初等数论
第一章至第五章复习

中山大学　计算机学院

8. 第一章小结

1. 如果c整除a，c整除b，那么c也能够整除$sa+tb$, 其中s,t为任意整数.
2. 合数n的最小正因子p一定是素数，且$p \leq \sqrt{n}$.
3. 素数一定有无穷多个.
4. 如果$a,b \in \mathbb{Z}^+, b|a$, 那么$(a,b)=b$.
5. $a=bq+c \Longrightarrow (a,b)=(b,c)$.
6. 如果$c|(ab)$, 且$(a,c)=1$, 则$c|b$. 特别地, 如果素数$p|(ab)$, 则要么$p|a$, 要么$p|b$.
7. 使用辗转相除法计算最大公因数.
8. 存在整数s,t使得$s \cdot a + t \cdot b = (a,b)$, 使用广义欧几里得除法可以计算整数$s$和$t$.
9. $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{|d|}$, 其中$d$是$a$和$b$的公因数. 特别地, $(\frac{x}{(x,y)}, \frac{y}{(x,y)}) = 1$.
10. $(a,c)=1 \Longrightarrow (ab,c)=(b,c)$.
11. $(a,b)=(a,ax+b)=(a+bx,b)$, 其中x是整数.
12. 算术基本定理, 整数的标准分解式.
13. $[a,b] = \dfrac{ab}{(a,b)}$
14. 一次不定方程解的存在性及表示，使用广义欧几里得除法求解一次不定方程.

1. 模m同余相等与整数相等的相似性.
2. $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d,m)=1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m.$
3. $\left.\begin{array}{c} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \end{array}\right\} \Longrightarrow a \equiv b \bmod [m_1, m_2]$
4. 完全(简化)剩余系的写法.
5. 整数a与正整数m互素, 则当x取遍模m的简化(完全)剩余系, 相应的数ax也构成模m的简化(完全)剩余系.
6. 设m_1与m_2互素, 如果x_1取遍模m_1的简化(完全)剩余系, x_2取遍模m_2的简化(完全)剩余系, 则$m_2x_1 + m_1x_2$取遍模m_1m_2简化(完全)剩余系.
7. Wilson定理及其证明思想.
8. $(m,n)=1 \Longrightarrow \varphi(mn)=\varphi(m)\varphi(n)$, 且$\varphi(p^\alpha)=p^\alpha - p^{\alpha-1}$.
9. Euler定理: 如果m是正整数, 且整数a与m互素, 则$a^{\varphi(m)} \equiv 1 \bmod m$.
10. Fermat小定理: 如果p是素数, a是整数, 则$a^p \equiv a \bmod p$.
11. 平方乘算法（模重复平方计算法）.

第三章小结

1. 一次同余方程$ax \equiv b \bmod m$的解法.
   计算$d=(a,m)$; 断是否$d\,|\,b$; 计算$\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$,和使得$s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$的$s$; 全部的解
   $$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \bmod m, \quad (k = 0, 1, 2, \cdots, d-1).$$
2. 利用中国剩余定理求解一次同余方程组.
   $$x \equiv M_1'M_1b_1 + M_2'M_2b_2 + \ldots + M_k'M_kb_k \bmod M.$$
3. 利用中国剩余定理进行模指数运算.
4. 高次同余方程的等价变形.
   - 如果$(a,m)=1$, 则同余方程$f(x) \equiv 0 \bmod m$与$af(x) \equiv 0 \bmod m$等价
   - 模m的同余恒等式$x^p - x \equiv 0 \bmod p$.
   - 多项式的欧几里德除法
5. 一般高次同余方程$f(x) \equiv 0 \bmod m$的求解思路.
   - 分解m为两两互素的整数之积$m_1, m_2, \ldots, m_k$;
   - 分别求解$f(x) \equiv 0 \bmod m_i$;
   - 构造一次同余方程组, 利用中国剩余定理求解.
6. 模为素数幂的同余方程$f(x) \equiv 0 \bmod p^\alpha$的求解思路.
7. 模为素数p的同余方程$f(x) \equiv 0 \bmod p$.

