第一章：

整除性质：

① $c|b, b|a \Rightarrow c|a$.

② $b|a \Rightarrow cb|ca$.

③ $c|a, c|b \Rightarrow \forall m,n\in\mathbb{Z}$. 有 $c|ma+nb$.

④ $b|a, a\neq 0 \Rightarrow |b|\leq|a|$.

⑤ $cb|ca \Rightarrow b|a$.

⑥ $b|a, a\neq 0 \Rightarrow \frac{a}{b}|a$. (注：$a=bq$. 令 $\frac{a}{b}=q|a$)

⑦ $b|a, a|b \Rightarrow b=\pm a$.

余数性质：

① $(a_1\pm a_2)=\langle\langle a_1\rangle\pm\langle a_2\rangle\rangle$,

② $\langle a_1 a_2\rangle=\langle\langle a_1\rangle\langle a_2\rangle\rangle$

定理：辗转相除法：

1 $a=bq+c$, $q\in\mathbb{Z} \Rightarrow (a,b)=(c,b)=r_n$.

2 $a>0, b>0$. $\exists m,n$ s.t. $(a,b)=ma+nb$. ↙ 证.

3 $a|bc$, $(a,b)=1 \Rightarrow a|c$.

4 $(a_1,a_2)=d_1$, $(a_3,d_1)=d_2\cdots(a_n,d_{n-1})=d_n$.

$\Rightarrow (a_1,a_2\cdots a_n)=d_n=a_1x_1+\cdots+a_nx_n$.

最小公倍数：$[a,b]=\frac{ab}{(a,b)}$

$(a_1,a_2)=1 \Rightarrow [a_1,b]=a_1b$.

但 $(a_1\cdots a_n)=1 \not\Rightarrow [a_1\cdots a_n]=|a_1\cdots a_n|$ eg：3与6

素数：

1 $a>1$, a 除1外min因数为素数，记为 q.

a 为合数时，$q\leq\sqrt{a}$.

2 p 素，$a\nu \Rightarrow p|a$ 或 $(p,a)=1$.

3. p 素，$p|ab \Rightarrow p|a$ or $p|b$.

梅森数：$M_p=2^p-1$ 2^n-1 素 $\Rightarrow n$ 素

定理：1. $a,b>0$. $s>1 \Rightarrow (s^a-1, s^b-1)=s^{(a,b)}-1$ ← 辗转相除法可证.

2. q 是 M_p 素因数，则 $q=2kp+1$.

费马数：$F_n=2^{2^n}+1$ $(n\geq 0)$. 定理：1. $\forall m\neq n$, $(F_m,F_n)=1$. ⇒ 素数无穷.

下指为素解法，列出不超 $\sqrt{n}$ 的全体素数，删去其倍数，留它本身.

定理：1 素数无穷多

2. 2是唯一偶素，素 $p=4k\pm1$ (无限多)

3 狄利克雷：$m, a\in\mathbb{Z}$, $(a,m)=1 \Rightarrow$ 素 $mk+a$ 无穷.

一次不定方程：$a_1x+a_2y=n$. ← 原式 解为 $x=x_0+\frac{a_2}{d}t$

有解充要：$(a_1,a_2)|n$. $y=y_0-\frac{a_1}{d}t$

$(a_1,a_2)=d \Rightarrow a_1x_0+a_2y_0=d$ *

$a_1kx_0+a_2ky_0=dk\triangleq n \Rightarrow \frac{a_1}{d}x+\frac{a_2}{d}y=\frac{n}{d}$

$\therefore x=kx_0$, $y=ky_0$ 是原式的解. 与原式同解.

设 (x_1,y_1) 是另解：$\left.\begin{aligned}a_1x_1+a_2y_1=kd\\ a_1kx_0+a_2ky_0=kd\end{aligned}\right\} \Rightarrow a_1(x_1-kx_0)=a_2(ky_0-y_1)$

$\Rightarrow \frac{a_1}{d}(x_1-kx_0)=\frac{a_2}{d}(ky_0-y_1)$

已知 $(\frac{a_1}{d},\frac{a_2}{d})=1$. 那么有 $\frac{a_2}{d}|x_1-kx_0 \Rightarrow t\cdot\frac{a_2}{d}=x_1-kx_0 \Rightarrow x_1=kx_0+\frac{a_2}{d}\cdot t$.

$y_1=ky_0-\frac{a_1}{d}\cdot t$.

s 元一次不定方程有解：$(a_1,a_2\cdots a_s)|n$

步骤：对 $(a_1,a_2)=d$. 先求 $a_1x+a_2y=d$ 的 x,y. 再乘 k 至 $n=|cd$ 时得 x_0,y_0.

则 $x_1=x_0+\frac{a_2}{d}t$. $y_1=y_0-\frac{a_1}{d}t$.

证：

$\because m=n+k$. 设 l 是 F_m, F_n 的最大公因

$\frac{F_{m-2}}{F_m}=\frac{2^{2^{n+k}}+1-2}{2^{2^{n+k}}+1}=\frac{2^{2^{n+k}}-1}{2^{2^{n+k}}+1}$

令 $2^{2^k}=x$ $\Rightarrow \frac{x^{2^k}-1}{x+1}=x^{2^k-1}-x^{2^k-2}\cdots+x-1$

由 $l|F_m$, $l|F_n|F_{m-2}$. 整数↑

$\Rightarrow l|2$. 因 F_m, F_n 奇 $\therefore l\neq 2$.

$\therefore l=1$. $\therefore (F_m,F_n)=1$

第二章

同余 $a \equiv b \pmod m$.

e.g. $8^{1234} \bmod 13$ 余？ $8^2 = 64 \equiv -1 \pmod{13}$.

$8^{1234} \equiv (64)^{617} \equiv 1 \pmod{13}$.

定理：1. $a \equiv b \pmod m \Leftrightarrow m \mid a-b$

2. 当 $a \equiv b,\ \alpha \equiv \beta \pmod m$.

$\Rightarrow$ ①. $ax+\alpha y \equiv bx+\beta y \pmod m$

②. $a\alpha \equiv b\beta \pmod m$.

③. $a^n \equiv b^n \pmod m$

④. $f(a) \equiv f(b) \pmod m$

e.g: $n>0$. 被9整除 $\Leftrightarrow$ 各位和被9整除.

$n = a\cdot 10^2 + b\cdot 10 + c\cdot 1 \equiv a+b+c \equiv 0 \pmod 9$

e.g 证明 $641 \mid 2^{2^5}+1 = 2^{32}+1$

$2^{32}+1 \equiv 0 \pmod{641}$.

e.g. n 是奇数，$3 \mid 2^n+1$. n 为偶，$3 \nmid 2^n+1$

$2^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod 3$

模二项式定理：p 为素，$(x+y)^p \equiv x^p + y^p \pmod p$

3. $ac \equiv bc \pmod m$，当 $(m,c)=d \Rightarrow a \equiv b \pmod{\frac{m}{d}}$

$m \mid (ac-bc) = c(a-b) \Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$

4. $a \equiv b \pmod{m_i}$. $i = 1, 2, \cdots n \Rightarrow a \equiv b \pmod{[m_1, \cdots, m_n]}$

e.g: 求 7^{7^7} 个位数：

已知 $7^2 = 49 \equiv -1 \pmod{10}$.

$\Rightarrow 7^4 \equiv 1 \pmod{10}$.

$7^7 \equiv (-1)^7 \equiv 3 \pmod 4$. 即 $7^7 = 4k+3$

$\therefore 7^{7^7} \equiv 7^{4k+3} \equiv 7^3 \equiv 3 \pmod{10}$

注：求 a^{b^c} 同余：① $a^k \equiv 1 \pmod m$. 求 k.

② $b^c = kq + r$. 即 $b^c \equiv r \pmod k$

③ $a^k \equiv a^r \pmod m$

剩余类：C_r ($r = 0, 1, \cdots m-1$) 表示余数为 r 的数集

$C_0, C_1 \cdots C_{m-1}$ 称模 m 剩余类.

定理：1. 某整数恰在 C_j 中. $x \equiv y \pmod m$ 则 $x, y \in C_j$

完全剩余系与简系：最小完全剩余系：

$a_0, a_1 \cdots a_{m-1}$ $\quad$ $0, 1, 2 \cdots m-1$.

