初等数论
第五章 原根与指标

中山大学 计算机学院

1. 指数

根据欧拉定理，当a与$m(m>1)$互素时，有$a^{\varphi(m)} \equiv 1 \bmod m$成立，

1.1. 指数

设$m>1$是整数，a是与m互素的正整数(即a处于模m的一个简化剩余系中)，称使得

$$a^e \equiv 1 \bmod m$$

的最小正整数e为a对模m的指数(或阶)，记作$\mathrm{ord}_m(a)$

如果a对模m的指数是$\varphi(m)$，这时称a为模m的原根.

示例：$m=7, \varphi(m)=6,$
对$a=1$来说，$1^1=1$，所以a的指数为1
对$a=2$来说，$2^1=2, 2^2=4, 2^3 \equiv 1 \bmod 7$，所以2的指数为3
对$a=3$来说，$3^1=3, 3^2 \equiv 2, \ldots, 3^6 \equiv 1 \bmod 7$，所以3的指数为6

类似计算，4的指数为3，5的指数为6，6的指数为2.
可见上述只有3,5是模7的原根

示例: $m = 15, \varphi(m) = 8$

$1 \sim 5$的数中与15互素的数有1,2,4,7,8,11,13,14
类似上述计算可以看出它们的指数分别为:

a	1	2	4	7	8	11	13	14
$\mathrm{ord}_m(a)$	1	4	2	4	4	2	4	2

可见没有模15的原根. 或者说"并不是对于任意大于1的整数m都有模m的原根".

定理

设m是大于1的整数，a与m互素. 整数d使得$a^d \equiv 1 \bmod m$当且仅当$\mathrm{ord}_m(a) \mid d$.

"必要性:"

$$\mathrm{ord}_m(a) \mid d \Longrightarrow d = k \cdot \mathrm{ord}_m(a) \Longrightarrow a^d = (a^{\mathrm{ord}_m(a)})^k \Longrightarrow a^d \equiv 1 \bmod m$$

"充分性:" 假设d使得$a^d \equiv 1 \bmod m$,
如果$\mathrm{ord}_m(a) \nmid d$, 则由欧几里德除法知, 存在整数$q, r$使得

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

从而

$$a^d \equiv a^r \cdot (a^{\mathrm{ord}_m(a)})^q \bmod m$$

而

$$a^d \equiv 1 \bmod m$$

从而$a^r \equiv 1 \bmod m$, 但这就与指数的定义矛盾.

根据欧拉定理, 如果a与m互素, $\varphi(m)$使得$a^{\varphi(m)} \equiv 1 \bmod m$, 因此有$\mathrm{ord}_m(a) \mid \varphi(m)$.
a对模m的指数必定是$\varphi(m)$的因子, 所以为了求a的指数, 只需要在$\varphi(m)$的因子中找.

示例: 求$\mathrm{ord}_{17}(5)$

因为$\varphi(17) = 16$的因子是1,2,4,8,16,

检查$5^1, 5^2, 5^4, 5^8, 5^{16}$,

可以发现只有$5^{16} \equiv 1 \bmod 17$

所以$\mathrm{ord}_{17}(5) = 16$, 从而5是模17的原根.

定理

设m是大于1的整数, a与m互素. 如果$n \mid m$, 则$\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

$$\left.\begin{array}{r} a^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \\ n \mid m \end{array}\right\} \Longrightarrow a^{\mathrm{ord}_m(a)} \equiv 1 \bmod n \Longrightarrow \mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$$

定理

设m是大于1的整数, a与m互素. 如果$b \equiv a \bmod m$, 则$\mathrm{ord}_m(a) = \mathrm{ord}_m(a)$.

事实上, $b \equiv a \bmod m \Longrightarrow a^{\mathrm{ord}_m(b)} \equiv b^{\mathrm{ord}_m(b)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$.
类似地, $b \equiv a \bmod m \Longrightarrow b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$.
所以有, $\mathrm{ord}_m(a) = \mathrm{ord}_m(a)$.

例如,

$$39 \equiv 5 \bmod 17 \Longrightarrow \mathrm{ord}_{17}(39) = \mathrm{ord}_{17}(5) = 16.$$

定理

设m是大于1的整数，a与m互素. 如果$ab \equiv 1 \bmod m$, 则$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

事实上

$$(ab)^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \Longrightarrow a^{\mathrm{ord}_m(a)} \cdot b^{\mathrm{ord}_m(a)} \equiv 1 \bmod m$$
$$\Longrightarrow b^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(b) \,|\, \mathrm{ord}_m(a).$$

类似地

$$(ab)^{\mathrm{ord}_m(b)} \equiv 1 \bmod m \Longrightarrow a^{\mathrm{ord}_m(b)} \cdot b^{\mathrm{ord}_m(b)} \equiv 1 \bmod m$$
$$\Longrightarrow a^{\mathrm{ord}_m(b)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(a) \,|\, \mathrm{ord}_m(b).$$

所以有, $\mathrm{ord}_m(a) = \mathrm{ord}_m(a)$.

例如,

$$5 \cdot 7 \equiv 1 \bmod 17 \Longrightarrow \mathrm{ord}_{17}(7) = \mathrm{ord}_{17}(5) = 16$$

定理

设m是大于1的整数, a与m互素.

$$a^0(=1), a^1, a^2, \ldots, a^{\mathrm{ord}_m(a)-1}$$

模m两两不同余.

如果存在$0 \le l < k \le \mathrm{ord}_m(a) - 1$ 使得$a^k \equiv a^l \bmod m$. 又因为a与m互素, 所以有$a^{k-l} \equiv 1 \bmod m$成立, 且$k - l < \mathrm{ord}_m(a) - 1$. 这就与指数的定义矛盾. $\diamond$

根据这个结论, 当$\mathrm{ord}_m(a) = \varphi(m)$时, 即$a$是模$m$的原根时,

$$\{a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}\}$$

这些数正好构成了模m的一个简化剩余系.

例如, $\{5^0, 5^1, \ldots, a^{\varphi(m)-1}\}$正好是模17的一个简化剩余系, 因为5是模17的一个原根.