6. 模为素数幂的同余方程$f(x) \equiv 0 \bmod p^\alpha$的求解思路.
   - 设法求解$f(x) \equiv 0 \bmod p^{\alpha-1}$.
   - 最终归结为模为素数p的同余方程$f(x) \equiv 0 \bmod p$的求解.
   - 如果c是$f(x) \equiv 0 \bmod p^{\alpha-1}$的一个解, 则可以通过求解关于$k$的一次同余方程

     $$f'(c) \cdot k \equiv \frac{-f(c)}{p^{\alpha-1}} \bmod p$$

     导出$f(x) \equiv 0 \bmod p^\alpha$对应于$c$的解.
   - 如果关于k的一次同余方程无解; 则没有对应于c的解.
     如果关于k的一次同余方程有唯一解k_1, 则对应于c的解为

     $$x \equiv c + p^{\alpha-1}k_1 \bmod p^\alpha.$$

     如果关于k的一次同余方程有p个解, 则对应于c的解为

     $$x \equiv c \bmod p^\alpha, x \equiv c + p^{\alpha-1} \bmod p^\alpha, \ldots, x \equiv c + p^{\alpha-1} \cdot (p-1) \bmod p^\alpha.$$

7. 模为素数p的同余方程$f(x) \equiv 0 \bmod p$.

第三章小结

7. 模为素数p的同余方程$f(x) \equiv 0 \bmod p$.
    - 任意模p的同余方程一定与一个次数不超过$p-1$的模p的同余方程等价;
    - 这个模p的次数为$n \leq p-1$的同余方程的解数至多为它的次数n;
    - 这个模p的次数为$n \leq p-1$的的同余方程的解数为n的充要条件为$x^p - x$被它除后所得余式的系数都是p的倍数.
    - "直接验证"和"因式分解"是求解模素数p的高次同余方程的两种一般解法.
    - 模p的二次同余方程求解有迭代法.
    - 原根指标法求解.

第四章小结

1. 二次剩余的基本概念.
   - 设素数$p > 2$, 如果$x^2 \equiv a \bmod p$有解，则称a是一个模p的平方剩余(二次剩余).否则，称a是一个模p的平方非剩余(二次非剩余).
   - 如果a是模p二次剩余, 那么$x^2 \equiv a \bmod p$的解数为2.
2. 列举模p的二次剩余.
   - 在模p的简化剩余系中, 恰有$\frac{p-1}{2}$个模p二次剩余, 恰有$\frac{p-1}{2}$个模p二次非剩余;
   - $\{1^2 \bmod p, 2^2 \bmod p, 3^2 \bmod p, \dots, \left(\frac{p-1}{2}\right)^2 \bmod p\}$是模$p$的全部二次剩余.
3. 判定模p的二次剩余.
   - a是模p的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$;
   - a是模p的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \bmod p$.
4. 勒让德符号及其基本性质.
5. 高斯引理及二次互反律.
6. 雅可比符号及其基本性质.
7. 计算模奇素数p的a的平方根.
8. 计算模合数m的a的平方根.

第四章小结

4. 勒让德符号及其基本性质.
    - $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.
    - $(\frac{a+kp}{p}) = (\frac{a}{p})$, 其中$k$为整数.
    - $a \equiv b \bmod p \Longrightarrow (\frac{a}{p}) = (\frac{b}{p})$
    - $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$,
    - $(a, p) = 1 \Longrightarrow (\frac{a^2}{p}) = 1$.
5. 高斯引理及二次互反律.
    - 设p是奇素数, a是整数, 且$(a, p) = 1$. 如果在整数$a \cdot 1, a \cdot 2, \ldots, a \cdot \frac{p-1}{2}$中模$p$后大于$\frac{p}{2}$的个数是$m$, 则$\left(\frac{a}{p}\right) = (-1)^m$.
    - $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, 其中$p \neq q$均为奇素数.
    - $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$和$\left(\frac{3}{p}\right)$.
6. 雅可比符号及其基本性质.
7. 计算模奇素数p的a的平方根.
8. 计算模合数m的a的平方根.

