1. 孙中国剩余

引理: $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$ 有解充要 $(m_1, m_2) \mid (b_1 - b_2)$

且若有解 x^+ 通解 $x \equiv x^+ \pmod{[m_1, m_2]}$

有解: $x = k_1 m_1 + b_1 = k_2 m_2 + b_2$

$k_1 m_1 - k_2 m_2 = b_2 - b_1$ 解充要: $(m_1, m_2) \mid (b_1 - b_2)$

寻找一组 k_1, k_2 $d = (m_1, m_2)$

$k_1 = \frac{b_2 - b_1}{d} \lambda_1$ $\frac{m_1}{d}\lambda_1 - \frac{m_2}{d}\lambda_2 = 1$

$k_2 = -\frac{b_2 - b_1}{d}\lambda_2$

$x = b_1 + (b_2 - b_1)\lambda_1 \frac{m_1}{(m_1, m_2)}$

下说明 $[m_1, m_2]$ 完系内仅有一解:

若否 $0 \le x, y < [m_1, m_2]$

$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$ $\begin{cases} y \equiv b_1 \pmod{m_1} \\ y \equiv b_2 \pmod{m_2} \end{cases}$

$\rightarrow \begin{cases} x \equiv y \pmod{m_1} \\ x \equiv y \pmod{m_2} \end{cases} \rightarrow x \equiv y \pmod{[m_1, m_2]}$

3元形式 有解 必要：任意两个有解 必要

充分：

$x \equiv x^* \pmod{[m_1, m_2]}$

$x \equiv b_3 \pmod{m_3}$

$x^* = b_1 + \frac{b_2 - b_1}{(m_1, m_2)} \lambda_1 m_1 = b_2 - \frac{b_2 - b_1}{(m_1, m_2)} \lambda_2 m_2$

$b_1 \equiv x^* \pmod{m_1}$

$b_2 \equiv x^* \pmod{m_2}$

又 $b_1 \equiv b_3 \pmod{(m_1, m_3)}$ $\quad b_3 \equiv x^* \pmod{(m_1, m_3)}$

$b_2 \equiv b_3 \pmod{(m_2, m_3)}$ $\quad b_3 \equiv x^* \pmod{(m_2, m_3)}$

① $(a, [b, c]) = [(a, b), (a, c)]$

proof: L, R 证相等，就证 $L \mid R$ & $R \mid L$

1) $R \mid a$ (显)

2) $(a, b) \mid b \mid [b, c]$ 故 $R \mid [b, c] \Rightarrow R \mid L$

3) $b / \gcd(b, c) = m$

$c / \gcd(b, c) = n$

$\mathrm{lcm}(b, c) = mc = bn$

$L = (a, bn) = (a, b) \cdot (a, n)$ $\quad (a, b) \mid (a, b)$

$(a, n) \mid (a, c)$

$L \mid R$

→ 得证

2. 与辗转相除联系

(1) 结束：$d_n' = (a,b)$ $x_n' = \frac{d_n'}{p}$ $y_n' = 0 = b_n$

b_{n-1}

$$\begin{cases} x_{n-1}' = y_n' \\ y_{n-1}' = x_n' - L\frac{a_{n-1}}{b_{n-1}}\rfloor y_n' \\ d_{n-1}' = x_{n-1}' a_{n-1} + y_{n-1}' b_{n-1} = gcd(a_{n-1}, b_{n-1}) \end{cases}$$

$\rightarrow$ $d = xa + yb = gcd(a,b)$

(2). 辗转相除法次数.

在 $a > b$ 时 a 模 b 余数 $< \frac{a}{2}$

$a < b$ 时 多算一次

3 (a) 缩系成对 < 存在 / 唯一

$(a,n)=1$　n 缩系 $\{n_1 \cdots n_{\varphi(n)}\}$

$an_1 \cdots an_{\varphi(n)}$ 仍缩 . ~~[illegible]~~ 的缩系

$\rightarrow \exists\ ab\equiv 1 \pmod n$

$ab_1 \equiv ab_2 \pmod n$　a, b_1, b_2 都和 n 互素.

