重要知识点

- 第1章：整数的可除性
- 第2章：同余
- 第3章：同余式
- 第4章：二次同余式与平方剩余
- 第8~9章：群、群的结构（第5章：原根与指标）

- 整除的概念、性质
- 素数的概念、性质
  - p是正合数n大于1的最小正因子，那么p必定是素数，并且$p \leq \sqrt{n}$.
  - 如果对所有小于等于$\sqrt{n}$的素数p来说，p都不能整除n，那么n必定是素数.
  - 素数一定有无穷多个.
- 欧几里德除法/带余除法
  - $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists (q,r), s.t.\ a = bq + r, \quad 0 \leq r < b$
  - $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \forall c, \exists (q,r), s.t.\ a = bq + r, c \leq r < b + c$
  - b进制数$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 = (a_k a_{k-1} a_{k-2} \ldots a_1 a_0)_b$
- 最大公因数、最小公倍数、互素
  - 辗转相除法/广义欧几里德除法 $a = bq + c \Longrightarrow (a,b) = (b,c)$
  - $\exists s,t \in \mathbb{Z}, s.t., (a,b) = s \cdot a + t \cdot b$
  - $(a,b) = 1 \iff \exists s,t \in \mathbb{Z}, s.t., s \cdot a + t \cdot b = 1$
  - 如果素数$p|(ab)$, 则要么$p|a$, 要么$p|b$.
  - 算术基本定理 GCD，LCM的形式

- 同余的概念、性质
  - $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d,m)=1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m$
  - $\left.\begin{array}{c} a \equiv b \bmod m \\ d|a,b,m \end{array}\right\} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$
- 剩余/剩余类/完全剩余系/简化剩余系 Wilson定理：$(p-1)! \equiv -1 \bmod p$
- 欧拉函数的性质
  - $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
  - $(m,n)=1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n)$
  - $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$，$\varphi(n) = n \cdot (1-\frac{1}{p_1}) \cdot (1-\frac{1}{p_2}) \cdot \ldots \cdot (1-\frac{1}{p_s})$
  - 欧拉定理：$1 < m \in \mathbb{Z}, (a,m)=1 \Longrightarrow a^{\varphi(m)} \equiv 1 \bmod m$
  - 费尔马小定理：p是素数，$a \in \mathbb{Z}$，则$a^p \equiv a \bmod p$
- 模指数计算/模幂运算：总共需要$2k$次模乘运算,k为指数n的二进制长度

- 一次同余
  - $d=(a,m)$，$ax\equiv b \bmod m$有解 $\Longleftrightarrow$ $d|b$。有解的话，解数必为d
  - 求解一次同余式$ax\equiv b \bmod m$：
    - 计算$d=(a,m)$，判断是否$d|b$，如果不是则无解；如果整除的话：
    - 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$s$；
    - 写出全部解$x\equiv s\cdot\frac{b}{d}+k\cdot\frac{m}{d} \bmod m,\quad (k=0,1,2,\cdots,d-1)$
- 中国剩余定理(孙子定理)：
  - $m_1,m_2,\ldots,m_k\in\mathbb{Z}^+$两两互素，$\begin{cases} x\equiv b_1 \bmod m_1 \\ x\equiv b_2 \bmod m_2 \\ \cdots\cdots \\ x\equiv b_k \bmod m_k \end{cases}$
  - $M=m_1\cdot m_2\cdot\ldots\cdot m_k,\quad M_1=\frac{M}{m_1},M_2=\frac{M}{m_2},\ldots,M_k=\frac{M}{m_k}$
    $M_1'M_1\equiv 1 \bmod m_1, M_2'M_2\equiv 1 \bmod m_2,\ldots,M_k'M_k\equiv 1 \bmod m_k$
  - $x\equiv M_1'M_1b_1+M_2'M_2b_2+\ldots+M_k'M_kb_k \bmod M$
- 同余方程的恒等变形
  - $f(x)\equiv 0 \bmod m$；$f(x)+ms(x)\equiv 0 \bmod m$；$f(x)+s(x)\equiv s(x) \bmod m$；$af(x)\equiv 0 \bmod m$
  - $h(x)\equiv 0 \bmod m$有m个解(如$x^p-x\equiv 0 \bmod p$)，
    有$f(x)=q(x)h(x)+r(x)$，则$f(x)\equiv 0 \bmod m \Longleftrightarrow r(x)\equiv 0 \bmod m$
  - $f(x)\equiv 0 \bmod m$有解$\Longrightarrow f(x)\equiv 0 \bmod d$有解，其中$d$为$m$的正因子

