Cnily03

信安数学基础考前复习

1）模重复平方计算法

对于大整数 m 和 n 计算$b^n \pmod m$，可采用模重复平方计算法。

2）费马小定理

若 p 为素数，$\gcd(a,p)=1$，则 $a^{p-1}\equiv 1 \pmod p$。

另一个形式：对于任意整数 a，有 $a^p \equiv a \pmod p$。

3）欧拉定理

若 $\gcd(a,m)=1$，则 $a^{\varphi(m)}\equiv 1 \pmod m$。

如果 m 为素数 p，那么$\varphi(m)=p-1$，就得到了费马小定理。

4）扩展欧几里得算法

下表以$a=240$，$b=46$为例演示了扩展欧几里得算法。所得的最大公因数是2，所得贝祖等式为$\gcd(240,46)=2=-9*240+47*46$。同时还有自验证等式$|23|*2=46$和$|-120|*2=240$。

序号 i	商 q_{i-1}	余数 r_i	s_i	t_i
0		240	1	0
1		46	0	1
2	240 ÷ 46 = 5	240 − 5 × 46 = 10	1 − 5 × 0 = 1	0 − 5 × 1 = −5
3	46 ÷ 10 = 4	46 − 4 × 10 = 6	0 − 4 × 1 = −4	1 − 4 × −5 = 21
4	10 ÷ 6 = 1	10 − 1 × 6 = 4	1 − 1 × −4 = 5	−5 − 1 × 21 = −26
5	6 ÷ 4 = 1	6 − 1 × 4 = 2	−4 − 1 × 5 = −9	21 − 1 × −26 = 47
6	4 ÷ 2 = 2	4 − 2 × 2 = 0	5 − 2 × −9 = 23	−26 − 2 × 47 = −120

这个过程也可以用初等变换表示。

$$\begin{pmatrix}240 & 46\\ 1 & 0\\ 0 & 1\end{pmatrix}\to\begin{pmatrix}10 & 46\\ 1 & 0\\ -5 & 1\end{pmatrix}\to\begin{pmatrix}10 & 6\\ 1 & -4\\ -5 & 21\end{pmatrix}\to\begin{pmatrix}4 & 6\\ 5 & -4\\ -26 & 21\end{pmatrix}\to\begin{pmatrix}4 & 2\\ 5 & -9\\ -26 & 47\end{pmatrix}$$ [3]

得到$-9\times 240+47\times 46=2$

5）中国剩余定理

对于一元线性同余方程组

$$\begin{cases} x &\equiv a_1 \pmod{n_1}\\ x &\equiv a_2 \pmod{n_2}\\ &\vdots\\ x &\equiv a_k \pmod{n_k}\end{cases}$$

其一般解法为：

1. 计算所有模数的积 n;
2. 对于第 i 个方程:
   a. 计算 $m_i=\frac{n}{n_i}$;
   b. 计算 m_i 在模 n_i 意义下的 逆元 m_i^{-1};
   c. 计算 $c_i=m_im_i^{-1}$（**不要对 n_i 取模**）。
3. 方程组在模 n 意义下的唯一解为：$x=\sum_{i=1}^{k}a_ic_i \pmod n$。

6）逆元求解

对于$ax\equiv 1 \pmod{n}$，x 为逆元，有模逆的充分必要条件是 a 与 n 互素，即$(a,\ n)=1$

有$as+nt=1$，使用扩展欧几里得求解出 s 即可。

7）线性同余方程求解（使用扩展欧几里得算法）

定理 1：线性同余方程 $ax\equiv b\pmod{n}$ 可以改写为如下线性不定方程：

$$ax+nk=b$$

其中 x 和 k 是未知数。这两个方程是等价的，有整数解的充要条件为 $\gcd(a,n)\mid b$。

应用扩展欧几里德算法可以求解该线性不定方程。根据定理 1，对于线性不定方程 $ax+nk=b$，可以先用扩展欧几里得算法求出一组 x_0,k_0，也就是 $ax_0+nk_0=\gcd(a,n)$，然后两边同时除以 $\gcd(a,n)$，再乘 b。就得到了方程

$$a\frac{b}{\gcd(a,n)}x_0+n\frac{b}{\gcd(a,n)}k_0=b$$

于是找到方程的一个解。

8）高次同余式求解

对于高次同余方程$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+ax+b\equiv 0\pmod{m}$.