$n \mid b_1 - b_2$　不同 $\in [n]$

(b) $x>0$　$a^{sx} \equiv 1 \pmod n$

$x=0$　$a^{sx} = 1 \equiv 1 \pmod n$

$x<0$　$a^{sx} \cdot a^{-sx} \equiv 1 \pmod n$

$a^{-sx} \equiv 1 \pmod n$　1 和 1 配对

$a^{sx} \equiv 1 \pmod n$

r ✓

~~教上 考虑降的情~~ 这里提出阶概念后更显，即 C.

(c) 若 $d \mid m$　✓

若 m　$a^m \equiv 1 \pmod n$　$m = kd + r$　$0 \le r < d$

$a^r \equiv 1 \pmod n$　$r < d$　矛盾

4. $a^{\varphi(n)/d} = a^{\frac{p-1}{d}(q-1)} \equiv 1 \pmod{q}$

$= a^{\frac{q-1}{d}(p-1)} \equiv 1 \pmod{p}$

$\rightarrow a^{\varphi(n)/d} \equiv 1 \pmod{pq} \equiv 1 \pmod{n}$

5. 6, 5

6. 推 (m, n) 的情況 呀

7. (a) $\forall z_1, z_2 \in \mathbb{Z}[\sqrt{-1}]$ $z_1 = a+b\sqrt{-1}$ $z_2 = c+d\sqrt{-1}$

$z_1+z_2 \in \mathbb{Z}[\sqrt{-1}]$

$z_1 z_2 \in \mathbb{Z}[\sqrt{-1}]$

$-z_1 \in \mathbb{Z}[\sqrt{-1}]$

$0, 1 \in \mathbb{Z}[\sqrt{-1}]$

(b). z_1, z_2 整 $z_1 = a+b\sqrt{-1}$ $z_2 = c+d\sqrt{-1}$

$z_1 z_2 = (ac-bd) + (ad+bc)\sqrt{-1} = 1$

$a, b, c, d \in \mathbb{Z}$

$$\begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases}$$

$d=0$ 时 $bc=0$ $ac=1$ $b=0$ 且 $ac=1$ $a, c = \pm 1$

$d \neq 0$ 时 $a = -\frac{bc}{d}$

$c=0 \rightarrow a=0$ $bd=1$ ± 1

$c \neq 0$ $a = \frac{-bf}{d} = \frac{1+bd}{c}$

$b(c^2+d^2)+1=0$ $cd \neq 0$ 矛盾

(d) $2=(1+\sqrt{-1})(1-\sqrt{-1})$ ∴ 不可约

∴ 非元一定不可约 故 不可逆元

(c) $p_i \mid q_1 \cdots q_k \to p_i \mid q_j$

$q_i \mid p_1 \cdots p_l \to q_i \mid p_j$

假设 $p_1 p_2 \mid q_m$ 则因 q_m 不可约

两边做 $k \le l$ $k \ge l$ $\Rightarrow k=l$

唯一分解要求且 非元一定不可约

非元一定不可约

不可约 $\to p_i = \varepsilon_i q_i$

8. (a) $a+b\sqrt{-5}$ 单位

$b=0$ 时 $\frac{1}{a}$ 在 $\mathbb{Z}$ 中 $(a \neq \pm 1)$

$b \neq 0$ 时 $\frac{1}{a+b\sqrt{-5}} = \frac{a-b\sqrt{-5}}{a^2+5b^2}$ 在 $\mathbb{Z}[\sqrt{-5}]$ 中

$$\text{要} \begin{cases} \frac{a}{a^2+5b^2} \in \mathbb{Z} \\ \frac{-b}{a^2+5b^2} \in \mathbb{Z} \end{cases} \quad \begin{array}{l} a > a^2+5b^2 \\ b > a^2+5b^2 \end{array} \quad ab \neq 0 \text{ 时矛盾}$$

(b) $(a+b\sqrt{-5})(c+d\sqrt{-5})=2$

$|\ |\ |\ |=2$

$|\ |^2 |\ |^2 = 4$

$(a^2+5b^2)(c^2+5d^2)=4$ 无解

$2 \mid (1+\sqrt{-5})(1-\sqrt{-5})=6$.