一般高次同余$f(x) \equiv 0 \bmod m \iff \begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x) \equiv 0 \bmod m_k \end{cases}$

1. 分解m为两两互素的数之积: $m_1, m_2, \ldots, m_k$;
2. 求解$f(x) \equiv 0 \bmod m_1$得到a_{11}, ... , 求解$f(x) \equiv 0 \bmod m_k$得到a_{k1};
3. 求解同余式组$\begin{cases} x \equiv a_{11} \bmod m_1 \\ x \equiv a_{21} \bmod m_2 \\ \cdots\cdots \\ x \equiv a_{k1} \bmod m_k \end{cases}$ 得到全部$T_1 T_2 \ldots T_k$个解.

当$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$时, 取$m_1 = p_1^{\alpha_1}$, $m_2 = p_2^{\alpha_2}$, ... , $m_k = p_k^{\alpha_k}$
求解$f(x) \equiv 0 \bmod m$归结为求解$f(x) \equiv 0 \bmod p^{\alpha}$

模素数幂高次同余方程

- 如果$f(x)\equiv 0 \bmod m$ (1)有解且$d|m$, 则$f(x)\equiv 0 \bmod d$ (2)也有解
设$x\equiv c_1\dots,c_s \bmod d$ 为(2)的全部解, $x\equiv a_1 \bmod m$ 为(1) 的一个解,
则$c_1,\dots,c_k$中有且仅有一个(记为c_i)满足$a\equiv c_i \bmod d$.
- 考虑$m=p^\alpha, d=p^{\alpha-1}, \alpha\geq 2$，$c$是同余方程$f(x)\equiv 0 \bmod p^{\alpha-1}$的解.
为求$f(x)\equiv 0 \bmod p^\alpha$与$c$模$d$同余的解$a$, 即$a=kd+c$, 将$a=kd+c$代入方程$f(x)\equiv 0 \bmod p^\alpha$确定$k$的值
$f'(c)d\cdot k+f(c)\equiv 0 \bmod m, \quad i.e., \quad f'(c)p^{\alpha-1}\cdot k\equiv -f(c) \bmod p^\alpha$
因$p^{\alpha-1}|f(c)$故$f'(c)\cdot k\equiv \frac{-f(c)}{p^{\alpha-1}} \bmod p$是关于$k$的一次同余方程
  1. 如果$(f'(c),p)=1$, 可求出唯一解$x\equiv k_1 \bmod p$;
  2. 如果$(f'(c),p)\neq 1$, $p|f'(c)$, 如果$p\nmid \frac{-f(c)}{p^{\alpha-1}}$,则无解;
  3. 如果$(f'(c),p)\neq 1$, $p|f'(c)$, 如果$p|\frac{-f(c)}{p^{\alpha-1}}$,则有$p$个解$k\equiv 0,1,\dots,p-1 \bmod p$;

  从而$f(x)\equiv 0 \bmod p^\alpha$对应于$f(c)\equiv 0 \bmod p^{\alpha-1}$的解为
$x\equiv c+p^{\alpha-1}k_1 \bmod m$或$x\equiv c+p^{\alpha-1}k \bmod m$,$k\equiv 0,1,\dots,p-1 \bmod p$
- 求解$f(x)\equiv 0 \bmod m$，归结为求解$f(x)\equiv 0 \bmod p^\alpha$，再归结为求解$f(x)\equiv 0 \bmod p$