6. 雅可比符号及其基本性质.
   - $\left(\frac{a}{m}\right) \triangleq \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots\cdots \left(\frac{a}{p_s}\right)$, 其中$m = p_1p_2 \dots p_s$是奇素数$p_i$的乘积.
   - 如果$(m, n) > 1$, 则$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$.
   - $\left(\frac{a+km}{m}\right) = \left(\frac{a}{m}\right)$, 其中$k$为整数.
   - $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
   - 如果$(a, m) = 1$, 则$\left(\frac{a^2}{m}\right) = 1$.
   - $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$, $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
   - 雅克比符号的互反律$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$, 其中$m, n$都是奇素数的乘积, 且$(m, n) = 1$.
   - 雅克比符号$\left(\frac{n}{m}\right) = 1$不表示二次同余方程$x^2 \equiv n \bmod m$一定有解, 没有欧拉判别条件, 也不存在类似勒让德符号的Gauss引理, 但是可以用来判断模m的二次同余方程无解.
7. 计算模奇素数p的a的平方根.
8. 计算模合数m的a的平方根.

7. 计算模奇素数p的a的平方根.
   - 特别地，如果$p=4k+3$，k为正整数，则模p的a的平方根为$x\equiv \pm a^{\frac{p+1}{4}} \bmod p$.
   - 一般地，将$p-1$写成是2的幂和一个奇数的乘积形式，即$p-1=2^t\cdot s$，其中$s\geq 1$.
   - 首先应用欧拉定理和欧拉判别条件，较容易求出同余方程
$$y^{2^{t-1}}\equiv 1 \bmod p$$
的一个形如$a^{-1}x_{t-1}^2$的解. 如果$t=1$，则$x_0 \bmod p$就是原二次同余式的一个解.
   - 如果$t>1$，在$a^{-1}x_{t-1}^2$基础上，能够比较容易地求出同余方程
$$y^{2^{t-2}}\equiv 1 \bmod p$$
的一个形如$a^{-1}x_{t-2}^2$的解. 如果$t=2$，则求解工作可以结束.
   - 如果$t>2$，在$a^{-1}x_{t-2}^2$基础上，继续类似的求解运算，即求出同余方程
$$y^{2^{t-3}}\equiv 1 \bmod p$$
的一个形如$a^{-1}x_{t-3}^2$的解;

7. 计算模奇素数p的a的平方根.
   - 一般地, 如果求出了同余方程
   $$y^{2^{t-k}} \equiv 1 \bmod p$$
   的一个形如$a^{-1}x_{t-k}^2$的解, 且$t > k$, 可以类似的求出同余方程
   $$y^{2^{t-k-1}} \equiv 1 \bmod p$$
   的一个形如$a^{-1}x_{t-k-1}^2$的解.
   - 继续下去, 一定能求出同余方程
   $$y^2 \equiv 1 \bmod p$$
   的一个形如$a^{-1}x_1^2$的解, 从而最终能够比较容易地求出
   $$y \equiv 1 \bmod p$$
   的一个形如$a^{-1}x_0^2$的解.
   - 完成原二次同余方程的求解, 即一个解$x_0 \bmod p$, 另一个是$-x_0 \bmod p$.

第四章小结

7. 计算模奇素数p的a的平方根.
   - 具体求解时，先任意选取模p的一个平方非剩余n，计算$b=(n^s \bmod p)$，从而有

$$b^{2^t}=(n^s)^{2^t}=n^{s\cdot 2^t}=n^{p-1}\equiv 1 \bmod p$$

$$b^{2^{t-1}}=(n^s)^{2^{t-1}}=n^{s\cdot 2^{t-1}}=n^{\frac{p-1}{2}}\equiv -1 \bmod p$$

   给定$p-1=2^t\cdot s$，同余方程$y^{2^{t-1}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-1}^2$ 的解是

$$x_{t-1}=(a^{\frac{s+1}{2}} \bmod p).$$

   - case 1: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv 1 \bmod p$，令$x_{t-2}=x_{t-1}$，则$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}}\equiv 1 \bmod p$的解.
   case 2: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv -1 \bmod p$，令$x_{t-2}=x_{t-1}\cdot b^{2^0}=x_{t-1}\cdot b$，则$a^{-1}x_{t-2}^2$是
   同余方程$y^{2^{t-2}}\equiv 1 \bmod p$的解.

