总复习
信息安全数学基础期末总复习

中山大学　计算机学院

第一章小结

1. 整除a的概念.
   - 习题1.8(2), 习题1.8(3), 习题1.8(4), 习题1.8(12), 习题1.8(40), 习题1.8(41)
2. 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.
3. 合数n的最小正因子p一定是素数，且$p \leq \sqrt{n}$.
   - 习题1.8(9), 习题1.8(10)
4. 素数一定有无穷多个.
   - 定理1.1.8, 习题1.8(13), 习题1.8(14), 例4.4.12, 习题4.8(27)
5. 如果$a, b \in \mathbb{Z}^+, b|a$, 那么$(a, b) = b$.
   - 习题1.8(26), 习题1.8(49)
6. $a = bq + c \Longrightarrow (a, b) = (b, c)$.
7. 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$p|b$.

第一章小结

8. 使用辗转相除法计算最大公因数.
   - 引理1.3.1, 引理1.3.2, 习题1.8(28), 习题1.8(34)
9. 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$t$.
   - 习题1.8(32)
10. $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{|d|}$, 其中$d$是$a$和$b$的公因数. 特别地, $(\frac{x}{(x,y)}, \frac{y}{(x,y)}) = 1$.
11. $(a, c) = 1 \Longrightarrow (ab, c) = (b, c)$.
12. $(a, b) = (a, ax + b) = (a + bx, b)$, 其中$x$是整数.
    - 习题1.8(24), 习题1.8(25), 习题1.8(29), 习题1.8(36),
13. 算术基本定理, 整数的标准分解式.
14. 最小公倍数$[a, b] = \dfrac{ab}{(a, b)}$

第二章小结

1. 同余的概念.
   - 例2.1.6, 习题2.6(6)
2. 模m同余相等与整数相等的相似性.
   - 习题2.6(15)
3. $\left.\begin{array}{l} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \end{array}\right\} \Longrightarrow a \equiv b \bmod [m_1, m_2]$
4. $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d, m) = 1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m, \quad \left.\begin{array}{c} a \equiv b \bmod m \\ d|a, b, m \end{array}\right\} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}.$
5. 完全(简化)剩余系的写法. 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.
   - 习题2.6(25), 习题2.6(26), 习题2.6(28), 习题2.6(31)
8. 欧拉函数的性质. $(m, n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n)$, 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$a^p \equiv a \bmod p$.
    - 习题2.6(33), 习题2.6(34), 习题2.6(35), 习题2.6(36)

第三章小结

1. 一次同余方程$ax \equiv b \bmod m$的解法.
   计算$d=(a,m)$; 判断是否$d\,|\,b$; 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
$$x \equiv s\cdot\frac{b}{d}+k\cdot\frac{m}{d} \bmod m, \quad (k=0,1,2,\cdots,d-1).$$
   - 习题3.5(1), 习题3.5(2)
2. 利用中国剩余定理求解一次同余方程组.
   $x \equiv M_1'M_1b_1+M_2'M_2b_2+\ldots+M_k'M_kb_k \bmod M.$
   - 习题3.5(3), 习题3.5(12), 习题3.5(13), 习题3.5(14), 习题3.5(15)
3. 利用中国剩余定理进行模指数运算.
   - 习题3.5(17), 习题3.5(18)
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.

第三章小结

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

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

   - 习题3.5(5), 习题3.5(6)

第三章小结

7. 模为素数p的同余方程$f(x) \equiv 0 \bmod p$.
   模素数高次同余方程(从而一般高次同余方程)没有那样完美的结论.
   1. 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;
   2. 这个模p的次数为$n \le p-1$的同余方程的解数至多为它的次数n;
   3. 这个模p的次数为$n \le p-1$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.
   4. "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.