模素数高次同余方程

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0,$
取$g(x)=x^p-x,\ f(x)=(x^p-x)q(x)+r(x)$
同余方程$f(x)\equiv 0 \bmod p \iff r(x)\equiv 0 \bmod p$

求解任意次数模p的同余方程,可以转换为求解次数不超过$p-1$方程

次数为n的模p同余方程，解数k至多为n

模素数p的高次同余方程的求解：

1. 模p同余方程等价于次数不超过$p-1$的模p同余方程
2. 模p的次数不超过$p-1$(比如记为n)的同余方程的解数至多为它的次数n
3. 模p的次数为$n(<p)$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

平方/二次(非)剩余的概念、个数、欧拉判别条件

a是模素数p的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$

a是模素数p的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \bmod p$

勒让德符号：$a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \bmod p$，其中$p$为奇素数

$$(\frac{a+kp}{p}) = (\frac{a}{p}), a \equiv b \bmod p \Longrightarrow (\frac{a}{p}) = (\frac{b}{p}),$$

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}), (a,p) = 1 \Longrightarrow (\frac{a^2}{p}) = 1$$

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

Gauss二次互反律：奇素数p, q, $(\frac{q}{p}) \cdot (\frac{p}{q}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

只要一个模4余1, 就有$(\frac{p}{q}) = (\frac{q}{p})$,否则$(\frac{p}{q}) = -(\frac{q}{p})$

雅克比符号$(\frac{a}{m}) \triangleq (\frac{a}{p_1}) \cdot \ldots \cdot (\frac{a}{p_s})$，其中$m = p_1 \ldots p_s$，$(\frac{a}{p_i})$为勒让得符号

若$(m,n) > 1$则$(\frac{m}{n}) = 0, (\frac{n}{m}) = 0$

$(\frac{a+km}{m}) = (\frac{a}{m})$

$(\frac{ab}{m}) = (\frac{a}{m})(\frac{b}{m})$

$$(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1 & \text{if } m \equiv 1 \bmod 4 \\ -1 & \text{if } m \equiv 3 \bmod 4 \end{cases}$$

$$(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1 & m \equiv \pm 1 \bmod 8 \\ -1 & m \equiv \pm 3 \bmod 8 \end{cases}$$

雅克比符号的互反律:$(m,n) = 1$, $(\frac{n}{m}) \cdot (\frac{m}{n}) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$

只要一个模4余1, 就有$(\frac{m}{n}) = (\frac{n}{m})$,否则$(\frac{m}{n}) = -(\frac{n}{m})$

计算雅克比符号(包括特殊情形勒让德符号)的值，并不需要分解素因数式；
有了雅克比符号，也大大方便了勒让德符号的计算(可直接翻转)

模数为2的幂次的二次同余方程$x^2 \equiv a \bmod 2^\delta$的判定与求解

1. $\delta = 2$ $x^2 \equiv a \bmod 4$ 有解 $\Longleftrightarrow$ $a \equiv 1 \bmod 4$ 解为$x \equiv \pm 1 \bmod 4$
2. $\delta > 2$ $x^2 \equiv a \bmod 2^\delta$ 有解 $\Longleftrightarrow$ $a \equiv 1 \bmod 8$，解的个数为4
    - $\delta = 3$时，$x \in \{\pm(1+4k) : k \in \mathbb{Z}\}$
    - $\delta = 4$时，利用模2^3下的解推出$x \in \{\pm(1+8l+4\cdot(\frac{a-1}{8} \bmod 2))\}, l \in \mathbb{Z}$
    - $\delta = 5$时，利用模2^4下的解推出$x \in \{\pm(x_4+16s+8\cdot(\frac{a-x_4^2}{16} \bmod 2))\}, s \in \mathbb{Z}$，其中$x_4 = 1+4\cdot(\frac{a-1}{8} \bmod 2)$
    - $\cdots$