定理

设m是大于1的整数, a与m互素. $a^k \equiv a^l \bmod m$当且仅当$k \equiv l \bmod \mathrm{ord}_m(a)$.

根据欧几里德除法, 存在整数q, r和q', r'使得

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

和

$$l = q' \cdot \mathrm{ord}_m(a) + r', \quad 0 \le r' < \mathrm{ord}_m(a)$$

成立, 从而有

$$a^k = a^{\mathrm{ord}_m(a) q + r} \equiv a^r \bmod m,$$

以及

$$a^l = a^{\mathrm{ord}_m(a) q' + r'} \equiv a^{r'} \bmod m$$

成立.

"必要性:" $a^k \equiv a^l \bmod m \Longrightarrow a^r \equiv a^{r'} \bmod m$, 于是$r = r'$, 所以$k \equiv l \bmod \mathrm{ord}_m(a)$

"充分性:" $k \equiv l \bmod \mathrm{ord}_m(a) \Longrightarrow r = r' \Longrightarrow a^k \equiv a^l \bmod m$ ◇

定理

设m是大于1的整数, a与m互素, k是非负整数. $\text{ord}_m(a^k) = \dfrac{\text{ord}_m(a)}{(\text{ord}_m(a), k)}$.

证明: 设$d = (\text{ord}_m(a), k)$. 先证明$\dfrac{\text{ord}_m(a)}{d} \mid \text{ord}_m(a^k)$.

$$\because a^{k\cdot\text{ord}_m(a^k)} = (a^k)^{\text{ord}_m(a^k)} \equiv 1 \bmod m$$

$$\therefore \text{ord}_m(a) \mid (k \cdot \text{ord}_m(a^k)) \qquad \therefore \frac{\text{ord}_m(a)}{d} \mid (\text{ord}_m(a^k) \cdot \frac{k}{d}).$$

又因为$(\dfrac{\text{ord}_m(a)}{d}, \dfrac{k}{d}) = 1$, 所以$\dfrac{\text{ord}_m(a)}{d} \mid \text{ord}_m(a^k)$.
另一方面,

$$\because (a^k)^{\frac{\text{ord}_m(a)}{d}} = (a^{\text{ord}_m(a)})^{\frac{k}{d}} \equiv 1 \bmod m \qquad \therefore \text{ord}_m(a^k) \mid \frac{\text{ord}_m(a)}{d} \qquad \diamond$$

例如, 5模17的指数是16, 则5^2(即8)模17的指数是$\dfrac{16}{(16,2)} = 8$.

推论

设m是大于1的整数，k是非负整数．如果a是模m的原根，则$a^k(k>0)$也是模m的原根当且仅当$(k,\varphi(m))=1$.

推论

设m是大于1的整数．如果模m有原根，则模m的原根的个数为$\varphi(\varphi(m))$，且从模m的简化剩余中均匀随机选取一个元素是模m原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}.$$

定理

设m是大于1的整数，a,b都是与m互素的整数，r是a的模m的指数，s是b的模m的指数，t是ab的模m的指数，则$t=rs$当且仅当r与s互素，即

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

证明: "充分性:" 需要说明t与rs相互整除.
先说明$t\,|\,(rs)$: $(ab)^{rs}=a^{rs}b^{rs}=(a^r)^s(b^s)^r\equiv 1 \bmod m\implies t\,|\,(rs)$
再说明$(rs)\,|\,t$: 只需要说明$r\,|\,t,s\,|\,t$, 而r与s互素, 所以$rs\,|\,t$. 为此,

$$a^{st}\equiv a^{st}(b^s)^t=(ab)^{st}=[(ab)^t]^s\equiv 1 \bmod m$$

$$\therefore r\,|\,(st)$$

又因为r与s互素, 所以有$r\,|\,t$;

$$b^{rt}\equiv b^{rt}(a^r)^t=(ab)^{rt}=[(ab)^t]^r\equiv 1 \bmod m$$

$$\therefore s\,|\,(rt)$$

又因为r与s互素, 所以有$s\,|\,t$.

下面证明"必要性:"
如果$t=rs$, 那么

$$\because (ab)^{[r,s]} = a^{[r,s]}b^{[r,s]} \equiv 1 \bmod m$$

$$\therefore t|[r,s] \qquad \therefore (rs)|[r,s] \qquad \therefore [r,s]=rs, \qquad \therefore (r,s)=1 \qquad \diamond$$

这个结论还说明,
不一定有

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

不一定有

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

例如, $m=10, a=b=3$, 则$\mathrm{ord}_m(ab)=2$, 而$\mathrm{ord}_m(a)=\mathrm{ord}_m(b)=4$.

定理

设m是大于1的整数，a,b均与m互素．存在c使得$\mathrm{ord}_m(c)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$.

回忆最小公倍数的性质，存在u,v使得

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

令

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

从而

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

这样a^s模m的指数与b^t模m的指数互素．再令$c=a^sb^t$，从而有

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

一般地，存在g使得$\mathrm{ord}_m(g)=[\mathrm{ord}_m(a_1),\mathrm{ord}_m(a_2),\ldots,\mathrm{ord}_m(a_k)]$，$2\le k\le\varphi(m)$.
还可以看到，如果$(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$，则有$\mathrm{ord}_m(ab)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$．如果没有该条件，则存在$c$使得$\mathrm{ord}_m(c)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$.

定理

设a, m, n两两互素，r是a模m的指数，s是a模n的指数，t是a模mn的指数. $t = [r, s]$，即$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$.

首先，由于$m \mid mn$，$n \mid mn$，所以有$r \mid t, s \mid t \Longrightarrow [r, s] \mid t$. 另一方面，

$$a^r \equiv 1 \bmod m \Longrightarrow a^{[r,s]} \equiv 1 \bmod m$$

$$a^s \equiv 1 \bmod n \Longrightarrow a^{[r,s]} \equiv 1 \bmod n$$

所以$a^{[r,s]} \equiv 1 \bmod mn$，从而有$t \mid [r, s]$. $\diamond$

(要注意与"$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$未必成立"的区别.)