① 将 m 分解为 $m=m_1m_2\ldots m_k$，化成方程组，m_i 数字小的话直接做。

② 更一般的解法，化成素数幂模同余方程组。将 m 分解为$m=\prod_p p^\alpha$ 的形式，然后化成$\bmod\ p^\alpha$ 的方程组，求解每一个方程，然后用中国剩余定理求解。

9）素数幂模同余方程的一般解法

对于$f(x)=\sum_{i=0}^{n}a_ix^i$，求解$f(x)\equiv 0\pmod{m}$的解，其中$m=p^\alpha$.

① 先进行化简，对于所有的系数a_i，变为模p^α的余数，所有a_i与 p 互素表示有解这一步可以保证所有的$a_i\nmid p^\alpha$，故这里只讨论$a_n\not\equiv 0\pmod{p}$的情况。

② 再从 $\bmod\ p$ 开始逐步升次进行验证筛选，例如求出 $\bmod\ p$ 下的解为

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

即$x=x_0+pt$. 然后对每个$x<p^2$进行验证，成立的话就得到 $\bmod\ p^2$ 下的解，如此递归。

减少验证的步骤可以考虑$f(x)$的导数$f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}$，对于当$m=p^{\alpha-1}$时，令$x_0$为方程$f(x)\equiv 0\pmod{p^{\alpha-1}}$的解，则：

1. 若 $f'(x_0)\not\equiv 0\pmod{p}$, 则存在整数 t 使得

$$x=x_0+p^{a-1}t \tag{3}$$

是方程

$$f(x)\equiv 0\pmod{p^a} \tag{4}$$

的解。

2. 若 $f'(x_0) \equiv 0 \pmod p$ 且 $f(x_0) \equiv 0 \pmod{p^a}$, 则对 $t = 0, 1, \ldots, p-1$, 由式 (3) 确定的 x 均为方程 (4) 的解。

3. 若 $f'(x_0) \equiv 0 \pmod p$ 且 $f(x_0) \not\equiv 0 \pmod{p^a}$, 则不能由式 (3) 构造方程 (4) 的解。

证明

我们假设式 (3) 是方程 (4) 的解，即

$$f(x_0 + p^{a-1}t) \equiv 0 \pmod{p^a}$$

整理后可得

$$f(x_0) + p^{a-1}tf'(x_0) \equiv 0 \pmod{p^a}$$

于是

$$tf'(x_0) \equiv -\frac{f(x_0)}{p^{a-1}} \pmod p \tag{5}$$

1. 若 $f'(x_0) \not\equiv 0 \pmod p$，则关于 t 的方程 (5) 有唯一解 t_0，代入式 (3) 可验证其为方程 (4) 的解。
2. 若 $f'(x_0) \equiv 0 \pmod p$ 且 $f(x_0) \equiv 0 \pmod{p^a}$，则任意 t 均能使方程 (5) 成立，代入式 (3) 可验证其均为方程 (4) 的解。
3. 若 $f'(x_0) \equiv 0 \pmod p$ 且 $f(x_0) \not\equiv 0 \pmod{p^a}$，则方程 (5) 无解，从而不能由式 (3) 构造方程 (4) 的解。

10）素数模同余式的解法

即讨论$\alpha = 1$的情况：

对于$f(x) = \sum_{i=0}^{n} a_i x^i$（$a_n \not\equiv 0 \pmod p$），求解$f(x) \equiv 0 \pmod p$的解.

上式的解数不会超过$\min(n, p)$.

① 先进行化简，对于所有的系数a_i，变为模p的余数，所有a_i与 p 互素表示有解。

② 如果$a_n \neq 1$，用扩展欧几里得算法求其模逆元，然后将首系数化为 1.

