	42	30	42	40	21		

例5.2.12 设$m = 167$, 求模m 的所有整数的指数表.

解 模$m = 167$ 的指数表为:

a	order	a	order	a	order	a	order	a	order	a	order
1	1	11	83	21	83	31	83	41	166	51	166
2	83	12	83	22	83	32	83	42	83	52	166
3	83	13	166	23	166	33	83	43	166	53	166
4	83	14	83	24	83	34	166	44	83	54	83
5	166	15	166	25	83	35	166	45	166	55	166
6	83	16	83	26	166	36	83	46	166	56	83
7	83	17	166	27	83	37	166	47	83	57	83
8	83	18	83	28	83	38	83	48	83	58	83
9	83	19	83	29	83	39	166	49	83	59	166
10	166	20	166	30	166	40	166	50	83	60	166

a	order	a	order	a	order	a	order	a	order	a	order
61	83	71	166	81	83	91	166	101	166	111	166
62	83	72	83	82	166	92	166	102	166	112	83
63	83	73	166	83	166	93	83	103	166	113	166
64	83	74	166	84	83	94	83	104	166	114	83
65	83	75	83	85	83	95	166	105	166	115	83
66	83	76	83	86	166	96	83	106	166	116	83
67	166	77	83	87	83	97	83	107	83	117	166
68	166	78	166	88	83	98	83	108	83	118	166
69	166	79	166	89	83	99	83	109	166	119	166
70	166	80	166	90	166	100	83	110	166	120	166

a	order	a	order	a	order	a	order	a	order
121	83	131	166	141	83	151	166	161	166
122	83	132	83	142	166	152	83	162	83
123	166	133	83	143	166	153	166	163	166
124	83	134	166	144	83	154	83	164	166
125	166	135	166	145	166	155	166	165	166
126	83	136	166	146	166	156	166	166	2
127	83	137	83	147	83	157	83		
128	83	138	166	148	166	158	166		
129	166	139	166	149	166	159	166		
130	83	140	166	150	83	160	166		

例5.2.13 求模$m = 53$ 的原根.

解 设$m = 53$, 则

$$\varphi(m) = \varphi(53) = 2^2 \cdot 13, \quad q_1 = 2,\ q_2 = 13.$$

因此,

$$\varphi(m)/q_1 = 26, \quad \varphi(m)/q_2 = 44.$$

这样,只需验证: g^{26}, g^4 模m是否同余于1. 对$2, 3, \ldots$ 逐个验算:

$$2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^8 \equiv 44, \quad 2^{12} \equiv 15,$$
$$2^{13} \equiv 30, \ 2^{26} \equiv 52 \equiv -1, \ (\mathrm{mod}\ 53).$$

因此, $g = 2$ 是模$m = 53$ 的原根.

例5.2.14 求模$m = 109$ 的原根.

解 设$m = 109$, 则

$$\varphi(m) = \varphi(109) = 108 = 2^2 \cdot 3^3, \quad q_1 = 2,\ q_2 = 3.$$

因此,

$$\varphi(m)/q_1 = 54, \quad \varphi(m)/q_2 = 36.$$

这样,只需验证: $g^{54},\ g^{36}$ 模m是否同余于1. 对$2,\ 3,\ 5,\ 6, \ldots$ 逐个验算:

$$\begin{aligned} &2^{54} \equiv 108,\ 2^{36} \equiv 1, \quad 3^{54} \equiv 1, \quad 3^{36} \equiv 63, \\ &5^{54} \equiv 1, \quad 5^{36} \equiv 63,\ 6^{54} \equiv 108,\ 6^{36} \equiv 63,\ (\mathrm{mod}\ 109). \end{aligned}$$

因此, $g = 6$ 是模$m = 109$ 的原根.

例5.2.15 求模$m = 113$ 的原根.

解 设$m = 113$, 则

$$\varphi(m) = \varphi(113) = 112 = 2^4 \cdot 7, \quad q_1 = 2,\ q_2 = 7.$$

因此,

$$\varphi(m)/q_1 = 56, \quad \varphi(m)/q_2 = 16.$$

这样,只需验证: $g^{56},\ g^{16}$ 模m是否同余于1. 对$2,\ 3,\ 5,\ 6, \ldots$ 逐个验算:

$$2^{56} \equiv 1,\ 2^{16} \equiv 109,\ 3^{56} \equiv 112,\ 3^{36} \equiv 49,\ (\mathrm{mod}\ 113).$$

因此, $g = 3$ 是模$m = 113$ 的原根.

例5.2.16 求模$m = 59$ 的原根.

解 设$m = 59$, 则

$$\varphi(m) = \varphi(59) = 2 \cdot 29, \quad q_1 = 2,\ q_2 = 29.$$

因此,

$$\varphi(m)/q_1 = 29, \quad \varphi(m)/q_2 = 2.$$

这样,只需验证: $g^{29},\ g^2$ 模m是否同余于1. 对$2,\ 3,\ \ldots$ 逐个验算:

$$2^2 \equiv 4,\ \ 2^{29} \equiv 58 \equiv -1,\ \ (\mathrm{mod}\ 59).$$

因此, $g = 2$ 是模$m = 59$ 的原根.

例5.2.17 求模$m = 61$ 的原根.

解 设$m = 61$, 则

$$\varphi(m) = \varphi(61) = 2^2 \cdot 3 \cdot 5, \quad q_1 = 2,\ q_2 = 29,\ q_3 = 5.$$

因此,

$$\varphi(m)/q_1 = 30, \quad \varphi(m)/q_2 = 20, \quad \varphi(m)/q_3 = 12.$$

这样,只需验证: $g^{30},\ g^{20},\ g^{12}$ 模m是否同余于1. 对$2,\ 3,\ \ldots$ 逐个验算:

$$2^{30} \equiv 60,\ \ 2^{20} \equiv 47,\ \ 2^{12} \equiv 9,\ \ (\mathrm{mod}\ 61).$$

因此, $g = 2$ 是模$m = 61$ 的原根.