推论

设p, q是两个不同的素数. 如果a与pq互素，则$\mathrm{ord}_{pq}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)]$. 一般地，如果$m$的标准分解式为$m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}$，$(a, m) = 1$，则有

$$\mathrm{ord}_m(a) = [\mathrm{ord}_{2^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \ldots, \mathrm{ord}_{p_s^{\alpha_s}}(a)].$$

注意与"式子$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$未必成立"的区别.

令

$$\beta \triangleq [\varphi(2^{\alpha_1}), \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})]$$

即β是$\varphi(2^{\alpha_1}), \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})$的最小公倍数,
由于$\mathrm{ord}_{p^\alpha}(a)|\varphi(p^\alpha)$, 从而$\beta$是$\mathrm{ord}_{2^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \ldots, \mathrm{ord}_{p_s^{\alpha_s}}(a)$的公倍数, 所以

$$[\mathrm{ord}_{2^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \ldots, \mathrm{ord}_{p_s^{\alpha_s}}(a)]|\beta$$

即

$$\mathrm{ord}_m(\alpha)|\beta$$

而$\varphi(2^{\alpha_1}) = \begin{cases} 1 & \alpha_1 = 0 \\ 1 & \alpha_1 = 1 \\ 2 & \alpha_1 = 2 \\ 2^{\alpha_1} - 2^{\alpha_1 - 1} = 2^{\alpha_1 - 1} & \alpha_1 \geq 3 \end{cases}$

所以

$$\beta = \begin{cases} [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ [2^{\alpha_1 - 1}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases}$$

5-1 从而有

$$\begin{cases} \mathrm{ord}_m(a) | [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ \mathrm{ord}_m(a) [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ \mathrm{ord}_m(a) [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ \mathrm{ord}_m(a) [2^{\alpha_1 - 1}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases} \quad \diamond$$

事实上，设a是奇数(比如表示成$a = 2t + 1, t \in \mathbb{Z}$)，则有$a^{2^{l-2}} \equiv 1 \bmod 2^l (l \geq 3)$成立，**可以对$l$使用数学归纳法证明这个等式:**

当$l = 3$时，$a^2 = 4t(t + 1) + 1 \equiv 1 \bmod 2^3$;

当$l = n$时成立，即$a^{2^{n-2}} \equiv 1 \bmod 2^n$，即$a^{2^{n-2}} = k \cdot 2^n + 1$，

当$l = n + 1$时，

$$a^{2^{n-1}} - 1 = (a^{2^{n-2}} - 1)(a^{2^{n-2}} + 1) = k \cdot 2^n (k \cdot 2^n + 2) = k^2 \cdot 2^{2n} + k \cdot 2^{n+1}$$

所以$a^{2^{n-1}} - 1 \equiv 0 \bmod 2^{n+1}, \qquad i.e., a^{2^{n-1}} \equiv 1 \bmod 2^{n+1}$

这个结论说明，$\mathrm{ord}_{2^l}(a) | 2^{l-2} (l \geq 3)$

所以我们有:

$$[\mathrm{ord}_{2^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \ldots, \mathrm{ord}_{p_s^{\alpha_s}}(a)] | 2^{\alpha_1 - 2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})$$

即$\mathrm{ord}_m(a) | 2^{\alpha_1 - 2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})$

5-2 从而有

$$\begin{cases} \mathrm{ord}_m(a) | [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ \mathrm{ord}_m(a) [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ \mathrm{ord}_m(a) [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ \mathrm{ord}_m(a) [2^{\alpha_1 - 2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases} \quad \diamond$$

重新记右边的最小公倍数为β, 即

$$m = p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s} : \beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})]$$

$$m = 2p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s} : \beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})]$$

$$m = 4p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s} : \beta = [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})]$$

$$m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s} : \beta = [2^{\alpha_1 - 2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})]$$

5-3 模m存在原根$\Longrightarrow m=1$, 或2, 或4, 或p^α, 或$2p^\alpha$(p是奇素数).

证明: 反设m不属于这几种情形, 那么m的形式就是$m=2^\alpha(\alpha\geq 3)$, 或是$m=2^\alpha p_1^{\alpha_1}\dots p_r^{\alpha_r}(\alpha\geq 2, r\geq 1)$, 或是$m=2^\alpha p_1^{\alpha_1}\dots p_r^{\alpha_r}(\alpha\geq 0, r\geq 2)$

$<1>$, 如果$m=2^\alpha(\alpha\geq 3)$, 则$\varphi(m)=2^{\alpha-1}$
但$\mathrm{ord}_{2^\alpha}(a)|2^{\alpha-1}$, 所以$\mathrm{ord}_m(a)\leq 2^{\alpha-2}<2^{\alpha-1}=\varphi(m)$, 可见这时模$m$没有原根;
$<2>$, 如果$m=2^\alpha p_1^{\alpha_1}\dots p_r^{\alpha_r}(\alpha\geq 2, r\geq 1)$,
即$m=4p_1^{\alpha_1}\dots p_r^{\alpha_r}(r\geq 1)$或$m=2^\alpha p_1^{\alpha_1}\dots p_r^{\alpha_r}(\alpha\geq 3, r\geq 1)$, 对应地
有$\varphi(m)=2\varphi(p_1^{\alpha_1})\dots\varphi(p_r^{\alpha_r})$ 和$\varphi(m)=2^{\alpha-1}\varphi(p_1^{\alpha_1})\dots\varphi(p_r^{\alpha_r})$

对应地,前述的$\beta=[2,\varphi(p_2^{\alpha_2}),\varphi(p_3^{\alpha_3}),\dots,\varphi(p_r^{\alpha_r})]$, 注意到$p_i$都是奇素数, 所以$\varphi(p_i^{\alpha_i})=p_i^{\alpha_i}-p_i^{\alpha_i-1}$都是偶数,所
以$\beta=[2,\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\dots,\varphi(p_r^{\alpha_r})]=[\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\dots,\varphi(p_r^{\alpha_r})]\leq$
$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})<2\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})=\varphi(m)$, 所以,
$\forall a, \mathrm{ord}_m(a)<\varphi(m)$, 可见这时模$m$没有原根;
和
$\beta=[2^{\alpha-2},\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\dots,\varphi(p_r^{\alpha_r})]\leq 2^{\alpha-2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})<$
$2^{\alpha-1}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})=\varphi(m)$,
所以, $\forall a, \mathrm{ord}_m(a)<\varphi(m)$, 可见这时模$m$没有原根;