③ 如果$n > p$，再进行降次，对于$\bmod p$的方程，其解数不会超过p，由费马小定理可知，对于任意整数 x 和素数 p 都有$x^p - x \equiv 0 \pmod p$，所以可对$f(x)$做多项式带余除法，即$f(x) = g(x)(x^p - x) + r(x)$，然后$f(x) \equiv r(x) \equiv 0 \pmod p$.

显然，如果 p 整除$r(x)$的所有系数，即$r(x) \equiv 0 \pmod p$恒成立，方程有 p 个解。

④ 求出其中一个解$x \equiv a_1$，作多项式带余除法$f(x) = q(x)(x - a_1) + r(x)$，由于$r(x)$为确切的整数 r 且$\deg q(x) = n - 1$，$f(a_1) \equiv r(a_1) = r \equiv 0$，故寻求其它解，只需令

$$f_1(x) = q(x),$$

随后求解

$$f_1(x) \equiv 0 \pmod p$$

即可。如此循环便得到所有的解。

11）素数模同余式的解数

① 对于$n > p$，做多项式带余除法得到$f(x) = g(x)(x^p - x) + r(x)$，若

$$f(x) \equiv r(x) \equiv 0 \pmod p$$

恒成立，即 p 整除$r(x)$的所有系数，则解数为 p，解为$x \equiv 0, 1, \cdots, p-1$.

② 对于$n \le p$，做多项式带余除法得到$x^p - x = q(x) \cdot f(x) + r(x)$，则$f(x)$有 n 个解的充分必要条件为$r(x) \equiv 0$恒成立，即 p 整除$r(x)$的所有系数。

12）平方剩余（二次剩余）

若$x^2 \equiv a \pmod{m}$，$(a,\ m) = 1$有解，则称 a 为模 m 的平方剩余（二次剩余）。

显然，± 1为模任何数的平方剩余。

13）平方剩余判别式：欧拉判别式 （p 为奇素数）

欧拉判别条件，p 为奇素数，则有以下充分必要条件：

a 为平方剩余：$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

a 为平方剩余：$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

由以上可得推论，对于与 p 互素的两数 a_1、a_2，如果都为模 p 平方剩余或者平方非剩余，由$(a_1 \cdot a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}}$，得$a_1 \cdot a_2$必为模 p 的平方剩余。

14）平方剩余的个数（p 为奇素数）

由欧拉判别条件，考查$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$的解数，即考查$\dfrac{p-1}{2}$次同余方程

$$f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

的解数，由于$x^p - x = x(x^{p-1} - 1) = x\left(x^{\frac{p-1}{2}} + 1\right)\left(x^{\frac{p-1}{2}} - 1\right)$，即$x^p - x$被$f(x)$余数为 0，则解数等于次数，即有$\dfrac{p-1}{2}$个解，所以：

p 的简化剩余系中，平方剩余有$\dfrac{p-1}{2}$个，非平方剩余有$\dfrac{p-1}{2}$个，

且当$x = 1,\ 2,\ \cdots,\ \dfrac{p-1}{2}$时，$x^2 \pmod{p}$两两同余，即恰好遍历$\dfrac{p-1}{2}$个平方剩余。

15）勒让德（Legendre）符号

定义$\left(\dfrac{a}{p}\right) = \begin{cases} 1, & \exists x \in \mathbb{Z},\ x^2 \equiv a \pmod{p} \\ -1, & \nexists x \in \mathbb{Z},\ x^2 \equiv a \pmod{p} \\ 0, & p \mid a \end{cases}$.

由欧拉判别条件易得，当 p 为**奇素数**时，$\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

当 p 为奇素数时，有：

① $\left(\dfrac{1}{p}\right) = 1$.

② $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$.

③ 周期性：$\left(\frac{a}{p}\right)=\left(\frac{a+p}{p}\right)=\left(\frac{a \bmod p}{p}\right)$，即若$a\equiv b \pmod p$则$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

④ 完全可乘性：$\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

⑤ 若 a 与 p 互素，由欧拉定理得$\left(\frac{a^2}{p}\right)\equiv a^{p-1}\equiv 1 \pmod p$.

