

1. (15pt) 考虑同余方程组

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

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

$$x \equiv b_3 \pmod{m_3}$$

其中, 对任意 $i \in \{1, 2, 3\}$, $b_i, m_i \in \mathbb{N}^+$ 。给出该同余方程组有解的充分必要条件并证明。(注意 m_1, m_2, m_3 两两互素只是有解的充分条件。)

充要条件: $\forall i, j \in \{1, 2, 3\}$, 有

$$b_i \equiv b_j \pmod{(m_i, m_j)}$$

证明:

① " \Leftarrow "

若 $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{(m_1, m_2)} \\ x \equiv b_2 \pmod{(m_1, m_2)} \end{cases} \Rightarrow b_1 \equiv b_2 \pmod{(m_1, m_2)}$

同理: $i=2, j=3$ 和 $i=1, j=3$ 时也可证得

② " \Rightarrow " ①

用到知识点: 同余的整除性质

(根据整除的传递性得到)

6. 整除性质: 若 $d | m$ 且 $a \equiv b \pmod{m}$, 则 $a \equiv b \pmod{d}$ (因为 $d | m | (b-a)$)

2. (15pt) 考慮如下算法：

EXTENDED-EUCLID(a, b)

- (a) if $b = 0$
- (b) then return $(a, 1, 0)$
- (c) $(d', x', y') = \text{EXTENDED-EUCLID}(b, a \bmod b)$
- (d) $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
- (e) return (d, x, y)

證明：

- (a) 輸出結果 (d, x, y) 滿足 $d = ax + by$ 。
- (b) 上述算法至多調用函數 EXTENDED-EUCLID $2\lceil \log a \rceil$ 次。

證明：(a) 归納法證明：設 $a = kb + r$

① 當輸入 $(a, 0)$ 時輸出 $(a, 1, 0)$

則 $d = a = a \cdot 1 + b \cdot 0$ 成立

② 已知 $d' = b \cdot x' + r \cdot y'$

$(d, x, y) = (d', y', x' - ky')$

則 $ax + by = ay' + b(x' - ky') = bx' + (a - bk)y' = bx' + ry' = d' = d$

即證得 $d = ax + by$

(b) 第二次迭代起 $a > b$, 這代一次 $(a, b) \rightarrow (b, a \bmod b)$, 迭代兩次

$(a, b) \rightarrow (a \bmod b, b \bmod (a \bmod b))$

則有 $a \bmod b < b$ 且 $(a \bmod b) + b \leq a$

則 $a \bmod b < \frac{a}{2}$

即每迭代兩次會減至半數以下

設每兩次迭代減半數, 迭代 $2k$ 次後有

$\frac{a}{2^k} < 1$ 則 $k > \log_2 a$ 取 $k = \lceil \log_2 a \rceil$ 為最多迭代次數

則 $n \leq 2k = 2\lceil \log_2 a \rceil$

3. (20pt) 记 $[n] = \{1, 2, \dots, n\}$, 考虑 $a \in [n]$ 且 $(a, n) = 1$ 。

(a) 证明存在唯一的 $b \in [n]$, 使得 $ab \equiv 1 \pmod{n}$.

3. 证明: (a) $\because (a, n) = 1$, 由裴蜀等式知, 存在 (x, y) , s.t. $ax + ny = 1$

证明存在性:

当 $x \in [n]$ 时, 取 $b = x$

当 $x \notin [n]$ 时, 取 $b = x - kn$, 则 $x = b + kn$, 其中 $b \in [n]$, $k \in \mathbb{Z}$

$$\therefore ab + n(y+k) = 1$$

即知 $\exists b \in [n]$, s.t. $ab \equiv 1 \pmod{n}$

证明唯一性:

反证法, 假设 $\exists b_1, b_2 \in [n]$, s.t.

$$ab_1 \equiv 1 \pmod{n}, ab_2 \equiv 1 \pmod{n}$$

$$\therefore n \mid a(b_1 - b_2)$$

$$\because (a, n) = 1 \quad \therefore n \mid b_1 - b_2$$

这与 $b_1, b_2 \in [n]$ 矛盾

综上, 存在唯一的 $b \in [n]$, s.t. $ab \equiv 1 \pmod{n}$

(b)

(b) 记上述 b 为 a^{-1} , 且对任意正整数 k 记 $a^{-k} = b^k$.