$< 3 >$, 如果$m = 2^{\alpha} p_1^{\alpha_1} \dots p_r^{\alpha_r} (\alpha \geq 0, r \geq 2)$, 即$m = p_1^{\alpha_1} \dots p_r^{\alpha_r} (r \geq 2)$ 或$m = 2p_1^{\alpha_1} \dots p_r^{\alpha_r} (r \geq 2)$ 或$m = 4p_1^{\alpha_1} \dots p_r^{\alpha_r} (\alpha \geq 3, r \geq 2)$ 对应地,

$\varphi(m) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$
$\varphi(m) = \varphi(2)\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$
$\varphi(m) = \varphi(4)\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = 2\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$
$\varphi(m) = \varphi(2^{\alpha})\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = 2^{\alpha-1}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$
相应的
$\beta = [1, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$
$\beta = [1, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$
$\beta = [2, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] = [\varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) < 2\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$
$\beta = [2^{\alpha-2}, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] \leq 2^{\alpha-2}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) < 2^{\alpha-1}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$
所以, $\forall a, \mathrm{ord}_m(a) < \varphi(m)$, 可见这时模$m$没有原根.

可见不论m属于反设的哪一种情形, 总有$\forall a, \mathrm{ord}_m(a) < \varphi(m)$, 所以对这些$m$, 模$m$都没有原根. 所以, 如果模$m$有原根的话, 只能是1, 或2, 或4, 或$p^{\alpha}$, 或是$2p^{\alpha}$ ◇

定理

设m, n互素，a_1, a_2均与mn互素. 存在a使得$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

根据中国剩余定理，同余式组$\begin{cases} x \equiv a_1 \bmod m \\ x \equiv a_2 \bmod n \end{cases}$有唯一解

$$x \equiv (x^{-1} \bmod m) \cdot n \cdot a_1 + (m^{-1} \bmod n) \cdot m \cdot a_2 \bmod M.$$

令$a = [x^{-1} \bmod m] \cdot n \cdot a_1 + [m^{-1} \bmod n] \cdot m \cdot a_2$，显然$a \equiv a_1 \bmod m, a \equiv a_2 \bmod n$，因此，

$$\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1), \quad \mathrm{ord}_n(a) = \mathrm{ord}_n(a_2).$$

从而

$$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)] = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)] \qquad \diamond$$

可以看出，如果$a_1 = a_2$，则$\mathrm{ord}_{mn}(a_1) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_1)]$. 如果没有条件$a_1 = a_2$，则存在$a$使得$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.
与此对比，如果$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，则有$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$. 如果没有该条件，则存在$c$使得$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$.

2. 模素数p的原根

定理

设p是素数，则模p有原根.

证明：在模p的简化剩余系中，存在g使得

$$\mathrm{ord}_p(g) = [\mathrm{ord}_p(1), \mathrm{ord}_p(2), \ldots, \mathrm{ord}_p(p-1)].$$

记这个最小公倍数为δ，即这个g的指数为δ，下面证明$\delta = p-1$，即g是模p的原根.
一方面，对这个g，一定有$g^{p-1} \equiv 1 \bmod p$，从而有$\delta \leq p-1$.
另一方面，由于δ是$\mathrm{ord}_p(1), \mathrm{ord}_p(2), \ldots, \mathrm{ord}_p(p-1)$的公倍数，所以

$$\mathrm{ord}_p(1) \mid \delta, \mathrm{ord}_p(2) \mid \delta, \ldots, \mathrm{ord}_p(p-1) \mid \delta.$$

这表明

$$1^\delta \equiv 1 \bmod p, 2^\delta \equiv 1 \bmod p, \ldots, (p-1)^\delta \equiv 1 \bmod p.$$

也是就是说，同余方程

$$x^\delta - 1 \equiv 0 \bmod p$$

至少有$p-1$个解，从而知道$\delta \geq p-1$. 所以，$\delta = p-1$.

定理

设p是奇素数，$q_1, q_2, \ldots, q_s$是$p-1$的所有素因数. g是模p原根当且仅当

$$g^{\frac{p-1}{q_i}} \not\equiv 1 (\bmod p), \quad i = 1, 2, \ldots, s.$$

示例: 求模$p = 23$的原根.

这里$p - 1 = 22 = 2 \cdot 11$, $p-1$的因子有$1, 2, 11, 22$.

先求$a = 2$对模23的指数:

$$2^2 \equiv 4 \bmod 23$$

$$2^{11} = (2^4)^2 \cdot 2^3 \equiv (-7)^2 \cdot 8 \equiv 3 \cdot 8 \equiv 1 \bmod 23$$

所以$\mathrm{ord}_{23}(2) = 11$, 2不是模23的原根;

再求$a=3$对模23的指数:

$$3^2 \equiv 9 \bmod 23$$

$$3^3 \equiv 4 \bmod 23$$

$$3^{11} = (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \bmod 23$$

所以$\mathrm{ord}_{23}(3) = 11$, 3不是模23的原根;

再求$a=4$对模23的指数:

$$4^2 \equiv -7 \bmod 23$$

$$4^{11} = (4^4)^2 \cdot 4^3 \equiv 3^2 \cdot (-5) \equiv 1 \bmod 23$$

所以$\mathrm{ord}_{23}(4) = 11$, 4不是模23的原根;

再求$a=5$对模23的指数:

$$5^2 \equiv 9 \bmod 23$$

$$5^{11} = (5^4)^2 \cdot 5^3 \equiv 4^2 \cdot 10 \equiv 4 \cdot (-6) \equiv -1 \bmod 23$$

$$5^{22} \equiv 1 \bmod 23$$

所以$\mathrm{ord}_{23}(5) = 22$, 5是模23的原根.

定理

设g是模$p^{\alpha+1}(\alpha \geq 1)$的原根，则$g$必是模$p^\alpha$的原根.