缩系：剩余类的同余 r 与 m 互素.

$\varphi(n) = 0, 1 \cdots n-1$ 中与 n 互素的数的个数

定理：1. $(a,m)=1$. x 通过 m 个缩系 $\Rightarrow ax$ 也通过.

2. Euler: $m>1$, $(a,m)=1$, 则 $a^{\varphi(m)} \equiv 1 \pmod m$

2. 费马小定理：$a^p \equiv a \pmod p$

p 为素. 当 $(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

一次同余式：$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_0 \equiv 0 \pmod m$

n = 次数

$f(x_0) \equiv 0 \pmod m$ 则 $x \equiv x_0$ 称解

不同解指不同余.

3. $(k,m)=1$ 当 $a_0, \cdots a_{m-1}$ 是模完全剩余系 $\Rightarrow ka_0, \cdots ka_{m-1}$ 是另组…

一次同余式求解：

定理：1. 设 $(a,m)=d$. $d \nmid b \Rightarrow ax \equiv b \pmod m$ 无解

$d \mid b \Rightarrow ax \equiv b \pmod m$ 有 d 个模 m 不同余的解

推论：若 $(a,m)=1$. 则 $ax \equiv b \pmod m$ 恰只有一解.

e.g: $4x \equiv 2 \pmod 6$ $\quad$ $(4,6) = 2 \mid 2$ 有解.

2. $(a,m)=1$. $ax \equiv 1 \pmod m$ 的解是 a 模 m 逆.

$a \equiv \pm 1 \pmod p \Leftrightarrow a$ 是其自身模 p 的逆.

该解：$x \equiv b \cdot a^{\varphi(m)-1} \pmod m$

3. Wilson: $(p-1)! + 1 \equiv 0 \pmod p$

法一：$(4,6)=2 \Rightarrow 2x \equiv 1 \pmod 3$ $\quad$ $x \equiv 1 \cdot 2^{\varphi(3)-1} \equiv 2 \pmod 3$

$\Rightarrow k \equiv 2+3k$. $k = 0, 1$ 即 $x \equiv 2, x \equiv 5 \pmod 6$

$d=2$ 个.

法二：有 $2a+3b=1 \Rightarrow \begin{cases} a=-1 \\ b=1 \end{cases}$ $\therefore -2x+3x = x \Rightarrow 2x \equiv -x+3x \equiv -x \equiv 1 \pmod 3$

$\therefore x \equiv 1 \pmod 3$ $\quad$ $x \equiv 1+k\cdot 3$ $\quad$ $k = 0, 1$.

$d=2$ 个.

$\varphi(n)$：欧拉函数　$n>2$，$\varphi(n)$必为偶

$n=p$　$\varphi(p)=p-1$.

$n=p^k$　$\varphi(p)=p^k-p^{k-1}$ ← 其中与p^k非互素的为np，最大为$p\cdot p^{k-1}$，则共p^{k-1}个不与p互素.

若$(m,n)=1$，则$\varphi(mn)=\varphi(m)\varphi(n)$ ⇒ 证明 ⇒ 若$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$\varphi(n)=n\cdot(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$

中国剩余定理：设m,n，$(m,n)=1$，对$\forall b,c$：

$x\equiv b\pmod m$，$x\equiv c\pmod n$.

恰有一解 $0\le x\le mn-1$

孙子剩余定理：$(m_1,m_2,\cdots,m_k)$两两互素，$m=m_1m_2\cdots m_k$，$m=m_iM_i$，$M_iM_i'\equiv 1\pmod{m_i}$.

则：$x=b_1\pmod{m_1}$　$x=b_2\pmod{m_2}\cdots x=b_k\pmod{m_k}$

有唯一解：$x=M_1M_1'b_1+M_2M_2'b_2+\cdots+M_kM_k'b_k\pmod m$

一次同余式组：$x=b_1\pmod{m_1}$，$x\equiv b_2\pmod{m_2}$，可解 $\Leftrightarrow (m_1,m_2)\mid b_1-b_2$.

↓ 对$[m_1,m_2]$解唯一.

eg：解联立同余式：$x\equiv 1\pmod 6$

$x\equiv 4\pmod 9$

$x\equiv 7\pmod{15}$

$(6,9)=3\mid 4-1$　$x\equiv b_2'\pmod{18}\equiv 13$

$(18,15)=3\mid 13-7=6$，$x\equiv b_3'\pmod{90}\equiv -23\equiv 67\pmod{90}$

定理3：$(m_1,m_2,\cdots,m_k)$两两互素，$m=m_1m_2\cdots m_k$，$f(x)\equiv 0\pmod m$有解

$\Leftrightarrow f(x)\equiv 0\pmod{m_i}$有一个$i$有解.

设$f(x)\equiv 0\pmod{m_i}$解数为T_i，则$f(x)\equiv 0\pmod m$的解数为$T=T_1T_2\cdots T_k$

eg：$x^3+1\equiv 0\pmod{15}$.

15分解为3,5，$f(x)=x^3+1\equiv 0\pmod 3\Rightarrow x\equiv 2\pmod 3$.

$x^3+1\equiv 0\pmod 5\Rightarrow x\equiv 4\pmod 5$.

$\Rightarrow$ $m_i=3$　$m_i=5$.

$m=15$　$M_1=5$　$M_2=3$.

$M_1'=2$　$M_2'=2$

$x\equiv 10\times 2+6\times 4=44\pmod{15}\equiv 14$

模素同余式：

定理，1 拉格朗日定理：$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\equiv 0\pmod p$最多有$n$解. p为素，$a_n\not\equiv 0\pmod p$ 条件.

eg：$x^2+3\equiv 0\pmod 5$ 无解.

2. $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\equiv 0\pmod p$的解数大于$n$，则$p\mid a_i$（$i=0,1,\cdots,n-1,n$）

3. $\forall p$素，$f(x)=(x-1)(x-2)\cdots(x-(p-1))-x^{p-1}+1$ 所有系数被p整除.

$f(x)$为至于$p-1$次多项式，因为$x^{p-1}-x^{p-1}=0$，而有$1,2,\cdots,p-1$，p个根

4. Wolstenholme：素$p>3$，$\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv 0\pmod{p^2}$

$(p-1)!\sum_{k=1}^{p-1}\frac{1}{k}\equiv 0\pmod{p^2}$

常二章：二次剩余.

$m>1$，若 $x^2\equiv n \pmod m$ $(n,m)=1$，则 n 为模 m 二次剩余，否则为二次非剩余.

p 为奇素：

定理：1 模 p 简 $1,2,\cdots p-1$ 中，有 $\frac{(p-1)}{2}$ 模 p 二次：$\langle 1\rangle_p,\langle 2^2\rangle_p\cdots\langle(\frac{p-1}{2})^2\rangle_p$，有 $\frac{(p-1)}{2}$ 个模 p 二次非.

2. Euler判定：n 是二次剩余 $\Leftrightarrow n^{\frac{p-1}{2}}\equiv 1 \pmod p$

二次非 $\Leftrightarrow n^{\frac{p-1}{2}}\equiv -1 \pmod p$

勒让德：$\left(\frac{n}{p}\right)=\begin{cases}1 & \text{二次}\\ -1 & \text{二次非}\end{cases}$

p 奇，$(n,p)=1$.

$p>2$ 素：① $\left(\frac{n}{p}\right)=\left(\frac{n+p}{p}\right)$

② $\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}} \pmod p$

③ $\left(\frac{1}{p}\right)=1$

④ 当 $n\equiv 0 \pmod p$ $\left(\frac{n}{p}\right)=0$ ⇒ 勒让德完全积性

证：$\left(\frac{mn}{p}\right)=(mn)^{\frac{p-1}{2}}\equiv m^{\frac{p-1}{2}}n^{\frac{p-1}{2}}\equiv\left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right) \pmod p$.

⇒ $p\mid\left(\frac{mn}{p}\right)-\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ → 0或±2.

由 p 为奇素 ⇒ $\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right)$

⇒ 一般 $n=\pm 2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

则 $\left(\frac{n}{p}\right)=\left(\frac{\pm 1}{p}\right)\cdot\left(\frac{2}{p}\right)^{\alpha}\cdot\left(\frac{p_1}{p}\right)^{\alpha_1}\cdots\left(\frac{p_k}{p}\right)^{\alpha_k}$.