方程$x^2 \equiv a \bmod p^\alpha$($a$与$p$互素)的判定与求解: $x^2 \equiv a \bmod p^\alpha$有解 $\Longleftrightarrow$ a为模p的二次剩余. 且有解的话, 解数为2

作为第3章的特例，求解$x^2 \equiv a \bmod p^\alpha$，归结为求解$x^2 \equiv a \bmod p$

模素数的二次同余方程$x^2 \equiv a \bmod p$求解

- 对特殊素数$p = 4k+3$，$a^{\frac{p-1}{2}} \equiv 1 \bmod p$，解为$x \equiv \pm a^{\frac{p+1}{4}} \bmod p$
- 对一般素数p，(若x_0为解则$a^{-1}x_0^2 \equiv 1 \bmod p$)
  1. 将$p-1$写成2的幂和奇数的乘积$p-1 = 2^t \cdot s$
     $a^{\frac{p-1}{2}} \equiv 1 \bmod p$，$(a^{-1} \cdot (a^{\frac{s+1}{2}})^2)^{2^{t-1}} \equiv 1 \bmod p$
     用$x_{t-1} = a^{\frac{s+1}{2}}$构造$y^{2^{t-1}} \equiv 1 \bmod p$的解$y = a^{-1}x_{t-1}^2$
  2. 任取模p的平方非剩余n，计算$b = (n^s \bmod p)$
     $b^{2^t} = n^{p-1} \equiv 1 \bmod p$，$b^{2^{t-1}} = n^{\frac{p-1}{2}} \equiv -1 \bmod p$
  3. $(a^{-1} \cdot (x_{t-1})^2)^{2^{t-1}} \equiv 1 \bmod p$则$(a^{-1} \cdot (x_{t-1})^2)^{2^{t-2}} \equiv \pm 1 \bmod p$令
     $x_{t-2} = x_{t-1}$，当$(a^{-1} \cdot (x_{t-1})^2)^{2^{t-2}} \equiv 1 \bmod p$时
     $x_{t-2} = x_{t-1} \cdot b$，当$(a^{-1} \cdot (x_{t-1})^2)^{2^{t-2}} \equiv -1 \bmod p$时
     则$y = a^{-1}x_{t-2}^2$为$y^{2^{t-2}} \equiv 1 \bmod p$的解
  4. $(a^{-1} \cdot (x_{t-2})^2)^{2^{t-2}} \equiv 1 \bmod p$则$(a^{-1} \cdot (x_{t-2})^2)^{2^{t-3}} \equiv \pm 1 \bmod p$令
     $x_{t-3} = x_{t-2}$，当$(a^{-1} \cdot (x_{t-2})^2)^{2^{t-3}} \equiv 1 \bmod p$时
     $x_{t-3} = x_{t-2} \cdot b^2$，当$(a^{-1} \cdot (x_{t-2})^2)^{2^{t-3}} \equiv -1 \bmod p$时
     则$y = a^{-1}x_{t-3}^2$为$y^{2^{t-3}} \equiv 1 \bmod p$的解
  5. $\cdots$ $x_0 = x_1$或$x_1 \cdot b^{2^{t-2}}$，$y = a^{-1}x_0^2$为$y \equiv 1 \bmod p$的解。x_0即为最终所求。

模合数的二次同余方程$x^2 \equiv a \bmod m$求解，$m = 2^{\delta} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\begin{cases} x^2 \equiv a \bmod 2^{\delta} \\ x^2 \equiv a \bmod p_1^{\alpha_1} \\ x^2 \equiv a \bmod p_2^{\alpha_2} \\ \dots\dots \\ x^2 \equiv a \bmod p_k^{\alpha_k} \end{cases}$$

要解决的问题是：
方程$x^2 \equiv a \bmod 2^{\delta}$的判定(与求解)，
方程$x^2 \equiv a \bmod p^{\alpha}$($a$与$p$互素)的判定(与求解).