证明：设$\mathrm{ord}_{p^\alpha}(g) = \delta$，从而$\delta | \varphi(p^\alpha)$，
另外，$g^\delta \equiv 1 \bmod p^\alpha$，即$g^\alpha = kp^\alpha + 1$，

$$
\begin{aligned}
(g^\delta)^p &= (kp^\alpha + 1)^p \\
&= C_p^0 (kp^\alpha)^p + C_p^1 (kp^\alpha)^{p-1} + \ldots + C_p^{p-2}(kp^\alpha)^2 + C_p^{p-1}(kp^\alpha) + C_p^p 1 \\
&= (kp^\alpha)^p + p(kp^\alpha)^{p-1} + \ldots + C_p^2 (kp^\alpha)^2 + C_p^1 (kp^\alpha) + 1 \\
&= A \cdot p^{\alpha+1} + kp^{\alpha+1} + 1
\end{aligned}
$$

$$\therefore (g^\delta)^p \equiv 1 \bmod p^{\alpha+1}, \qquad i.e., g^{p\delta} \equiv 1 \bmod p^{\alpha+1}$$

从而应该有$\mathrm{ord}_{p^{\alpha+1}}(g) | p\delta$, $i.e., \varphi(p^{\alpha+1}) | p\delta$, $i.e., p^\alpha(p-1) | p\delta$，从而$p^{\alpha-1}(p-1) | p\delta$，
即$\varphi(p^\alpha) | \delta$.
因此，$\delta = \varphi(p^\alpha)$，即$g$确实也是模$p^\alpha$的原根. $\diamond$

注:二项式定理公式: $(a+b)^n = \sum_{i=0}^n C_n^i a^{n-i} n^i$
$= C_n^0 a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + C_n^3 a^{n-3} b^3 + \ldots + C_n^{n-1} a b^{n-1} + C_n^n b^n$

定理

设g是模p^α的原根，则必有$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^\alpha)$，或$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^{\alpha+1})$

证明：由于$p^\alpha|p^{\alpha+1}$，由前面指数的性质知：

$$\mathrm{ord}_{p^\alpha}(g)|\mathrm{ord}_{p^{\alpha+1}}(g)$$

所以我们有$\varphi(p^\alpha)|\mathrm{ord}_{p^{\alpha+1}}(g)=k\cdot\varphi(p^\alpha)$ 另一方面，我们知道：$\mathrm{ord}_{p^{\alpha+1}}|\varphi(p^{\alpha+1})$，从而$\varphi(p^{\alpha+1})=k'\cdot\mathrm{ord}_{p^{\alpha+1}}(g)$，从而$\varphi(p^{\alpha+1})=k'\cdot k\cdot\varphi(p^\alpha)$
即$p^\alpha(p-1)=kk'p^{\alpha-1}(p-1)$
从而$kk'=p$，即$k=1$且$k'=p$,或者是$k=p$且$k'=1$,

所以$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^\alpha)$,
或$\mathrm{ord}_{p^{\alpha+1}}(g)=p\varphi(p^\alpha)=p\cdot p^{\alpha-1}(p-1)=p^\alpha(p-1)=\varphi(p^{\alpha+1})$. $\diamond$

定理

g是模奇素数p的原根，且g满足$g^{p-1}=1+rp, p\nmid r$，则g是模$p^{\alpha}(\forall\alpha\geq 1)$的原根.

证明：我们先来证明对这个原根g来说总有：

$$\forall\alpha\geq 1, g^{\varphi(p^{\alpha})}=1+r_{\alpha}p^{\alpha}, p\nmid r_{\alpha}$$

其中r_{α}是一个整数.
归纳法：$\alpha=1$时就是已知条件;
假设$\alpha=n$时有$g^{\varphi(p^{n})}=1+r_{n}p^{n}, p\nmid r_{n}$,
当$\alpha=n+1$时，由于$\varphi(p^{k+1})=p\varphi(p^{k})$，所以:

$$\begin{aligned}
g^{\varphi(p^{n+1})} &= g^{p\varphi(p^{n})}=(g^{\varphi(p^{n})})^{p}=(1+r_{n}p^{n})^{p}\\
&= 1+C_{p}^{1}r_{n}p^{n}+C_{p}^{2}(r_{n}p^{n})^{2}+C_{p}^{3}(r_{n}p^{n})^{3}+\ldots\\
&= 1+p^{n+1}r_{n}+C_{p}^{2}r_{n}^{2}p^{2n}+\ldots\\
&= 1+p^{n+1}[r_{n}+\ldots]\\
&= 1+r_{n+1}p^{n+1}
\end{aligned}$$

由于$p\nmid r_{n}$，所以$p\nmid r_{n+1}$. 即$\alpha=n+1$时也成立.

这样, 我们就知道对于满足定理要求的g来说有:

$$g^{\varphi(p)} = 1 + r_1 p, p \nmid r_1 \qquad g^{\varphi(p^2)} = 1 + r_2 p^2, p \nmid r_2$$
$$g^{\varphi(p^3)} = 1 + r_3 p^3, p \nmid r_3 \qquad g^{\varphi(p^4)} = 1 + r_4 p^4, p \nmid r_4 \qquad \ldots$$

由于g是模p的原根, 由前一定理知道$\mathrm{ord}_{p^2}(g) = \varphi(p)$或$\varphi(p^2)$,
如果$\mathrm{ord}_{p^2}(g) = \varphi(p)$的话, 则有$g^{\varphi(p)} \equiv 1 \bmod p^2$, 即$g^{\varphi(p)} = 1 + kp \cdot p$,
与$g^{\varphi(p)} = 1 + r_1 p (p \nmid r_1)$矛盾, 所以$\mathrm{ord}_{p^2}(g) = \varphi(p^2)$, 即$g$是模$p^2$的原根.

再根据g是模p^2的原根, $g^{\varphi(p^2)} = 1 + r_3 p^3 (p \nmid r_3)$类似可以推出$g$是模$p^3$的原根.