7. 计算模奇素数p的a的平方根.
   - case 1: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$, 令$x_{t-3} = x_{t-2}$, 则$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.
     case 2: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p$, 令$x_{t-3} = x_{t-2} \cdot b^{2^1}$, 则$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.
   - case 1: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$, 令$x_{t-4} = x_{t-3}$, 则$a^{-1}x_{t-4}^2$是同余方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.
     case 2: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p$, 令$x_{t-4} = x_{t-3} \cdot b^{2^2}$, 则$a^{-1}x_{t-4}^2$是同余方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.
   - $\vdots$
   - case 1: 如果$(a^{-1}x_1^2)^{2^0} \equiv 1 \bmod p$, 令$x_0 = x_1$, 则$a^{-1}x_0^2$是同余方程$y^{2^0} \equiv y \equiv 1 \bmod p$的解.
     case 2: 如果$(a^{-1}x_1^2)^{2^0} \equiv -1 \bmod p$, 令$x_0 = x_1 \cdot b^{2^{t-2}}$, 则$a^{-1}x_0^2$是同余方程$y^{2^0} \equiv y \equiv 1 \bmod p$的解.

第四章小结

8. 计算模合数m的a的平方根.
   - 同余方程$x^2 \equiv a \bmod p^\alpha$有解当且仅当$a$为模$p$的二次剩余，且有解时解数为2.
   - 同余方程$x^2 \equiv a \bmod 2^\delta$的判定与求解

     如果$\delta = 2$，有解当且仅当$a \equiv 1 \bmod 4$，且有解时解数为2.
     如果$\delta \geq 3$，有解当且仅当$a \equiv 1 \bmod 8$，且有解时解数为4.
     当$\delta = 3$时，$2^\delta = 8$：通过检查发现同余方程$x^2 \equiv 1 \bmod 8$的解有4个，它们是$x \equiv \pm 1, \pm 5 \bmod 8$. 具有这种形式的所有整数可以表示为

     $$\pm(1 + t_3 \cdot 2^2),$$

     其中$t_3 = 0, \pm 1, \pm 2 \ldots$.
     当$\delta = 4$时，$2^\delta = 16$：设c是$x^2 \equiv a \bmod 16$的解，则c也是$x^2 \equiv 1 \bmod 8$的解. 将$c = \pm(1 + t_3 \cdot 2^2)$代入$x^2 \equiv a \bmod 16$，从而确定出$t_3$的取值

     $$t_3 \equiv \frac{a-1}{8} \bmod 2.$$

     这样，方程$x^2 \equiv a \bmod 16$的解(具有这种形式的所有整数)就是：

     $$\pm(1 + t_3 \cdot 2^2 + t_4 \cdot 2^3) = \pm(x_4 + t_4 \cdot 2^3)$$

     其中$t_3 = 0, 1$，且$t_4 = 0, \pm 1, \pm 2 \ldots$，而$x_4 = 1 + t_3 \cdot 2^2$.

8. 计算模合数m的a的平方根.
   - 同余方程$x^2 \equiv a \bmod p^\alpha$有解当且仅当$a$为模$p$的二次剩余，且有解时解数为2.
   - 同余方程$x^2 \equiv a \bmod 2^\delta$的判定与求解
     当$\delta = 5$时，$2^\delta = 32$：设c是方程$x^2 \equiv a \bmod 32$的解，则c也是$x^2 \equiv a \bmod 16$的解，将$c = \pm(x_4 + t_4 \cdot 2^3)$代入同余方程$x^2 \equiv a \bmod 32$，从而确定出$t_4$的取值
     $$t_4 \equiv \frac{a - x_4^2}{2^4} \bmod 2.$$
     这样，方程$x^2 \equiv a \bmod 32$的解(具有这种形式的所有整数)就是:
     $$\pm(x_4 + t_4 \cdot 2^3 + t_5 \cdot 2^4) = \pm(x_5 + t_5 \cdot 2^4)$$
     其中$t_4 = 0, 1$，且$t_5 = 0, \pm 1, \pm 2 \ldots$，而$x_5 = x_4 + t_4 \cdot 2^3$.
   - 上述过程继续下去，最终求出$x^2 \equiv a \bmod 2^\delta$的解. 它们对模$2^\delta$为4个解，记为
     $$x_\delta = \pm(x_{\delta-1} + t_{\delta-1} \cdot 2^{\delta-1}) \bmod 2^\delta,$$
     其中$t_{\delta-1} = 0, 1$.

定义（指数与原根）

设m是大于1的整数，a与m互素. 使得$a^e \equiv 1 \bmod m$的最小正整数e被称为a对模m的**指数(或阶)**，记作$\mathrm{ord}_m(a)$. 如果$\mathrm{ord}_m(a) = \varphi(m)$，则称$a$为模$m$的**原根**. 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.