积性函数：

$(m,n)=1$，$f(mn)=f(m)\cdot f(n)$.

完全积性：

$\forall m,n$，$f(mn)=f(m)\cdot f(n)$.

3. $\forall$ 奇素 p：$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & p\bmod 4=1\\ -1 & p\bmod 4=3\end{cases}$

4. $\forall$ 奇素 p：$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & p=\pm 1 \pmod 8\\ -1 & p=\pm 3 \pmod 8\end{cases}$

证：$p=5$：$2\cdot 2\ \ 4\equiv 1\cdot(-1)$

$p=7$：$2\cdot 1\ \ 2\equiv 2\cdot(-1)^2$；$2\cdot 3\ \ 6\equiv 1\cdot(-1)$；$2\cdot 2\ \ 4\equiv 3\cdot(-1)^3$

一般 p：$2^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}$

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

5. 二次互反律，$p>2$，$q>2$ 而素 $p\neq q$：$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$

高斯引理：p 奇素，$(n,p)=1$，对 $\frac{(p-1)}{2}$ 个数：$\langle n\rangle_p,\langle 2n\rangle_p,\cdots\langle\frac{p-1}{2}\cdot n\rangle_p$.

其中有 m 个大于 $\frac{p}{2}$，那么 $\left(\frac{n}{p}\right)=(-1)^m$

艾森斯坦引理：p 是奇素，$(n,p)=1$，则 $\left(\frac{n}{p}\right)=(-1)^{T(n,p)}$，$T(n,p)=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{jn}{p}\right]$ 取整

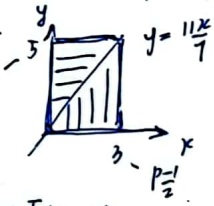
⇒ 只要 p 可存在一个 $4k+1$，$\left(\frac{n}{p}\right)=\left(\frac{q}{p}\right)$.

当 $p\cdot q=4k+3$，$\left(\frac{n}{p}\right)=-\left(\frac{q}{p}\right)$.

由艾森斯坦引理证二次互反律：

$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=T(p,q)+T(q,p)=\sum_x\left[\frac{qx}{p}\right]+\sum_y\left[\frac{py}{q}\right]$

p,q：$p=7$，$q=11$.



⇒ $T(p,q)+T(q,p)=\frac{p-1}{2}\cdot\frac{q-1}{2}$

雅可比符号：m 正奇，$m=p_1p_2\cdots p_t$，$(n,m)=1$，则 $\left(\frac{n}{m}\right)=\prod_{i=1}^{t}\left(\frac{n}{p_i}\right)=$

① 高斯引理不成立.

② $t=1$ 时，与勒让德性质作用

$t\neq 1$ 时，$\left(\frac{n}{m}\right)=-1$，$x^2\equiv n \pmod m$ 无解.

$\left(\frac{n}{m}\right)=1$，不一定有解.

定理：1. $n\equiv n_1 \pmod m$ $(n,m)=1\Rightarrow\left(\frac{n}{m}\right)=\left(\frac{n_1}{m}\right)$

$(n,m)=1=(n_1,m_1)\Rightarrow\left(\frac{n}{m}\right)\left(\frac{n}{m_1}\right)=\left(\frac{n}{mm_1}\right)$

$(n,m)=1=(n_1,m)\Rightarrow\left(\frac{n}{m}\right)\left(\frac{n_1}{m}\right)=\left(\frac{nn_1}{m}\right)$

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

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

4. m,n 正奇，$(m,n)=1\Rightarrow\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}$

应用：$n=pq$，$p\neq q$ 素.

$x^2\equiv a \pmod n$ 有解 $x\equiv x_0 \pmod n$，$(a,n)=1$.

↓

有四个不同余解.

第四章

算术函数：定义在所有正整数上.

定理：1. $(m,n)=1$. $\varphi(mn)=\varphi(m)\varphi(n)$. Euler是积性的.

2. $\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$

3. $\sum_{d|n}\varphi(d)=n$ eg $n=8$ $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(4)=1,2$, $\varphi(8)=1,3,5,7$ } 8个

高度合数：$n>1$. 对$\forall m<n$. 有$\tau(m)<\tau(n)$.

莫比乌斯反演：由下⇒下.

莫比乌斯函数：Mobius $\mu(n)\triangleq\begin{cases}1 & n=1\\ (-1)^s & l_1=l_2=\cdots=l_s=1\\ 0 & 某 l_j>1\end{cases}$

$n=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$ 乘性

定理：2. $\sum_{d|n}\mu(d)=\begin{cases}1 & n=1 \Leftrightarrow \mu(1)=1\\ 0 & n\neq 1\end{cases}$

证：$n=p_1p_2$. $d=1, p_1, p_2, n$.

$\mu(1)=1$ $\mu(p_1)=-1$ $\mu(p_2)=-1$ $\mu(n)=1$

$\Rightarrow \sum_{d|n}\mu(d)=0$.

法二：

$n=p_1^2p_2$ $d=1, p_1, p_1^2, p_1p_2, p_1p_2^2, p_2$.

1 −1 0 1 0 −1

$\Rightarrow \sum_{d|n}\mu(d)=0$.

定义：$F(n)=\sum_{d|n}f(d)$ n所有正因子在f处的和. F和函数

因子和函数：$\sigma(n)=\sum_{d|n}d$.

因子个数函数：$\tau(n)=\sum_{d|n}1$.

定理：1. f积性 ⇒ F积性.

引：$(m,n)=1$. t_1,t_2分别通过m,n全部因子

⇒ t_1t_2通过mn的全部因子.

推，$\sigma(n)$. $\tau(n)$都为积性.

引，$\sigma(p^\alpha)=1+p+p^2\cdots+p^\alpha=\frac{p^{\alpha+1}-1}{p-1}$

$\tau(p^\alpha)=\alpha+1$

2. $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\Rightarrow \sigma(n)=\prod_{j=1}^{k}\frac{p_j^{\alpha_j+1}-1}{p_j-1}$

$\tau(n)=\prod_{j=1}^{k}(\alpha_j+1)$

如果n为$\in\mathbb{Z}^+$且$\sigma(n)=2n$，n完全数

3. n偶完全数 $\Leftrightarrow n=2^{m-1}(2^m-1)$

$m\geq 2$, s.t. 2^m-1素. M_m

↳ m素.

证二：多项下也为积性的.

$F(p^\alpha)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^\alpha)$

$=1-1+0\cdots+0=0$

3. Mobius反演：$F(n)=\sum_{d|n}f(d)\Rightarrow f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})$

证：$\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(d)\cdot\sum_{e|\frac{n}{d}}f(e)=\sum_{e\cdot d|n}\mu(d)f(e)$

$=\sum_{e|n}\sum_{d|\frac{n}{e}}\mu(d)f(e)=\sum_{e|n}f(e)\sum_{d|\frac{n}{e}}\mu(d)\overset{e=n}{=}f(n)$

$\sum_{d|\frac{n}{e}}\mu(d)=\begin{cases}1 & e=n\\ 0 & 其他\end{cases}$.