这个过程继续下去可知, 满足定理要求的g是模$p^\alpha (\forall \alpha \geq 1)$的原根. $\diamond$

定理

设g'是模奇素数p的原根, 则$g = g', g = g' + p, g = g' + 2p, \dots, g = g' + (p-1)p$都是模$p$的原根.

这是显然的, 因为对于$g = g' + tp, t = 0, 1, \dots, p-1$, 有$g \equiv g' \bmod p$
所以有$\forall i \geq 1 : g^i \equiv g'^i \bmod p$,
而g'是模p的原根, 即

$$g'^i \not\equiv 1 \bmod p, (i < p-1)$$

$$g'^{p-1} \equiv 1 \bmod p$$

从而

$$g^i \not\equiv 1 \bmod p (i < p-1)$$

$$g^{p-1} \equiv 1 \bmod p$$

即g也是模p的原根.. $\diamond$

另外我们也可以看到, 在这p个g中, 除了一个外, 其他的g都满足:$g^{p-1} = 1 + rp, p \nmid r$.

事实上, 注意到

$$g^{p-1} = (g' + tp)^{p-1} = g'^{p-1} + (p-1)g'^{p-2}(tp) + Ap^2$$

其中A是一个整数. 由于g'是模p的原根, 可设$g'^{p-1} = 1 + ap$, 从而

$$g^{p-1} = 1 + [(p-1)g'^{p-2}t + a]p + Ap^2 = 1 + [(p-1)g'^{p-2}t + (a + Ap)]p$$

又由于$(p, p-1) = 1, (p, g') = 1$, 所以$(p, (p-1)g') = 1$, $(p, (p-1)g'^2) = 1$,
$(p, (p-1)g'^3) = 1, \ldots, (p, (p-1)g'^{p-2}) = 1$,
所以关于t的一次同余方程$(p-1)g'^{p-2}t + (a + Ap) \equiv 0 \bmod p$有唯一解.
这也就是说p个g中只有一个不满足条件$g^{p-1} = 1 + rp, p \nmid r$, 其余都满足.

这样我们就可以说: 设p是奇素数, g'为模p的原根,
则$g = g', g = g' + p, g = g' + 2p, \ldots, g = g' + (p-1)p$都是模$p$的原根, 且只有一个不满足条件$g^{p-1} = 1 + rp, p \nmid r$, 其余都满足.

在这个结论中, 如果我们还要求g'满足条件"g'为奇数", 则由于$t=0,1,2,\ldots,p-1$中至少有2个偶数, 从而$g=g'+tp(t=0,1,\ldots,p-1)$中至少有两个是奇数, 所以这两个中(从而这$p$个$g$中)必定存在一个满足: (i)是奇数;(ii)是模p的原根;(iii)满足条件$g^{p-1}=1+rp, p\nmid r$.

如果原根g'不是奇数(即是偶数), 则令$g'':=g'+p$, 则g''是一个为奇数的模p的原根, 用这个g''来构造g即可.

综上, 我们总可以有任意的模p的原根g', 构造一个为奇数的模p的原根$\tilde{g}$满足$\tilde{g}^{p-1}=1+rp, p\nmid r$.

找到的这个$\tilde{g}$自然也是模$p^\alpha(\forall\alpha \geq 1)$的原根.

由于$\tilde{g}$是奇数, 所以我们可以知道

$$\tilde{g}^d \equiv 1 \bmod p^\alpha \iff \tilde{g}^d \equiv 1 \bmod 2p^\alpha$$

事实上, 如果$\tilde{g}^d \equiv 1 \bmod 2p^\alpha$, 则显然有$\tilde{g}^d \equiv 1 \bmod p^\alpha$;
反之, 如果$\tilde{g}^d \equiv 1 \bmod p^\alpha$, 即$p^\alpha|\tilde{g}^d - 1$,, 而$2|\tilde{g}^d - 1$, 且$(2, p) = 1$, 所以$[2, p^\alpha] = 2p^\alpha$, 且$2p^\alpha|\tilde{g}^d - 1$, 即$\tilde{g}^d \equiv 1 \bmod 2p^\alpha$.

这样,我们就知道

$$\mathrm{ord}_{p^\alpha}(\tilde{g}) = \mathrm{ord}_{2p^\alpha}(\tilde{g})$$

$$\therefore \mathrm{ord}_{2p^\alpha}(\tilde{g}) = \varphi(p^\alpha)$$

$$\because \varphi(2p^\alpha) = \varphi(p^\alpha)$$

$$\therefore \mathrm{ord}_{2p^\alpha}(\tilde{g}) = \varphi(2p^\alpha)$$

即找到的这个$\tilde{g}$也是模$2p^\alpha$的原根.

整理我们得到的结论:

1. p为奇素数, 模p的原根必存在, 比如说是g';
2. 有这个模p的原根g'可以构造出一个模p的原根$\tilde{g}$满足: 是奇数, 且$\tilde{g}^{p-1} = 1 + rp (p \nmid r)$;
3. 这个模p的原根$\tilde{g}$也是模p^α的原根;
4. 这个模p的原根$\tilde{g}$也是模$2p^\alpha$的原根;

上述几点说明:

一方面模p的原根必定存在, 模p^α的原根必定存在, 模$2p^\alpha$的原根必定存在;

另一方面,只要知道了模p的任意一个原根, 就可以计算出来模p^α的原根和模$2p^\alpha$的原根.

定理

模m有原根的充要条件是$m=1$,或2,或4,或p^{α},或$2p^{\alpha}$.

在指数的性质中, 我们已经证明了模m有原根的必要条件:
模m有原根$\Longrightarrow m=1$,或2,或4,或p^{α},或$2p^{\alpha}$

所以,下面我们需要证明模m有原根的充分条件:
$m=1$,或2,或4,或p^{α},或$2p^{\alpha}\Longrightarrow$ 模m有原根.

事实上, 很容易检查:

- 如果$m=1$的话, 模1的原根就是1: $\varphi(m)=1, 1^1=1$;
- 如果$m=2$的话, 模2的原根就是1: $\varphi(m)=1, 1^1=1$;
- 如果$m=4$的话, 模4的原根就是3: $\varphi(m)=2, 3^1=3, 3^2=9\equiv 1 \bmod 4$;
- 前面业已说明$m=p^{\alpha}$时, 模m有原根; $m=2p^{\alpha}$时, 模m有原根.