1. 整数d使得$a^d \equiv 1 \bmod m$当且仅当$\mathrm{ord}_m(a) \mid d$.
2. 如果$n \mid m$，则$\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.
3. 如果$ab \equiv 1 \bmod m$，则$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.
4. 如果a是模m的原根，则$\{a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}\}$构成模$m$的一个简化剩余系.
5. $a^k \equiv a^l \bmod m$当且仅当$k \equiv l \bmod \mathrm{ord}_m(a)$
6. $\mathrm{ord}_m(a^k) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)}$，其中$k$是非负整数.
7. 如果模m有原根，则模m的原根的个数为$\varphi(\varphi(m))$.

第五章小结

定理

设m是大于1的整数，a, b均与m互素.

1. 存在$c = a^s b^t$使得$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$，其中$s = \frac{\mathrm{ord}_m(a)}{u}$，$t = \frac{\mathrm{ord}_m(b)}{v}$，而$u, v$是使得

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

都成立的一对整数.

2. 如果$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$，则$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.
3. 一般地，存在整数g使得$\mathrm{ord}_m(g) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \ldots, \mathrm{ord}_m(a_k)]$，其中$2 \leq k \leq \varphi(m)$.

定理

设m, n互素. $(a_1, m) = (a_2, n) = 1$. 存在整数a使得$(a, mn) = 1$且$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2)]$，且$a$可以通过中国剩余定理计算得到. 如果$a_1 = a_2$，则$\mathrm{ord}_{mn}(a_1) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_1)]$.

第五章小结

定理

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

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

定理

模m有原根的充要条件是$m = 1$,或2,或4,或p^α,或$2p^\alpha$, 其中p为奇素数, $\alpha \geq 1$.

1. p为奇素数, 模p的原根必存在, 例如是g', 它可以通过对$2, 3, 4, \ldots$依次验证得到.
2. $g = g', g = g' + p, g = g' + 2p, \ldots, g = g' + (p-1)p$都是模$p$的原根, 它们当中至少有两个是奇数, 且只有一个不满足条件$g^{p-1} = 1 + rp, p \nmid r$, 其余都满足.
3. 任意一个满足$g^{p-1} = 1 + rp, p \nmid r$的模$p$的原根$\tilde{g}$都是模$p^\alpha$的一个原根.
4. 任意一个满足$g^{p-1} = 1 + rp, p \nmid r$的是奇数的模$p$的原根$\tilde{g}$都是模$2p^\alpha$的一个原根.
5. 在实际计算过程中, 可以先确定g^{p-1}模p^2的余数, 然后再判断是否有$p \nmid r$.

第五章小结

1. 指标的基本概念及性质
   - 对于任意的与m互素的整数a，在$0\sim(\varphi(m)-1)$之间存在唯一的整数r，使得$g^r\equiv a \bmod m$. 把这个整数r称为以g为底的a对模m的指标，记作$\mathrm{ind}_g a$.
   - 如果$g^s\equiv a \bmod m$，则$s\equiv \mathrm{ind}_g a \bmod \varphi(m)$.
   - $\mathrm{ind}_g(a_1\ldots a_n)\equiv \mathrm{ind}_g a_1+\ldots+\mathrm{ind}_g a_n \bmod \varphi(m)$.
2. 指标与指数
   - $\varphi(m)=(\varphi(m),\mathrm{ind}_g a)\cdot \mathrm{ord}_m(a)$.
   - g是模m原根，a是模m的原根当且仅当$(\varphi(m),\mathrm{ind}_g a)=1$.
   - 如果模m有原根，则在模m的简化剩余系中，指数为e的整数个数是$\varphi(e)$.
3. 原根指标法解简单高次同余方程$x^n\equiv a \bmod m$
   - 高次同余方程$x^n\equiv a \bmod m$被转化为一次同余方程$ny\equiv \mathrm{ind}_g a \bmod \varphi(m)$的求解问题，其中$g$是模$m$原根.
   - 同余方程$x^n\equiv a \bmod p$有解当且仅当$(n,\varphi(m))\,|\,\mathrm{ind}_g a$，其中$g$是模$m$原根. 如果有解，解数为$(n,\varphi(m))$.
   - 如果模m有原根，则同余方程$x^n\equiv a \bmod m$有解当且仅当$a^{\frac{\varphi(m)}{d}}\equiv 1 \bmod m$，其中$d=(n,\varphi(m))$.