二次同余方程的求解方法:

1. 模素数的二次方程$x^2 \equiv a \bmod p$的解的判定与求解;
2. 模为2^δ的二次方程$x^2 \equiv a \bmod 2^\delta$的解的判定与求解(有解的话, 解数为4, 从$x^2 \equiv a \bmod 2^3$开始求解);
3. 模为p^α的二次方程$x^2 \equiv a \bmod p^\alpha$的解的判定与求解(有解的话, 解数为2, 从$x^2 \equiv a \bmod p$开始求解);
4. 模为合数的二次方程$x^2 \equiv a \bmod m$(a与m互素)的解的判定与求解(利用2与3).

第8-9、5章 群

- 群的概念、性质，群的阶、群元素的阶，剩余类群
- 子群的概念、性质、判断
- 陪集的概念及性质，正规子群、商(集)群、拉格朗日定理：子群的阶/元素的阶整除群的阶
- Z_p^*乘法群，循环群(两类)，生成元(个数)
- 群同态/同构的概念、性质、例子，核

指数/阶； 原根/生成元； 指标/对数

- a与m互素，则整数d使得$a^d \equiv 1 \bmod m \iff \mathrm{ord}_m(a)|d$
  如果a与m互素，自然有$\mathrm{ord}_m(a)|\varphi(m)$
  为了求a的指数，只需要在$\varphi(m)$的因子中找即可
- 设a与m互素，$n|m \implies \mathrm{ord}_n(a)|\mathrm{ord}_m(a)$
- $ab \equiv 1 \bmod m \implies \mathrm{ord}_m(a) = \mathrm{ord}_m(b)$ (即a与它的逆元同阶)
- 设$m > 1, (a, m) = 1$，则$a^k \equiv a^l \bmod m \iff k \equiv l \bmod \mathrm{ord}_m(a)$
- $\mathrm{ord}_m(a^k) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)}$
  如果a是模m的原根,则$a^k(k > 0)$也是模m的原根 $\iff (k, \varphi(m)) = 1$
  模m有$\varphi(\varphi(m))$个原根
  简化剩余中任取一个元素是模m原根的概率为$\dfrac{\varphi(\varphi(m))}{\varphi(m)}$

指数/阶； 原根/生成元； 指标/对数

- $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \iff (\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$
  一般地，未必有$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$
  也未必有$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$
  已知a, b均与m互素，则存在c使得$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$
- $(a, m) = (a, n) = (m, n) = 1 \Longrightarrow \mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$
  如果a与$pq(p \neq q)$互素，显然有$\mathrm{ord}_{pq}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)]$
  如果$m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$，$(a, m) = 1$，则有
  $\mathrm{ord}_m(a) = [\mathrm{ord}_{2^{\alpha_1}}(a), \mathrm{ord}_{p_2^{\alpha_2}}(a), \dots, \mathrm{ord}_{p_s^{\alpha_s}}(a)]$
- $(m, n) = 1$，a_1, a_2均与mn互素，则存在a使得$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$
- 模m存在原根$\Longrightarrow m = 1$，或2，或4，或p^α，或$2p^\alpha$ (p是奇素数)

指数/阶； 原根/生成元； 指标/对数

- 设p是素数, 则模p有原根
- 设g是模$p^{\alpha+1}(\alpha \geq 1)$的原根, 则$g$必是模$p^\alpha$的原根
- 设g是模p^α的原根, 则必有$\mathrm{ord}_{p^{\alpha+1}}(g) = \varphi(p^\alpha)$, 或$\mathrm{ord}_{p^{\alpha+1}}(g) = \varphi(p^{\alpha+1})$
- g是模奇素数p的原根, 满足$g^{p-1} = 1 + rp, p \nmid r$, 则$g$是模$p^\alpha(\forall\alpha \geq 1)$的原根
- 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.
- 我们总可以由任意的模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.
- 模m有原根的充要条件是$m = 1$,或2,或4,或p^α,或$2p^\alpha$

指数/阶； 原根/生成元； 指标/对数
整理的结论:

1. p为奇素数, 模p的原根必存在, 比如说是g';
2. 由这个模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;

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。

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。

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