说明: 上述求模m的原根问题最终归结为求模p的原根问题.

但是求模p的原根没有统一的方法, 只能对具体的素数p按照原根的定义逐个数去试.

3. 指标

我们前面看到，当g是模m的原根时(即g与模m互素，$\mathrm{ord}_m(g)=\varphi(m)$)，$g^1,g^2,\dots,g^{\varphi(m)-1},g^{\varphi(m)}$两两模$m$不同余，它们构成了一个模$m$的简化剩余系：$\{g^1,g^2,\dots,g^{\varphi(m)-1},g^{\varphi(m)}\}$.

换句话说，对于任意的与m互素的整数a(即a是模m的一个简化剩余)来说，在$1\sim\varphi(m)$之间存在唯一一个数r，使得$g^r\equiv a \bmod m$，我们就把这个数r称为以g为底的a对模m的指标，记作$\mathrm{ind}_g a$，或$\mathrm{ind} a$(注意到此时g必须为模m的原根)

比如，$g=5$是模$m=17$的一个原根，且

5^1	5^2	5^3	5^4	5^5	5^6	5^7	5^8	5^9	5^{10}	5^{11}	5^{12}	5^{13}	5^{14}	5^{15}	5^{16}
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

所以以5为底9对模17的指标就是10，以5为底4对模17的指标就是12...

定理

$g^s \equiv a \bmod m \Longrightarrow s \equiv \mathrm{ind}_g a \bmod \varphi(m)$

事实上,

$$\begin{aligned} \because g^s &\equiv a \bmod m \\ g^{\mathrm{ind}_g a} &\equiv a \bmod m \\ \therefore g^s &\equiv g^{\mathrm{ind}_g a} \bmod m \end{aligned}$$

不妨设$\mathrm{ind}_g a \leq s$ 由于$(g, m) = 1$,

$$\therefore g^{s - \mathrm{ind}_g a} \equiv 1 \bmod m$$

另外,由于g是原根, 所以g的指数是$\varphi(m)$, 从而$\varphi(m) | (s - \mathrm{ind}_g a)$,
即$s \equiv \mathrm{ind}_g a \bmod \varphi(m)$ $\diamond$

示例：已知6是模41的原根，以6为底的9对模41的指标为30，即$\mathrm{ind}_6 9 = 30$，求$x^5 \equiv 9 \bmod 41$的解：

设x_1是这个方程的解，则有$x_1^5 \equiv 9 \bmod 41$
即x_1^5与9在同一个模41的剩余类中，而9与41互素，所以x_1^5与41互素，从而x_1与41互素.

因为6是模41的原根，所以可设$x_1 = 6^{y_1} \bmod 41$，则$x_1^5 \equiv 9 \bmod 41$就等价于$6^{5y_1} \equiv 9 \bmod 41$，从而

$$5y_1 \equiv \mathrm{ind}_6 9 \bmod 40 (\because g^s \equiv a \bmod m \Longrightarrow s \equiv \mathrm{ind}_g a \bmod \varphi(m))$$

即

$$5y_1 \equiv 30 \bmod 40, \qquad i.e., \quad y_1 \equiv 6, 14, 22, 30, 38 \bmod 40$$

对应的有

$$x \equiv 6^6 \bmod 41, x \equiv 6^{14} \bmod 41, \ldots\ldots \qquad \diamond$$

定理

g为模m的原根, $a_1, \ldots, a_n$均与m互素, 则
$\text{ind}_g(a_1 \ldots a_n) \equiv \text{ind}_g a_1 + \ldots + \text{ind}_g a_n \mod \varphi(m)$

事实上,

$$\left.\begin{array}{r} g^{\text{ind}_g(a_1)} \equiv a_1 \mod m \\ g^{\text{ind}_g(a_2)} \equiv a_2 \mod m \\ \ldots\ldots \\ g^{\text{ind}_g(a_n)} \equiv a_n \mod m \end{array}\right\} \Longrightarrow (a_1 a_2 \ldots a_n) \equiv g^{\text{ind}_g(a_1)} g^{\text{ind}_g(a_2)} \ldots g^{\text{ind}_g(a_n)} \mod m$$

$$\Longrightarrow (a_1 a_2 \ldots a_n) \equiv g^{\text{ind}_g(a_1)+\text{ind}_g(a_2)+\ldots+\text{ind}_g(a_n)} \mod m$$

$$\Longrightarrow \text{ind}_g(a_1) + \text{ind}_g(a_2) + \ldots + \text{ind}_g(a_n) \equiv \text{ind}_g(a_1 a_2 \ldots a_n) \mod \varphi(m) \qquad \diamond$$

指数与指标间的联系:

假设g为模m的原根，a与m互素，其指标记为$\mathrm{ind}_g a$，a的指数记作$\mathrm{ord}_m(a)$，则:
事实上，我们知道$g^{\mathrm{ind}_g a} \equiv a \bmod m$,

$$
\begin{aligned}
\mathrm{ord}_m(a) &= \mathrm{ord}_m(g^{\mathrm{ind}_g a}) (\because r \equiv s \bmod m \Longrightarrow \mathrm{ord}_m r = \mathrm{ord}_m s) \\
&= \frac{\mathrm{ord}_m(g)}{(\mathrm{ord}_m(g), \mathrm{ind}_g a)} \\
&= \frac{\varphi(m)}{(\varphi(m), \mathrm{ind}_g a)} \\
& \quad i.e., \varphi(m) = (\varphi(m), \mathrm{ind}_g a) \cdot \mathrm{ord}_m(a)
\end{aligned}
$$

由此可见,

定理

a是模m的原根 $\Longleftrightarrow$ $(\varphi(m), \mathrm{ind}_g a) = 1$

定理

在模m的简化剩余系中, 指数等于e的整数个数是$\varphi(e)$.