推：$\frac{n}{e}\leftarrow d$ $\frac{e}{n}\leftarrow\frac{n}{d}$

$n=\sum_{d|n}\mu(\frac{n}{d})\sigma(d)$ $d\cdot e=n$

$1=\sum_{d|n}\mu(\frac{n}{d})\tau(d)$

4. F乘性 ⇒ f乘性.

第五章

次数(阶)：$(a,m)=1$，$a^l\equiv 1 \pmod m$，l为a模m的次数(阶) $\triangleq \mathrm{ord}_m a$

定理：1 $\mathrm{ord}_m a=l$，$a^n\equiv 1 \pmod m$ $n>0 \Rightarrow l\mid n$

推：a对模m次数l，则 $l\mid \varphi(m)$

2. $\mathrm{ord}_m a=l$，则 $1, a, a^2, \cdots a^{l-1}$ 两两不同余。

3. $(a,m)=1$，$m>0$：$a^i\equiv a^j \pmod m \Leftrightarrow i\equiv j \pmod{\mathrm{ord}_m a}$

4. $\mathrm{ord}_m a=l$，$\lambda>0$，$\mathrm{ord}_m a^\lambda=l_1 \Rightarrow l_1=\frac{l}{(\lambda,l)}$

推：$\mathrm{ord}_m a=l$，则 $\varphi(l)$个a^λ $(\lambda,l)=1$ 对模m也为l。

定理证明：一方面 $\mathrm{ord}_m a^\lambda=l_1 \therefore (a^\lambda)^{l_1}=a^{\lambda l_1}\equiv 1 \pmod m$

又$\because \mathrm{ord}_m a=l \therefore l\mid \lambda l_1$。

$\therefore \frac{l}{(\lambda,l)}\mid \frac{\lambda}{(l,\lambda)}\cdot l_1 \Rightarrow \frac{l}{(\lambda,l)}\mid l_1$ —(1)

另一方面：由 $\mathrm{ord}_m a=l$ 知：

$(a^\lambda)^{\frac{l}{(\lambda,l)}}=(a^l)^{\frac{\lambda}{(\lambda,l)}}\equiv 1 \pmod m$。

又$\because \mathrm{ord}_m a^\lambda=l_1 \therefore l_1\mid \frac{l}{(\lambda,l)}$ —(2)。

由(1)、(2) $\Rightarrow l_1=\frac{l}{(\lambda,l)}$

5. p素，如果$\exists a$，$\mathrm{ord}_p a=l$，则恰有$\varphi(l)$个模p不同余整数，对p次数均为l。

证明：由定2知 $a^0, a^1, a^2, \cdots a^{l-1}$ 两两不同余。—(1)

且它们都是 $x^l\equiv 1 \pmod p$ 的解。—(2)。

由Lagrange定理知(1)给出(2)的所有l个两两不同余解。

而(1)中恰有$\varphi(l)$个阶为l的数a^λ，$(\lambda,l)=1$

6. $l\mid p-1$，次数为l的模p互不同余的整数是$\varphi(l)$个。

与定万无别，但只有素p成立，$(g^u,m)=1$。

原根：$(g,m)=1$，$\mathrm{ord}_m g=\varphi(m)$

g^u两两不同余，$\mathrm{ord}_m g=\varphi(m)$ } $\Rightarrow$ 缩系

定理：1. $(g,m)=1$，g为模m原根 $\Leftrightarrow$ $g, g^2, \cdots g^{\varphi(m)}$ 组成模m缩系。

2. g为模m原根，m为>1：g^u为模m原根 $\Leftrightarrow (u,\varphi(m))=1$

3. m有一原根，则m共有$\varphi(\varphi(m))$个不同余原根。

证明：$\mathrm{ord}_m g=\varphi(m)$，$g, g^2, \cdots g^{\varphi(m)}$ 不同余。

$\mathrm{ord}_m g^u=l=\frac{\varphi(m)}{(u,\varphi(m))}$ ↗ 共有$\varphi(\varphi(m))$个u与$\varphi(m)$互素。

$\mathrm{ord}_m g=\varphi(m)$，$\mathrm{ord}_m g^u=\varphi'(m)$ } $\varphi'(m)=\frac{\varphi(m)}{(u,\varphi(m))}$

4. 素数p恰好有$\varphi(p-1)$不同余原根，$m=p$，$\varphi(m)=p-1$

5. m存在原根当且仅当 $m=2, 4, p^t, 2p^t$。 { r模p^t原根，r奇 $\Rightarrow 2p^t$原根。 … r偶 $\Rightarrow r+p^t$为$2p^t$原根。

6. $\forall k\geq 3$，5模2^k次数都为2^{k-2}

例：$2^x\equiv 1 \pmod 7$ 的解。

已知2模7的次数为3，则 $3\mid x$。

由定理3：令$i<j$。

$\Rightarrow$ 若 $a^i\equiv a^j \pmod m$

$a^{j-i}\equiv 1 \pmod m$

$\therefore \mathrm{ord}_m a\mid j-i$，即 $i\equiv j \pmod{\mathrm{ord}_m a}$

$\Leftarrow$ $i\equiv j \pmod{\mathrm{ord}_m a}$

设 $j\equiv q\,\mathrm{ord}_m a+i$

$a^j\equiv a^{\mathrm{ord}_m a\cdot q+i}\equiv a^i \pmod m$

模p^2的原根：到处有一个

$\because p$素奇，且有原根r $\Rightarrow$ r或$r+p$是p^2原根

模p^k的原根：

1. p奇素，$\forall k$，p^k均有原根。

2. 如r为p和p^2原根 $\Rightarrow r$为p^k原根。

模2^k的原根：

定理：a奇，对$k\geq 3$有：

$a^{\frac{\varphi(2^k)}{2}}=a^{2^{k-2}}\equiv 1 \pmod{2^k}$

推：对$\forall k\geq 3$，2^k无原根。

次数计算：

$(a,m)=1$，$m>0$，$\mathrm{ord}_m a=l \mid \varphi(m)$，则$\varphi(m)$的因子 $d_1, d_2 \cdots d_s$，通过 $a^{d_1}, a^{d_2} \cdots a^{d_s}$ 可计算 l。

定理：1. $m=p_1^{k_1} \cdots p_t^{k_t}$，$\mathrm{ord}_m a=[\mathrm{ord}_{p_1^{k_1}} a, \mathrm{ord}_{p_2^{k_2}} a \cdots \mathrm{ord}_{p_t^{k_t}} a]$

2. $\mathrm{ord}_{p^i} a=f_i \Rightarrow f_{i+1}=f_i$ 或 pf_i。

如果 $p^i \| a^{f_i}-1 \Rightarrow f_j=\begin{cases} f_2 & 2 \le j \le i \\ p^{j-i} f_2 & j>i \end{cases}$

e.g. $a=7$，$p=3$，求 f_{10}，$k p^2$

$f_2=\mathrm{ord}_{3^2} a=\mathrm{ord}_{48}7=2$　$7^2-1=48$

$2^4=16 \| 48$　$f_{10}=\begin{cases} f_2 & 2 \le j \le i \\ p^{10-4} \cdot f_2 & j>i. \ \checkmark \ 10>4 \end{cases}$

$=2^6 \cdot 2=2^7$

e.g. $a=2$，$m=45$。

$45=3^2 \cdot 5$。

$\mathrm{ord}_5 2=4$。

$\mathrm{ord}_9 2=6$

$[4,6]=12 \Rightarrow \mathrm{ord}_{45} 2=12$。

证明定理2：

第一部分：$a^{f_{i+1}} \equiv 1 \pmod{p^{i+1}}$

$\Rightarrow a^{f_{i+1}} \equiv 1 \pmod{p^i}$

$\therefore \mathrm{ord}_{p^i} a=f_i \mid f_{i+1}$

下面证 $f_{i+1} \mid p f_i$：$a^{pf_i}-1=(a^{f_i}-1)\sum_{k=0}^{p-1}(a^{f_i})^k$

$p^i \mid a^{f_i}-1$ ✓ $-(1)$.

$\Rightarrow \sum_{k=0}^{p-1}(a^{f_i})^k \equiv p \pmod{p^2} \Rightarrow \sum_{k=0}^{p-1}(a^{f_i})^k \equiv 0 \pmod p$，$p \mid \sum_{k=0}^{p-1}(a^{f_i})^k$ $-(2)$.

$a^{f_i}+a^{2f_i}+\cdots+a^{(p-1)f_i}$

$\downarrow \quad \downarrow \quad \cdots \quad \downarrow$

$1 \quad 1 \quad \cdots \quad 1$.

由 $(1),(2)$，知 $p^{i+1} \mid (a^{f_i}-1)\cdot\sum_{k=0}^{p-1}(a^{f_i})^k=a^{pf_i}-1$.

$\Rightarrow a^{pf_i} \equiv 1 \pmod{p^{i+1}}$

$\therefore f_{i+1}=\mathrm{ord}_{p^{i+1}} a \mid pf_i$　$f_{i+1} \ne f_i$

第二部分：$2 \le j \le i$，$f_j \mid f_i$

由 $p^i \mid a^{f_j}-1 \Rightarrow a^{f_j} \equiv 1 \pmod{p^j}$

$\therefore \mathrm{ord}_{p^j} a=f_j \mid f_i$.

① 当 $j \le i$：$f_j \mid f_i \mid f_i$，$\therefore f_j=f_i$.