16）高斯引理（p 为奇素数）

对于奇素数 p，若 a 与 p 互素，则令 m 为集合$\mathcal{A}=\left\{ax_i \mid x_i=1,\ 2,\ \cdots,\ \frac{p-1}{2}\right\}$中模 p 的最小正剩余大于$\frac{p}{2}$的个数，即

$$m=\operatorname{card}\left(\left\{x \mid x\in\mathcal{A}\wedge(\exists y)\left(x\equiv y \pmod p\wedge\frac{p}{2}<y<p\right)\right\}\right).$$

则有$\left(\frac{a}{p}\right)=(-1)^m$.

当 p 为奇素数时，有：

① $\left(\frac{2}{p}\right)=(-1)^m$，$m=k$当$p=4k\pm1$，即$m=\frac{p^2-1}{8}$.

② 若$(a,\ 2p)=1$，则$\left(\frac{a}{p}\right)=(-1)^{T(a,\ p)}$, $T(a,\ p)=\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{a\cdot k}{p}\right\rfloor$.

17）二次互反律

对于互素（不同的）**奇素数** p 和 q，有$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$.

18）雅可比（Jacobi）符号

对于**奇素数**的乘积$m=p_1p_2\cdots p_r$，与勒让德符号类似，定义

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

当$\left(\frac{a}{m}\right)=-1$时$x\equiv a \pmod m$无解，但当$\left(\frac{a}{m}\right)=1$时**不能充分给出有解**。

类似地，当 m 为奇数时有：

① $\left(\frac{1}{m}\right)=1$.

② $\left(\frac{-1}{m}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & m\equiv 1 \pmod 4\\ -1, & m\equiv 3 \pmod 4\end{cases}$.

③ （m 为**正奇数**）$\left(\frac{a}{m}\right)=\left(\frac{a+m}{m}\right)$，即若$a\equiv b \pmod m$则$\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$.

④ （m 为**正奇数**）$\left(\frac{a\cdot b}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.

⑤ （m 为**正奇数**）若 a 与 m 互素，则$\left(\dfrac{a^2}{m}\right)=1$.

⑥ $\left(\dfrac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

⑦ 二次互反律：对于不同的奇数 m, n 有$\left(\dfrac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\dfrac{m}{n}\right)$.

19）求解二次同余式：模 p 平方根（$p=4k+3$ 型）

① 对于素数$p\equiv 3 \pmod 4$，若同余式$x^2\equiv a \pmod p$有解，则解为

$$x\equiv\pm a^{\frac{q+1}{2}}\equiv\pm a^{\frac{p+1}{4}} \pmod p,\ q=\frac{p-1}{2}.$$

因为$\left(\pm a^{\frac{q+1}{2}}\right)^2\equiv a^q\cdot a\equiv a \pmod p$，其中$a^q\equiv a^{\frac{p-1}{2}}\equiv 1 \pmod p$.

② 对于$p\equiv q\equiv 3 \pmod 4$，有$\left(\dfrac{a}{p}\right)=\left(\dfrac{a}{q}\right)=1$，则同余式$x^2\equiv a \pmod{p\cdot q}$有解，

对于整数 s, t 满足$s\cdot p+q\cdot t=1$，同余式解为

$$x\equiv\pm\left(a^{\frac{p+1}{4}} \bmod p\right)\cdot t\cdot q\pm\left(a^{\frac{q+1}{4}} \bmod q\right)\cdot s\cdot p \pmod{p\cdot q}$$

20）求解二次同余式：模 p 平方根（p 为任意奇素数）

21）求解二次同余式：模 m 平方根（下文中 p 为奇素数）

对$x^2\equiv a \pmod m$求解，将 m 进行质因数分解$m=2^\delta\prod\limits_p p^\alpha$，化成同余式组。

① $x^2\equiv a \pmod{p^\alpha}$有解的充分必要条件是$x^2\equiv a \pmod p$有解。因为对于二次同余方程$f(x)=x^2-a\equiv 0 \pmod{p^\alpha}$，$f'(x)=2x\not\equiv 0 \pmod p$，故有高次同余方程式的相关内容可知，当$\alpha=1$的解$x_1$唯一确定一个解$x_\alpha$，而二次剩余模 p 时有两个解，故最终模p^α有两个解。

② $x^2\equiv a \pmod{2^\delta}$有解的必要条件为$\begin{cases} a\equiv 1 \pmod 4, & \delta=2 \\ a\equiv 1 \pmod 8, & \delta\geq 3 \end{cases}$.