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;
   - $\{1^2 \bmod p, 2^2 \bmod p, 3^2 \bmod p, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p\}$是模$p$的全部二次剩余.
     - 习题4.8(24)
3. 欧拉判定模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 $\iff a^{\frac{p-1}{2}}\equiv -1 \bmod p$.
   - 习题4.8(31), 习题4.8(32)

第四章小结

4. 勒让德符号及其基本性质，二次互反律.
   - $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.
   - $(\frac{a+kp}{p}) = (\frac{a}{p})$，其中$k$为整数.
   - $a \equiv b \bmod p \Longrightarrow (\frac{a}{p}) = (\frac{b}{p})$
   - $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$，
   - $(a, p) = 1 \Longrightarrow (\frac{a^2}{p}) = 1$.
   - $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$，其中$p \neq q$均为奇素数.
   - $\left(\frac{-1}{p}\right)$，$\left(\frac{2}{p}\right)$和$\left(\frac{3}{p}\right)$.
   - 结合勒让德符号的基本性质，利用二次互反律计算勒让德符号.
   - 习题4.8(20)，习题4.8(35)，习题4.8(36)

第四章小结

5. 雅可比符号及其基本性质.
   - $\left(\frac{a}{m}\right) \triangleq \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \cdots \cdot \left(\frac{a}{p_s}\right)$, 其中$m = p_1 p_2 \ldots p_s$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.

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$x \equiv \pm a^{\frac{p+1}{4}} \bmod p$.
     - 例4.6.1, 例4.6.2
   - 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，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, 容易求出同余方程$y^{2^{t-2}} \equiv 1 \bmod p$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, 继续求解, 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;
   - 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$t > k$, 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, 我们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, 从而最终求出同余方程$y \equiv 1 \bmod p$的一个形如$a^{-1}x_0^2$的解.
   - 至此, 完成原二次同余方程的求解，一个解$x_0 \bmod p$, 另一个是$-x_0 \bmod p$.

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(其中的$x_{t-1}$)是

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

这是因为

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

如果$t=1$，则$x_0^2\equiv a^{s+1}\equiv a \bmod p$，即$x_0 \bmod p$就是原二次同余式的一个解.

如果$t>1$，下面是找出方程$y^{2^{t-2}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-2}^2$的解的方法.
由于$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv 1 \bmod p$，而且$(a^{-1}x_{t-1}^2)^{2^{t-1}}=[(a^{-1}x_{t-1}^2)^{2^{t-2}}]^2$
所以必定有

$$(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$, 则令$x_{t-2} = x_{t-1}$, 且有

$$(a^{-1}x_{t-2}^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$$

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

$$\begin{aligned}(a^{-1}x_{t-2}^2)^{2^{t-2}} &= (a^{-1}x_{t-1}^2b^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}}(b^2)^{2^{t-2}} \\ &= (a^{-1}x_{t-1}^2)^{2^{t-2}}b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}} \equiv 1 \bmod p$的解.
如果$t = 2$, 则$x_0^2 \equiv a \bmod p$, 即$x_0 \bmod p$就是原二次同余式的一个解.

所以, 不论$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$还是$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$, 总能利用方程

$$y^{2^{t-1}} \equiv 1 \bmod p$$

一个形如$a^{-1}x_{t-1}^2$的解, 计算出方程

$$y^{2^{t-2}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-2}^2$的解.

类似地, 如果$t > 2$, 必定有

$$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$, 则令$x_{t-3} = x_{t-2}$, 且有

$$(a^{-1}x_{t-3}^2)^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p$, 则令$x_{t-3} = x_{t-2} \cdot b^{2^1}$, 则$x_{t-3}^2 = x_{t-2}^2 \cdot b^{2^2}$, 且有

$$\begin{aligned}(a^{-1}x_{t-3}^2)^{2^{t-3}} &= (a^{-1}x_{t-2}^2 b^{2^2})^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} (b^{2^2})^{2^{t-3}} \\ &= (a^{-1}x_{t-2}^2)^{2^{t-3}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.
如果$t = 3$, 则$x_0^2 \equiv a \bmod p$, 即$x_0 \bmod p$就是原二次同余式的一个解.

类似地，如果$t>3$，必定有

$$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$，则令$x_{t-4}=x_{t-3}$，且有

$$(a^{-1}x_{t-4}^2)^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-4}^2$是同余方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p$，则令$x_{t-4}=x_{t-3}\cdot b^{2^2}$，则$x_{t-4}^2=x_{t-3}^2\cdot b^{2^3}$，且有

$$\begin{aligned}(a^{-1}x_{t-4}^2)^{2^{t-4}} &= (a^{-1}x_{t-3}^2 b^{2^3})^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}}(b^{2^3})^{2^{t-4}} \\ &= (a^{-1}x_{t-3}^2)^{2^{t-4}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-4}^2$是方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.
如果$t=4$，则$x_0^2 \equiv a \bmod p$，即$x_0 \bmod p$就是原二次同余式的一个解.
如果$t>4$，则继续找出方程$y^{2^{t-5}} \equiv 1 \bmod p$的一个形如$a^{-1}x_{t-5}^2$的解.