② 当 $j=i+1$，$f_{i+1}=f_i$ 或 pf_i

若 $f_{i+1}=f_i=f_j=a^{f_j}=a^{f_{i+1}} \equiv 1 \pmod{p^{i+1}}$

则 $p^{i+1} \mid a^{f_j}-1$ 与 $p^i \| a^{f_j}-1$ 矛盾。定理：g 为 m 原根，$(a,m)=(b,m)=1$

$\therefore f_{i+1}=pf_i$

指数：

g 为 m 原根，$(n,m)=1$　p 为素 $\Rightarrow f_{i+1}=pf_i$ 或 f_i

必有唯一 k，$0 \le k < \varphi(m)$，s.t.：

$n \equiv g^k \pmod m$　$k=n$ 对模 m 指数 $=\mathrm{ind}_g n$（离散对数）

1. $\mathrm{ind}(ab) \equiv \mathrm{ind}a+\mathrm{ind}b \pmod{\varphi(m)}$

$\mathrm{ind}ab=k$　$ab \equiv g^k \pmod m$.

$\mathrm{ind}a+\mathrm{ind}b=k_1+k_2 \Rightarrow a \cdot b \equiv g^{k_1} \cdot g^{k_2} \pmod m$

$\therefore \mathrm{ind}ab \equiv \mathrm{ind}a+\mathrm{ind}b \pmod{\varphi(m)}$

2. $\mathrm{ind}a^n \equiv n\,\mathrm{ind}a \pmod{\varphi(m)}$

3. $\mathrm{ind}1=0$　$\mathrm{ind}g=1$

4. $\mathrm{ind}(-1)=\frac{\varphi(m)}{2}$　$m>2$.

5. g_1 也为 m 原根：$\mathrm{ind}_g a \equiv \mathrm{ind}_g g_1 \cdot \mathrm{ind}_{g_1} a \pmod{\varphi(m)}$

$g^{\varphi(m)} \equiv 1$.　$g^{\mathrm{ind}_g a} \equiv a \pmod m$

$g_1^{\varphi(m)} \equiv 1$.　$\equiv 1 \cdot g^{\mathrm{ind}_g g_1 \cdot \mathrm{ind}_{g_1} a}$

$\Rightarrow \mathrm{ind}_g a \equiv \mathrm{ind}_g g_1 \cdot \mathrm{ind}_{g_1} a \pmod{\varphi(m)}$

e.g. 解同余式：$3x \equiv 11 \pmod{13}$，13 原根为 2。

$\Rightarrow \mathrm{ind}(3x) \equiv \mathrm{ind}11 \equiv \mathrm{ind}3+\mathrm{ind}x \pmod{\varphi(13)}$

$7 \quad 4 \quad 3$.　$\Rightarrow x \equiv 8 \pmod{13}$

原根计算：

定理：$m>1$，$\varphi(m)$ 素因子为 $q_1, q_2 \cdots q_s$，$(g,m)=1$

g 为 m 原根 $\Leftrightarrow g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod m$

证明：$\Rightarrow$ 显然

$\Leftarrow$ 已知 $g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod m$，如果 g 非原：

设 $\mathrm{ord}_m g=d$，若 $d<\varphi(m)$.

$d \mid \varphi(m)$ 且 $\frac{\varphi(m)}{d}>1$.

$\therefore \exists\, 1 \le i \le s$，$q_i \mid \frac{\varphi(m)}{d}$

则令 $\frac{\varphi(m)}{d}=kq_i$

$\therefore \frac{\varphi(m)}{q_i}=kd$

$g^{\frac{\varphi(m)}{q_i}} \equiv g^{kd} \equiv$

与题设矛盾

2. a 对奇素 p 次数为 $d<p-1$.

$\Rightarrow a^\lambda$，$\lambda=1,2 \cdots d$ 都不为 p 原根。

$a^1, a^2 \cdots a^d$ 均不同余。

$a^d \equiv 1 \pmod p$.

a^λ 次数为 $\frac{d}{(\lambda,d)}<d$，更不可能为原根。

求 p 原根：列出 $1,2 \cdots p-1$.

取 $a=2$，计算 2 次数，若 $d=p-1$，2 为原

若 $d<p-1$，2 幂均非

再取其他，直到只剩下 $\varphi(p-1)$ 个数

对奇素，恰有 $\varphi(p-1)$ 个原根。

二项同余式：$x^k \equiv n \pmod m$

$k\,\mathrm{ind}x \equiv \mathrm{ind}n \pmod{\varphi(m)}$

定理：m 有原根 g，$(n,m)=1$，$x^k \equiv n \pmod m$ 有解

$\Leftrightarrow (k,\varphi(m)) \mid \mathrm{ind}n$，如有解，恰有 d 解

d.

群论：

群：非空集合 G 上定义运算 $(G,*)$.
① 非空.
② 封闭.
③ 结合律 $a*(b*c)=(a*b)*c$
④ 单位元 $e*a=a*e=a$.
⑤ 逆元 $a*b=e=b*a$
⑥ 交换 $\Rightarrow$ Abel群.

半群：① 非空 G.
② 二元运算 "$\cdot$" 封闭.
③ 结合律 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
不要求单位元逆元.

半群满足：① 单位元 e: $\forall a,\ a\cdot e=e\cdot a=a$.
② 逆元：$\forall a,\exists a^{-1}$, s.t. $a\cdot a^{-1}=a^{-1}a=e$

e.g: $(\mathbb{Z},+)$ $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$ Abel群
$(\mathbb{Z},\cdot)$ 非群，因为无逆元.
$(\mathbb{Q}^*,\cdot)$ $(\mathbb{R}^*,\cdot)$ $(\mathbb{C}^*,\cdot)$ 是群.

e.g 2: $\mathbb{Z}_n=\{0,1,\cdots n-1\}$ 关于模 n 加法群
单位元：0 逆元存在.

e.g: p 素，$F_p=\mathbb{Z}_p$，令 $F_p^*=F_p\setminus\{0\}$ 对模 p 乘法成群 $(\mathbb{Z}_p^*,*)$ p 阶系.

$|G|$: G 中元素个数 $=\begin{cases}|G|<\infty \text{ 有限群}\\ |G|=\infty \text{ 无限群}\end{cases}$

e.g: 置换群：A^A：A 上所有变换，$\circ$ 映射复合.
$(A^A,\circ)$ 是半群.
S：A 上可逆变换.
$(S,\circ)$ 成对称群.

$f=\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}$，$i_1,i_2\cdots i_n$：$n$ 级置换.
n 次置换.

e.g: 循环群 D_n $\rho_k(i)=k+i$ $k=i=0,1\cdots n-1$. $\rho_k=\rho_1^k$
$\tau_0=\begin{pmatrix}0&1&2&\cdots&n-1\\ 0&n-1&n-2&\cdots&1\end{pmatrix}$
$\tau_k(i)=k+n-i$ $k,i=0,1,2\cdots n-1$

e.g: $\mathbb{Z}_n\setminus\{0\}$ 关于模 n 乘法？
$\mathbb{Z}_n^*=\{a\mid a\in\mathbb{Z}_n,(a,n)=1\}$ 关于模 n 乘法成群.
$(a,n)=1$. $\mathrm{ord}_n a=d$，则 $a,a^2\cdots a^d$ 为 $\mathbb{Z}_n$ 循系.
$\langle a\rangle$ 为循环群，$|\langle a\rangle|=d$

e.g: 定义在数域 K 上全体 n 级可逆矩阵对矩阵乘成群.
→ 一般线性群，$\triangleq GL_n(K)$
特殊线性群：全体行列式 $=1$ 的群，为 $GL_n(K)$ 子群.

e.g: Klein四元群 与 $Z_8^*=\{1,3,5,7\}$ 同构

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

左(右)单位.
$(G,\cdot)$ 半群：1 $e_l\in G$. $\forall a$ 有 $e_l\cdot a=a$，e_l 为单位元.
2 $e_r\in G$ 同理.

定理：1. 半群有左右单位元，$e_l=e_r$.
2. $e=e_l=e_r$ 唯一.

生成群：循环群，$\langle S\rangle$：包含 S 的最小子群.
$\langle S\rangle=\bigcap_{i\in I}H_i$，$H_i$ 包含 S 的所有子群.
若 $S=\{a_1\cdots a_m\}$ 有限，$H=\langle a_1\cdots a_m\rangle$ 为有限生成群.
$G=\langle a\rangle$ 循环群.