22）$x^2+y^2=p$

$x^2+y^2=p$有整数解的充分必要条件是$p=2$或$\left(\dfrac{-1}{p}\right)=1$即$p=4k+1$.

23）指数、原根

若 a 与 m **互素**，则使得$a^e\equiv 1 \pmod m$满足的最小整数 e 称为 a 对模 m 的指数，记作$\mathrm{ord}_m(a)$，当指数$\mathrm{ord}_m(a)=\varphi(m)$时，$a$ 称为对模 m 的原根。

显然，根据欧拉定理，有$a^{\varphi(m)}\equiv 1 \pmod m$成立。

24）指数的基本性质

① 任何使$a^d\equiv 1 \pmod m$满足的 d 都是指数$e=\mathrm{ord}_m(a)$的倍数，即$\mathrm{ord}_m(a)\mid d$.

特别地，有$\mathrm{ord}_m(a)\mid\varphi(m)$.

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

③ 若 a 对 m 的模逆元为a^{-1}则$\mathrm{ord}_m(a)=\mathrm{ord}_m(a^{-1})$.

④ 若$0\le n<\mathrm{ord}_m(a)$，则a^n模 m 两两不同余。

特别地，当$\mathrm{ord}_m(a)=\varphi(m)$，即 a 为原根时，a^n构成模 m 的简化剩余系。

⑤ 易证$d\equiv k\ (\mathrm{mod}\ \mathrm{ord}_m(a))\ \Leftrightarrow\ a^d\equiv a^k\ \ (\mathrm{mod}\ m)$.

⑥ $\mathrm{ord}_m(a^d)=\dfrac{\mathrm{ord}_m(a)}{(d,\ \mathrm{ord}_m(a))}$.

特别地，当 a 为其中一个原根 g 时，$\mathrm{ord}_m(g^d)=\dfrac{\varphi(m)}{(d,\ \varphi(m))}=\varphi(m)$. 则$g^d$为原根当且仅当$(d,\ \varphi(m))=1$.

⑦ $a^{\mathrm{ord}_m(a)}\equiv 1\ (\mathrm{mod}\ m),\ m>1$，$k\mid \mathrm{ord}_m(a)$且$\mathrm{ord}_m(a^d)=k,\ 1\le d\le \mathrm{ord}_m(a)$，则$\dfrac{\mathrm{ord}_m(a)}{k}\mid d$且这样的 d 有$\varphi(k)$个。

⑧ g 为模 m 的其中一个原根，则模 m 共有$\varphi(\varphi(m))$个原根g^d满足$(d,\ \varphi(m))=1$.

⑨ $\mathrm{ord}_m(a\cdot b)=\mathrm{ord}_m(a)\cdot \mathrm{ord}_m(b)$.

$n\mid m\ \Rightarrow\ \mathrm{ord}_n(a)\mid \mathrm{ord}_m(a)$.

⑩ $(m,\ n)=1\ \Rightarrow\ \mathrm{ord}_{mn}(a)=[\mathrm{ord}_{\mathrm{m}}(a),\ \mathrm{ord}_{\mathrm{n}}(a)]=[\mathrm{ord}_{\mathrm{m}}(a_1),\ \mathrm{ord}_{\mathrm{n}}(a_2)]$，其中$a_1$、$a_2$与 mn 互素。

更一般地，对于 m 的简化剩余系的每一个a_i，存在整数 a 使得

$$\mathrm{ord}_m(a)=[\mathrm{ord}_m(a_1),\ \mathrm{ord}_m(a_2),\ \cdots,\ \mathrm{ord}_m(a_{\varphi(m)})]$$