假设a与m互素(即在一个简化剩余系中), 则

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

记$i = \mathrm{ind}_g a$(从而$1 \le i \le \varphi(m)$), 则有

$$e = \mathrm{ord}_m(a) \iff e = \frac{\varphi(m)}{(\varphi(m), i)}$$

这样指数等于e的a的个数就是使得$e = \frac{\varphi(m)}{(\varphi(m),i)}$成立的$i$的个数, 所以只需讨论式子

$$e = \frac{\varphi(m)}{(\varphi(m), i)} \iff (\varphi(m), i) = \frac{\varphi(m)}{e} \iff (\frac{i}{\frac{\varphi(m)}{e}}, \frac{\varphi(m)}{\frac{\varphi(m)}{e}}) = 1$$

$$i.e., (i', e) = 1(0 \le i' \le e)$$

这样使得$e = \frac{\varphi(m)}{(\varphi(m),i)}$成立的$i$的个数就是使得$(i', e) = 1(0 \le i' \le e)$的$i'$的个数, 即$\varphi(e)$. $\diamond$

根据这个结论, 模m的简化剩余系中指数为$\varphi(m)$的整数(即原根)的个数就是$\varphi(\varphi(m))$.

4. n次剩余

$m>1$, a与m互素, 如果同余式$x^n \equiv a \bmod m$有解, 则称a为模m的n次剩余. 否则, 称为模m的n次非剩余.

定理

设g是模m的一个原根, a与m互素, 则$x^n \equiv a \bmod m$有解 $\iff$ $(n,\varphi(m))|\text{ind}_g a$.
如果有解的话, 解数为$(n,\varphi(m)$.

证明: "$\Longrightarrow$:" 设同余式有解: $x \equiv x_0 \bmod m$, 即$x_0^n \equiv a \bmod m$, 也就是说x_0^n与a在同一个模m剩余类中,
而a与m互素, 所以x_0^n也与m互素,
从而x_0也与m互素, 即x_0是模m的一个简化剩余,
这样就存在一个整数u使得$x_0 \equiv g^u \bmod m$,
从而$g^{un} \equiv a \bmod m$, 从而$un \equiv \text{ind}_g a \bmod \varphi(m)$
也就是说, $ny \equiv \text{ind}_g a \bmod \varphi(m0$有解,
从而应该$(n,\varphi(m))|\text{ind}_g a$.

"$\Longleftarrow$:" 如果$(n,\varphi(m))|\text{ind}_g a$, 则一次同余式$ny \equiv \text{ind}_g a \bmod \varphi(m)$有解, 且解数为$(n,\varphi(m))$,

比如说$y \equiv u \bmod \varphi(m)$是一个解, 则$nu \equiv \text{ind}_g a \bmod \varphi(m)$, 即$nu = k\varphi(m) + \text{ind}_g a$, 从而$(g^u)^n = g^{un} = g^{k\varphi(m)+\text{ind}_g a} = g^{k\varphi(m)} g^{\text{ind}_g a} \equiv a \bmod m$, 即$x \equiv y^u \bmod m$就是原$n$次同余方程的一个解. $\diamond$

令$d=(n,\varphi(m))$,
由前我们看到, $x^n\equiv a \bmod m$有解$iff(n,\varphi(m))|\mathrm{ind}_g a$

下面来说明

$$(n,\varphi(m))|\mathrm{ind}_g a \iff \exists s\in\mathbb{Z}, s.t., \frac{\varphi(m)}{(n,\varphi(m))}=s\cdot\mathrm{ord}_m(a)$$

注意到我们总有结论$\varphi(m)=(\varphi(m),\mathrm{ind}_g a)\cdot\mathrm{ord}_m(a)$可以使用.

"$\Longrightarrow$:" 已知$(n,\varphi(m))|\mathrm{ind}_g a$, 即$d|\mathrm{ind}_g a$
设$n=k_n d, \varphi(m)=kd, \mathrm{ind}_g a=k_i d$, 则

$$\begin{aligned}\frac{\varphi(m)}{(n,\varphi(m))} &= \frac{(\varphi(m),\mathrm{ind}_g a)\cdot\mathrm{ord}_m(a)}{d}\\ &= \frac{(kd,k_i d)\cdot\mathrm{ord}_m(a)}{d}\\ &= \frac{(k,k_i)d\cdot\mathrm{ord}_m(a)}{d}=(k,k_i)\cdot\mathrm{ord}_m(a)\end{aligned}$$

s已找到.

"$\Longleftarrow$:" 反过来，已知

$$\exists s \in \mathbb{Z}, s.t., \frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \mathrm{ord}_m(a)$$

要证$d|\mathrm{ind}_g a$. 设$\varphi(m) = kd$，由

$$\frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \mathrm{ord}_m(a)$$

知

$$k = s \cdot \mathrm{ord}_m(a) \tag{1.1}$$

又由$\varphi(m) = (\varphi(m), \mathrm{ind}_g a) \cdot \mathrm{ord}_m(a)$知

$$kd = (\varphi(m), \mathrm{ind}_g a) \cdot \mathrm{ord}_m(a) \tag{1.2}$$

将(1.1)代入(1.2)知

$$(\varphi(m), \mathrm{ind}_g a) = sd$$

从而

$$d|\mathrm{ind}_g a \qquad \diamond$$

至此,我们证明了

$$(n,\varphi(m))|\mathrm{ind}_g a \iff \exists s\in\mathbb{Z}, s.t., \frac{\varphi(m)}{(n,\varphi(m))} = s\cdot \mathrm{ord}_m(a)$$

即

$$(n,\varphi(m))|\mathrm{ind}_g a \iff \mathrm{ord}_m(a)|\frac{\varphi(m)}{(n,\varphi(m))}$$

从而我们可以说:

$$\begin{aligned} x^n \equiv a \bmod m \text{ 有解} &\iff (n,\varphi(m))|\mathrm{ind}_g a \\ &\iff \mathrm{ord}_m(a)|\frac{\varphi(m)}{(n,\varphi(m))} \\ &\iff a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv 1 \bmod m \end{aligned}$$

这样我们就有结论: 模m原根存在, 则

$$a\text{是模}m\text{的}n\text{次剩余} \iff a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv 1 \bmod m. \qquad \diamond$$