群同构：$(G,\cdot)$，$(G',\circ)$ 两群. $f:G\to G'$
同态：$\forall a,b\in G$. $f(a\cdot b)=f(a)\circ f(b)$
同构：f 双射 ✓. 记 $G\cong G'$. Klein四元群

e.g: $(\mathbb{R}^+,\cdot)\cong(\mathbb{R},+)$ f：取对数.

e.g: $U_n=\{e^{\frac{2k\pi}{n}i}\mid k=0,1\cdots n-1\}$ 复数域 n 次单位根群与谁同构？
$(\mathbb{Z}_n,+)\to(U_n,\cdot)$ $k\mapsto e^{\frac{2k\pi}{n}i}$ 取对数

群的性质：1. 半群是群 $\Leftrightarrow$ $ax=b$，$ya=b$ 有解.
2. 有限半群是群 $\Leftrightarrow$ 左右消去律成立.

定理：1. $(G,\cdot)$ 群，S 非空，$S\subseteq G$. 由 S 生成子群：
$\langle S\rangle=\{a_1^{r_1}a_2^{r_2}\cdots a_{t+1}^{r_{t+1}}\mid a_i\in S,r_i\in\mathbb{Z},t\in\mathbb{N}\}$.
$D_n=\langle\rho_1,\tau_0\rangle$ $\langle a\rangle=\{a^k\mid k\in\mathbb{Z}\}$.
$H_m=\{mk\mid k\in\mathbb{Z}\}$. $H_m=\langle m\rangle$ $(\mathbb{Z},+)=\langle 1\rangle$.
$(\mathbb{Z}_n,+)=\langle\bar{1}\rangle$ $(\mathbb{Z}_p^*,\cdot)$

循环群性质：定理 2：$(G,\cdot)=\langle a\rangle$ 生成元 1，-1.
① $o(a)=\infty$ $G\cong(\mathbb{Z},+)$ 无限循环群. 生成元 $(a,n)=1$
② $o(a)=n$. $G\cong(\mathbb{Z}_n,+)$. n 阶循环群. 记 C_n
e.g: $(\mathbb{Z}_n^*,\cdot)=\langle g\rangle$ → 原根. $o(g)=\varphi(n)$
$(\mathbb{Z}_n^*,\cdot)\cong(\mathbb{Z}_{\varphi(n)},+)$
所有生成元为 $(a,\varphi(n))=1$，共 $\varphi(\varphi(n))$ 个.

g^n
③ 循环群子群循环：$\begin{cases}(\mathbb{Z},+):H_m=\langle m\rangle & m=0,1,2m\\ (\mathbb{Z}_n,+):\langle 0\rangle,\langle d\rangle, & d\mid n\end{cases}$

变换群：A上所有可逆变换 = A上对称群.
对称群的所有子群：变换群.

置换群：$|A|=n$. A上对称群为n次对称群：S_n.
S_n子群：n次置换群

轮换：$\{a_1 \cdots a_l\} \subseteq \{1,2,\cdots,n\}$, n级置换r满足：
$r(a_1)=a_2 \quad r(a_2)=a_3 \cdots r(a_l)=a_1$
$r(a)=a \quad a\in\{1,2\cdots n\}\setminus\{a_1\cdots a_l\}$
r为一长度为l的轮换，记$r=(a_1\ a_2 \cdots a_l)$
$l=2$：对换 $l=1$：单位元

陪集：$(G,\cdot)$群. $H\le G$子群. $a\in G$：
$aH=\{ax \mid a\in G, x\in H\}$ 为H左陪集. Ha为右..
e.g.：$(Z,+)$. H_m左右陪集相同 模m剩余类
e.g.：F上所有n维向量对加法成群. $A_{m\times n}X=0$ 解空间H是其子群.
H的陪集：$AX=0$. 解 $X=H$.
$AX=b$. 特解α. 则H陪集 $\alpha+H$.
e.g.：S_3子群 $H=\{(1),(1\ 2)\}$.
$(1\ 3)H$. $H(1\ 3)$ $(1\ 2\ 3)H$.

模H同余：同一陪集中，每个元素都可作为代表元.
性质：① $aH=H \Leftrightarrow a\in H$. $\forall h\in H$. $ah=h'\in H$. $a\in H$.
② $aH=bH \Leftrightarrow b\in aH$ $ah=bh' \Rightarrow b=ahh'^{-1}\in aH$
③ 两陪相等：$aH=bH \Leftrightarrow a^{-1}b\in H$ $ah=bh' \Rightarrow h=a^{-1}bh'$
$Ha=Hb \Leftrightarrow ba^{-1}\in H$ 同理.
④ $\forall a,b$ 有 $aH=bH$ 或 $aH\cap bH=\phi$
$\therefore S^L=\{a_i \mid i\in I\}$ 是H左完全代表元系，则$\{aH \mid a\in S^L\}$是G一划分.
$G=\bigcup_{a\in S^L} aH$. 类似可定S^R.
证：若$aH\cap bH\ne\phi$ $\exists x\in aH\cap bH$.
$\exists h_1,h_2\in H$, s.t. $ah_1=bh_2$
$\therefore b=ah_1h_2^{-1}\in aH$ $\therefore bh_3=ah_1h_2^{-1}h_3$，即$bH=aH$.
⑤ H确定G上两等价关系：$\sim_L$：$a\sim_L b \Leftrightarrow a^{-1}b\in H$
$\sim_R$：$a\sim_R b \Leftrightarrow ba^{-1}\in H$

陪集指数：$[G:H]$
H左右陪集的个数.
定理：1. $H\le G$.
$S_L=\{aH \mid a\in G\}$
$S_R=\{Ha \mid a\in G\}$.
存在S_L到S_R的双射.

商集：$G/\sim_L=\{aH \mid a\in S^L\}$.
$G/\sim_R=\{Ha \mid a\in S^R\}$.
e.g.：$Z/H_m=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}$.
定理2：$|G|<+\infty$. 可设$[G:H]=m$
$\therefore \exists a_i, 1\le i\le m$ s.t. $G=\bigcup_{i=1}^{m} a_iH$ ← a_i个数
令f：$H\to a_iH$ $\therefore |a_iH|=|H|$ $\therefore |G|=m|H|$

2. Lagrange：$|G|<\infty$, $H\le G$. 则$|G|=|H|\cdot[G:H]$
推：① $|H| \mid |G|=m|H|$ ② $\forall a\in G$. $o(a)\mid |G|$, $a^{|G|}=e$ ③ $|G|=p$
证明由①知$|H|=1$或p：1, a, … 模p同余 ⟹ $G=C_p$

对称群 子 变换群
$|A|=n$ ↓ $|S_n|=n!$ ↗
n次对称群S_n 子 置换群. e.g.：二面体群D_n
子：S=偶 ⟶ A_n(σ偶置换)：n次交错群.

① 每个置换都能写成不相交轮换之积.
② 轮换的阶 = 轮换长度l.

定理：1 σ：n次置换，$\sigma=r_1r_2\cdots r_k$（不考虑顺序是唯一的）
$o(r_i)=l_i$ 则 $o(\sigma)=[l_1,l_2,\cdots,l_k]$

2 σ分解为对换之积：$\sigma=\pi_1\pi_2\cdots\pi_s$ 不要求相交
s奇偶由σ唯一确定，与分解无关. 不一定唯一.
证：定义$D(x_1\ x_2\cdots x_n)=\prod_{i<j}(x_i-x_j)=(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)$
$(x_2-x_3)\cdots(x_2-x_n)$
$\cdots$
$(x_{n-1}-x_n)$
$D(x_1x_2x_3)=(x_1-x_2)(x_1-x_3)(x_2-x_3)$
$\forall$ n级置换σ, $\sigma(D)\triangleq(x_{\sigma_1}\ x_{\sigma_2}\cdots x_{\sigma_n})$
$=\prod_{i<j}(x_{\sigma_i}-x_{\sigma_j})=\pm D$.

$\sigma(1\ 2\ 3)=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ ← 对换两次
$\sigma(D)=(x_2-x_3)(x_3-x_1)(x_1-x_2)=D$.