成立。

25）求解模 p 原根（p 为奇素数）

对于$a^{\varphi(p)}\equiv a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$，显然共有$\varphi(\varphi(p))=\varphi(p-1)$个原根。

① 当 p 足够小时，通过枚举法进行验证找出其中一个原根 g，然后通过构造g^d满足$(d,\ p-1)=1$得到所有原根。

② 找到$p-1$的所有质因数q_i，求所有的$n=\dfrac{p-1}{q_i}$，对于每一个$g<p$，如果对于所有 n 都有$g^n\not\equiv 1\ (\mathrm{mod}\ p)$，则 g 为原根，随后进行构造。

26）求解模 p^α 原根（p 为奇素数）

① 先找到模 p 的原根g_i.

② 找到一个g_i使得g_i或g_i+p为模p^2的原根，找到的原根记为 g.

③ 对于更高次α，找到的模p^2的原根 g 为模p^α的原根。

④ 通过构造g^d满足$(d,\ \varphi(p^\alpha))=1$找到所有原根。

27）求解模 $2p^\alpha$ 原根（p 为奇素数）

① 先找到模p^α的原根g_i.

② 找到一个g_i使得g_i或g_i+p^α为奇数，则找到的奇数为模$2p^\alpha$的一个原根。

③ 通过构造g^d满足$(d,\ \varphi(2p^\alpha))=1$找到所有原根。

28）模2^δ的指数

① $\operatorname{ord}_{2^\delta}(a)\le\varphi(2^\delta)/2=2^{\delta-1}$.

② $\operatorname{ord}_{2^\delta}(5)=2^{\delta-1}$.

29）模 m 原根（下文中 p 为奇素数）

对于$a^{\varphi(m)}\equiv1\ (\operatorname{mod} m)$，有原根的充分必要条件是当$m=2$，4，$p^\alpha$，$2p^\alpha$.

① 对于$m=2$，4或足够小时，通过枚举法得出原根。

② 否则，对于$m=p^\alpha$，根据模p^α的方法找出原根。

③ 否则，对于$m=2p^\alpha$，根据模$2p^\alpha$的方法找出原根。

30）指标

若 g 为模 m 的一个原根，易证存在唯一的满足$1\le r\le\varphi(m)$的整数 r，使得$g^r\equiv a\ (\operatorname{mod} m)$成立，此时 r 称为以 g 为底的 a 对模 m 的一个指标，记作$r=\operatorname{ind}_g a$.

① 若 a 与 m 互素，$g^s\equiv a\ (\operatorname{mod} m)$，则$s\equiv r\equiv\operatorname{ind}_g a\ (\operatorname{mod}\varphi(m))$.

特别地，$\operatorname{ind}_g 1\equiv0\ (\operatorname{mod}\varphi(m))$.

② 若 a_i与 m 互素，则$\operatorname{ind}_g\prod\limits_i a_i=\sum\limits_i\operatorname{ind}_g a_i\ \ (\operatorname{mod}\varphi(m))$.

31）n 次同余式（a 与 m 互素）

$x^n\equiv a\ (\operatorname{mod} m)$有解的充分必要条件是$(n,\ \varphi(m))\mid\operatorname{ind}a$.

此时，也有$\dfrac{\varphi(m)}{d}\operatorname{ind}a\equiv0\ (\operatorname{mod}\varphi(m))\ \Leftrightarrow\ a^{\frac{\varphi(m)}{d}}\equiv1\ (\operatorname{mod} m)$, $d=(n,\ \varphi(m))$为a是模 m 的 n 次剩余的充分必要条件。

32）指数为 e 时的 a

对于$a^e\equiv1\ (\operatorname{mod} m)$的更一般的情况：

① $\operatorname{ord}_m(a)=e=\dfrac{\varphi(m)}{(\operatorname{ind}a,\ \varphi(m))}$.

② 在模 m 的简化剩余系中，a 的个数为$\varphi(e)$.

特别地，当 a 为原根时，原根个数为$\varphi(\varphi(m))$.