第五章小结

1. 指数与原根的基本概念
   - 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.
2. 指数与原根的基本性质. 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$\mathrm{ord}_m(a) \mid d$.
   - 如果$n \mid m$, 则$\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.
   - 如果$ab \equiv 1 \bmod m$, 则$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.
   - 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.
   - $a^k \equiv a^l \bmod m$当且仅当$k \equiv l \bmod \mathrm{ord}_m(a)$
   - $\mathrm{ord}_m(a^k) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)}$, 其中$k$是非负整数.
   - 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

3. 寻找模p的原根
   - 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

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

4. 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，$\alpha \geq 1$.
   - p为奇素数，模p的原根必存在，例如是g'，可通过对$2, 3, 4, \ldots$依次验证得到.
   - 如果g'是模m的原根，$g = g', g = g' + p, g = g' + 2p, \ldots, g = g' + (p-1)p$都是模$p$的原根.
   - 满足$\tilde{g}^{p-1} = 1 + rp,\ p \nmid r$的模$p$的原根$\tilde{g}$都是模$p^\alpha$的一个原根.
   - 满足$\tilde{g}^{p-1} = 1 + rp,\ p \nmid r$的是奇数的模$p$的原根$\tilde{g}$都是模$2p^\alpha$的一个原根.

   - 习题5.4(11)，习题5.4(12)，习题5.4(13)，习题5.4(14)

第五章小结

5. 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$s \equiv \mathrm{ind}_g a \bmod \varphi(m)$.
   - $\mathrm{ind}_g(a_1 \ldots a_n) \equiv \mathrm{ind}_g a_1 + \ldots + \mathrm{ind}_g a_n \bmod \varphi(m)$.
6. 指标与指数
   - 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$\varphi(e)$.
7. 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$(n, \varphi(m)) \mid \mathrm{ind}_g a$，其中$g$是模$m$原根. 如果有解，解数为$(n, \varphi(m))$

第八章第九章小结

知识点:

1. 群，子群，陪集，正规子群，商群，对称群，置换群和循环群的基本概念.
2. 群的同态与同构的基本概念，同态核的基本概念
3. 群的阶和群元素的阶的基本概念，以及Lagrange定理的结论.
4. 无限循环群同构于整数加群，而n阶循环群同构于模n剩余类群，

能力:

1. 给定集合和运算能够判断是否构成群，
2. 给定群的子集合能够判断是否构成子群，
3. 能判断两个群是否同态或同构，知道群同态或群同构的一些典型例子.
4. 能够判断一个群是否为循环群.
5. 给定n阶循环群的生成元g，能够确定群元素g^i的阶，其中$0 \le i \le n-1$，也即g^i的生成子群的阶.

第十章小结

知识点:

1. 环, 交换环, 有单位元环, 零因子环, 整环, 域的基本概念.
2. 环的同态与同构的基本概念.
3. 环特征的基本概念和基本性质.
4. 子环, 理想, 商环的基本概念.

能力:

1. 给定集合和运算能够判断是否构成环.
2. 给定环的子集合能够判断是否构成子环或理想.
3. 给定环的理想能够确定其商环, 并能够判断该商环是整环还是域.

建议学习的典型证明过程

1. 辗转相除法求最大公因数的正确性.
   - 参考ppt chap1a.pdf
2. 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.
   - 定理2.2.3, 定理2.3.4
3. Euler定理和Fermat小定理的证明.
4. wilson定理的证明.
5. 中国剩余定理的构造证明.
6. Euler判别条件的证明.
7. 模奇素数幂p^α的二次同余方程解的存在性证明.
   - 参考定理4.6.4
8. $\mathrm{ord}_m(a^k) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)}$的证明.
   - 参考定理5.1.4
9. g是模p的原根的充要条件证明.
   - 参考定理5.2.2
10. 关于群的Lagrange定理的证明.