π为对换. 则$\pi(D)=-D$. $\pi=\begin{pmatrix}1&2\cdots&i\cdots&j\cdots&n\\1&2\cdots&j\cdots&i\cdots&n\end{pmatrix}$
对$\forall$轮换σ. $\sigma(D)$定值
若$\sigma=\pi_1\pi_2\cdots\pi_s$，则$\pi_1\pi_2\cdots\pi_s(D)$定值
且$\pi_1\pi_2\cdots\pi_s(D)=(-1)^sD$ 由s奇偶决定
{ s为偶：偶置换（动奇数个数）
{ s为奇：奇..（动偶个数）
$|A_n|=\frac{n!}{2}$
$A_n\le S_n$
F所有n次偶置换构成的集合：n次交错群：A_n
因为偶复合为偶.

3. Cayley定理：$\forall$群 $\cong$ 变换群
$\forall$有限群 $\cong$ 置换群.
e.g.：与Klein四元群同构的置换群：
e, $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$.
a b c
e.g.：$S_n=\langle(1\ 2),(1\ 3),(1\ 4),\cdots(1\ n)\rangle$

证：$|A_n|=\frac{n!}{2}$ 对于$(1\ 2\cdots n)$有n!种排列. 偶置换产生的$\frac{n!}{2}$种
因为换一次样出现一逆序. 而在所有排列中逆序…

e.g: 确定S_3所有子群. $|S_3|=3!=6$ 因子: 1, 2, 3, 6

二阶: $\langle(12)\rangle$ $\langle(13)\rangle$ $\langle(23)\rangle$

三阶: $\langle(123)\rangle$ $\langle(132)\rangle$.

e.g: 证明 $|A_n|=\frac{n!}{2}$. $[S_n:|A_n|]=2$ A_n有两个陪集

只需证 $\forall$两奇换, $\sigma_1 A=\sigma_2 A \Leftrightarrow \sigma_2^{-1}\sigma_1 A=A \Leftrightarrow \sigma_2^{-1}\sigma_1\in A$

定理: $A,B\le G$. $|A|\cdot|B|<\infty \Rightarrow |AB|=\frac{|A|\cdot|B|}{|A\cap B|}$

e.g: 证明 Euler: $(a,n)=1$. $\forall a\in\mathbb{Z}_n^*$. $o(a)\mid\varphi(n)$

$\overset{kd}{\overset{\|}{}}$

要么 $o(a)=1$, 要么 $o(a)=\varphi(n)$ 同数 $d \Rightarrow a^{\varphi(n)}=e\equiv e\pmod{dn}$

补: 子群: $S\subseteq G$ e.g: $H_m=\{mk\mid k\in\mathbb{Z}\}$. $H_m\le(\mathbb{Z},+)$.

定理: 1 $H\le G\Leftrightarrow \forall a,b\in H$. 有 $a^{-1}b\in H$. (或 ab^{-1})

若有限, 则只需 $ab\in H$.

2. ① $H_1\le G$. $H_2\le G\Rightarrow H_1\cap H_2\le G$.

② $H_1\cup H_2\le G\Leftrightarrow H_1\le H_2$ 或 $H_2\le H_1$.

③ $H_1H_2\le G\Leftrightarrow H_1H_2=H_2H_1$

$o(a)=n$, $a^n=e$: n为所. (不存在, 则a为无限阶元)

3. 元素阶|群阶; $a^m=e\Leftrightarrow o(a)\mid m$

① $o(a)=\lambda$. $o(a^k)=\frac{\lambda}{(k,\lambda)}$

② $o(a)=m$, $o(b)=n$, 若 $(m,n)=1$ 且 $ab=ba$, 则 $o(ab)=mn$

一方面: $o(ab)=\lambda$ $(ab)^\lambda=e$

$(ab)^{mn}=(ab)\cdot(ab)\cdots(ab)=a^{mn}b^{mn}=e$

$\therefore \lambda\mid mn$.

另一方面: $e=(ab)^{\lambda m}=a^{\lambda m}b^{\lambda m}=b^{\lambda m}$

则 $o(b)=n\mid\lambda m$, $n\mid\lambda$

同理得 $m\mid\lambda$, $(m,n)=1$ $\Rightarrow mn\mid\lambda$

$\therefore \lambda=mn$.

单群: $G\neq\{e\}$, 除本身与e外元素地正规子群, 称G为单群.

e.g: p素, $(\mathbb{Z}_p,+)=C_p$ 交换群中单群必有C_p这一类.

e.g: n次交错群A_n $(n\ge5)$是单群.

群同态: $(G,\cdot)$, $(G',\circ)$ $f:G\to G'$ 满足:

$\forall a,b\in G$. 有 $f(a\cdot b)=f(a)\circ f(b)$ f为$G\to G'$同态.

f单射: 单同态 f满射: 满同态、f双射: 同构.

e.g: 1): $f:(\mathbb{R},+)\to(\mathbb{R},+)$. $x\to -x$.

2): $f:(\mathbb{Z},+)\to(\mathbb{Z}_n,+)$ $k\to\langle k\rangle_n$

3): $H\le G$. $f:G\to G/H$ $a\to aH$

同态性质: 1. 单位元 5. $N\le f(G)\Rightarrow f^{-1}(N)\le G$ } 关于子群. 正规可通

2. 逆元 6. $N\trianglelefteq f(G)\Rightarrow f^{-1}(N)\trianglelefteq G$ }

3. 子群 7. $o(a)<\infty\Rightarrow o(f(a))\mid o(a)$ ($\in G'$, $\in G$)

4. 正规子群 H.

正规子群: $H\trianglelefteq G$: $\forall g\in G$ 有 $gH=Hg$. 其中 $H\le G$.

e.g: 1) 1阶子. G的子群是G的正规子群. 陪集指数为$|G|$和1.

2). $H\le G$. 若 $[G:H]=2$. 则 H 是 G 正规子群.

3). 若 G 交换, 则 G 所有子群均为正规子群.

判定: 1. $\forall a\in G$. 有 $aH=Ha$.

$H\le G$. 2. $\forall a\in G$. $h\in H$. 有 $aha^{-1}\in G$

3. $\forall a\in G$. 有 $aHa^{-1}\subseteq H$.

4. $\forall a\in G$. 有 $aHa^{-1}=H$.

1)⇒2)

2)⇒3): 显然

3)⇒4):

$\forall a\in G$. $a^{-1}\in G$ $aHa^{-1}\subseteq H$ *2

$\therefore H\le aHa^{-1}$ *1

由*1, *2 ⇒ $aHa^{-1}=H$.

4)⇒1): 显然,

若 $aHa^{-1}=H\Rightarrow aH=Ha$

商群: $H\trianglelefteq G$. 定义商集: $G/H=\{aH\mid a\in G\}$

$=\{Ha\mid a\in G\}$

定理: 1 $H\trianglelefteq G$. G/H 对于集乘法成群, → 商群

e.g: $H_m\trianglelefteq\mathbb{Z}$. $\mathbb{Z}/H_m=\{\bar0,\bar1,\bar2,\cdots,\overline{m-1}\}\cong\mathbb{Z}_m$

3. $(G,\cdot)$ 有限交换群. p为素. $p\mid|G|$, 则 G 中有 p 阶元

证: $|G|=p$. 结论成立. $G=C_p$

假设 $|G|<n$. 且 $p\mid|G|$ 时有 p 阶元. 下面证 $|G|=n$ 时成立

取 $a\in G$. $a\neq e$. 设 $o(a)=k$.

若 $p\mid k$, 则 $o(a^{\frac{k}{p}})=p$ 阶 $=\frac{k}{(k,\frac{k}{p})}=p$

若 $p\nmid k$, 因 $p\mid n$, $p\mid n$

所以 $p\mid k\mid n\Rightarrow p\mid\frac{n}{k}$ $\frac{k}{p}$ 主要为了该元 世是G中p阶元

令 $H=\langle a\rangle$. $|H|=k$. 则 $|G/H|=\frac{n}{k}$

由归纳假设, G/H 中含有 p 阶元. 记作 $\bar c$ $o(\bar c)=p$ G/H

$(cH)^p=c^pH^p=c^pH=H$ 即 $c^p\in H$.

由 $|H|=k$ 知 $|c^p|^k=(c^k)^p=e$ $\therefore o(c^k)_G=p$ 或 1.

且 $c^k\neq e$. 否则有 $c^kH=(cH)^k=(\bar c)^k=H$.

那么 $o(\bar c)=p\mid k$. 与 $p\nmid k$ 矛盾

$\therefore o(c^k)=p$.

群同态基本定理：　$\ker f$ = f 的核 $f^{-1}(e') = \{a \mid a \in G, f(a) = e' \in G'\}$ 核是单位元 (G') 的原像

$f: G \to G'$，设 $\ker f = K$.

① $K \trianglelefteq G$.

② $\forall a \in \mathrm{Im} f$，若 $f(a) = a'$，$f^{-1}(a') = aK$. $f(aK) = f(a) \circ f(K) = a' \circ e' = a'$

③ f 为单同态 $\Leftrightarrow K = \{e\}$

eg: $f: (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$.

$a \xrightarrow{f} a \bmod n$

φ ↘ $a+\mu_m$ ↗ δ

2、$f: G \to G'$ 满，设 $\ker f = K$.

① $\delta: G/K \to G'$ $\Rightarrow \delta$ 是同构. $\delta(a_1K \cdot a_2K) = \delta(a_1 K K a_2) = \delta(a_1 a_2 K) = f(a_1 a_2)$

$aK \to a' = f(a)$

$G \to G'$ ‖

$f(a_1) \cdot f(a_2)$

‖ ‖

$\delta(a_1K) \cdot \delta(a_2K)$

② φ 为 $G \to G/K$ 自然同态，$\exists\, G/K \xrightarrow{\delta} G'$ 使 $f = \delta\varphi$

G ↘ φ 满，G/K $\xrightarrow{f\text{满}}$ G' ↗ δ 同构.

环论：

环：$(A,+,\cdot)$

① $(A,+)$ 交换群.

② $(A,\cdot)$ 为半群.

③. 分配律：$a(b+c)=ab+ac$.
$(b+c)a=ba+ca$

除环：对乘法交换：域.
含乘法单位元：幺环.

特殊元素：

①. 零元：加法0. ③. 单位元：乘法1. $0\cdot a=a\cdot 0=0$

② 负元：加法逆 ④ 逆元：乘法逆 ← 0无逆元.

⑤. 单位正则元：乘法可逆元

⑥ 零因子：$ab=0$ 但 $a,b\neq 0$ a：右零因子. a为右零因子.
b：右零因子. 只要 $a\neq 0,\exists b\neq 0$, s.t. $ab=0$

环类：①. 整环：无零因子. 交换幺环. (乘法可交换. 有1. 无零因子)

② 除环：环内必有非0元. 非0元必有逆元. 有单位元. 关于乘法成群 $(A^*,\cdot)$
$(A^*,\cdot)$ 成群 ↳ 行不行! ↳ 乘法有逆 ↳ 乘法1.

③. 域：同时为整环. 除环. (乘法可交换. 有1. 有逆. 无零因子)

conclusion：剩余类环 $\mathbb{Z}_n$ 为域 $\Leftrightarrow$ n素. $(A^*,\cdot)$ 为交换群.
无零因子.

子环：$S\subseteq A$ (子环)， 子集和：$S+T=\{x+y\mid x\in S, y\in T\}$.

条件：1. $a,b\in S$. $a-b\in S$.
2. $a,b\in S$. $ab\in S$.

积：$ST=\{\sum xy\mid x\in S, y\in T$ 有限和$\}$.

理想：$I\subseteq A$. $(I,+)$ 为 $(A,+)$ 正规子群
关于加法成交换群.

定义：I为A子环：
1. $\forall x\in I, a\in A, ax\in I$，即 $aI\subseteq I$，I为A右理想
2. $\forall x\in I, a\in A, xa\in I$，即 $Ia\subseteq I$，I为A右理想
} ⇒ 理想.

说明：① 0子. 子的交A理想.
② A交换. 右ideal=右ideal
③. 环A非零I为理想. I子集：$\forall a,b\in I, a-b\in I$. — 子环.
$\forall x\in I, a\in A, ax, xa\in I$ — 理想.

④. 环A有单位元. I为理想：$1\in I\Leftrightarrow I=A$
⑤. 理想交. 和. 积也为理想. 吸收

吸收：$AI\subseteq I$. $IA\subseteq I$.

理想：对环吸收的子环.

正规子群：对群交换的子群.

生成子环：包含S最小子环 $[S]$.

生成理想：包含S最小理想 (S).

e.g：环A=Z所有可能的理想=(n).
$(12)\subset(6)\subset(2)\subset(1)=\mathbb{Z}$.
可定义整除. 因子. 带余除法
主理想整环. 所有理想为主理想
唯一因子分解整环.

e.g：F域. F[X]中X生成理想为：多项式环.

吸收
$(1)=A$.

$[a]=\{\sum n_k a^k\mid n_k\in\mathbb{Z}, k\in\mathbb{Z}^+\}$.

$(a)=\{\sum(kxy+sa+at+na)\mid x,y,s,t\in A, n\in\mathbb{Z}\}$
主理想.

A有单位元. 可交换：$(a)=\{xa\mid x\in A\}=Aa=aA$

商环：$\{x+I\mid x\in A\}$ A模I同余

① 数环：$(\mathbb{Z},+,\cdot)$. $(\mathbb{Q},+,\cdot)$. $(\mathbb{R},+,\cdot)$.

② 高斯环：$\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$ 成环.

③. 模n剩余类环.

④ 全矩阵环 $M_n(\mathbb{Z})$. $M_n(\mathbb{Q})$. $M_n(\mathbb{R})$

⑤. 多项式环 $\mathbb{Z}[x]$. $R[x]$.

e.g：I既右零因子 $\Leftrightarrow$ 右消去律成立.

⇒：反证. 设知 $a\neq 0$，非右零因子.
当 $ab=ac$
$a(b-c)=0$
$\Rightarrow b=c$
∴ 右消成立.

⇐：右消成立：
任给 $a\neq 0$，且 $ab=0$
∴ $ab=a\cdot 0$
由右消 $\Rightarrow b=0$

e.g：除环非域：Hamilton四元数
$H=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{R}\}$
乘法不满足交换律.

关于有限环：

①. A为非零有限环：A为除环 $\Leftrightarrow$ A无零因子.

② 有限整环一定为域（一定有逆元）

注①：A非零有限环，$(A^*,\cdot)$ 成半群
$\Leftrightarrow$ 左右消去律成立 $\Leftrightarrow$ 无左右零因子.

注②：A整环. 无零因子. 交换幺环
有限 ⇒ A为除环 ⇒ $(A^*,\cdot)$ 成群 ⇒ A为域.

同态：$f: A \to A'$ 满足：

① $f(a+b) = f(a) + f(b)$

② $f(ab) = f(a) f(b)$

f 首先为加法群同态。

加法群同态核：$0' \in A'$ 的全原像，称 f 核。

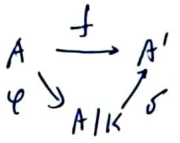
f 为单同态：$\ker(f) = \{0\}$。

环同态定理：

$f: A \to A'$ 满 $\Rightarrow$ I. $K = \ker(f)$ 是 A 理想。

II. $\delta: A/K \to A'$ 为环同构。

$a+K \to f(a)$



III. 自然同态 $\varphi: A \to A/K \Rightarrow f = \delta\varphi$

$a \to a+K$.

环 → 域：

回顾：极大理想：不含于自身的最大集合的理想（路标）

I 为理想，$J \supset I$ 时必有 $J = A$，则 I 为极大 ideal。（I 非平凡，故 $I \neq 0$）

整数环理想 $(p) = pZ$ 为极大理想。

$Z \to Z_p$：定理：A：交换环（乘法可交换，有1元），M 为 A 极大理想，则 A/M 域。

eg：$Z/(p)$。

F 域，$F(x)/(p(x))$，$p(x) \in F(x)$ 为不可约多项式。

扩大：构造分式域

eg：$Q = \{b/a \mid a, b \in Z, a \neq 0\}$ ← 包含 Z 最小域。 $P(F[x]) = \{f(x)/g(x) \mid f(x), g(x) \in F[x], g(x) \neq 0\}$

定理：无零因子交换环（可以无乘法1元），则它含 0 的最小域为 $P = \{b/a \mid a, b \in D$ 且 $a \neq 0\}$，$\cong P(D)$