假设整数 s, t 使得 $a^s \equiv 1 \pmod{n}$ 且 $a^t \equiv 1 \pmod{n}$, 证明对于任

意整数 $r \in \{sx + ty \mid x, y \in \mathbb{Z}\}$, 有 $a^r \equiv 1 \pmod{n}$.

(注意 s, t, r, x, y 均可为负数。)

相关知识点: 同余的运算性质

指数法则 $(a^m)^k \equiv a^{mk} \pmod{n}$

值得注意的是, 指数运算只定义在整数上时, 需要保证指数的非负

运算性质: 若 $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m}$, 则:

- $a \pm c \equiv b \pm d \pmod{m}$ (因为 $m \mid (a-b) \pm (c-d) = (a \pm c) - (b \pm d)$)
- $ac \equiv bd \pmod{m}$ (因为 $m \mid (a-b)c + (c-d)b = ac - bd$)
- $a^k \equiv b^k \pmod{m}$ (对任意正整数 k)

解: 不妨取 s, t 均大于 0.

$$\textcircled{1} x > 0, \text{ 则 } a^{sx} \equiv (a^s)^x \equiv 1^x \pmod{n} = 1$$

$$\textcircled{2} x < 0, \text{ 则 } a^{sx} \equiv b^{-sx} \equiv b^{-sx} \cdot a^{-sx} \equiv (ab)^{-sx} \equiv 1 \pmod{n}$$

综上有 $a^{sx} \equiv 1 \pmod{n}$

同理有 $a^{ty} \equiv 1 \pmod{n}$

$$\text{则有 } a^r \equiv a^{sx+ty} \equiv a^{sx} \cdot a^{ty} \equiv 1 \pmod{n} \quad (\text{乘法运算})$$

(c) 令 d 为最小的正整数使得 $a^d \equiv 1 \pmod{n}$, 证明对于任意整数 m ,
 $a^m \equiv 1 \pmod{n}$ 当且仅当 $d | m$. (注意 m 可为负数。)

① " \Leftarrow " $\because a^d \equiv 1 \pmod{n}$ 且 $d | m$, 则 $m = kd$, $k \in \mathbb{Z}$
 由(b)的证明可得 $a^m \equiv a^{kd} \equiv 1 \pmod{n}$ 成立

② " \Rightarrow " 已知 $a^d \equiv 1 \pmod{n}$, $a^m \equiv 1 \pmod{n}$
 反证, 假设 $d \nmid m$, 则 $m = kd+r$, $k \in \mathbb{Z}, r \in [0]$, $a^m \equiv a^{kd+r} \equiv (a^d)^k \cdot a^r \equiv a^r \pmod{n}$
 这与 $a^m \equiv 1 \pmod{n}$ 矛盾 故假设错误, 得 $d | m$

4. (15pt) 用数学归纳法证明欧拉函数的求解公式。

已知 $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, p_i 为互不相同素数,
 要证 $\varphi(n) = \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}) = n \prod_{i=1}^k (1 - \frac{1}{p_i})$

证明 数学归纳法:

用质因数分解的长度来归纳:

设 $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

当 $k=1$ 时, 则 $n = p^r$

则 $\varphi(n) = \varphi(p^r) = p^{r-1} \cdot (p-1) = p^r \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p}\right)$

假设对所有质因子个数 $\leq k$ 的整数 n , 该公式都成立

即 $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$

对质因子个数为 $k+1$ 的整数 m

$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} p_{k+1}^{r_{k+1}}$
 $\varphi(m) = \varphi(n) \varphi(p_{k+1}^{r_{k+1}}) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \cdot p_{k+1}^{r_{k+1}} \left(1 - \frac{1}{p_{k+1}}\right) = m \prod_{i=1}^{k+1} \left(1 - \frac{1}{p_i}\right)$

即可证得。

5. (10pt) 设 $n = pq$ 其中 p, q 为素数, 令 $d = \gcd(p-1, q-1)$ 。证明对任意 a 满足 $(a, n) = 1$, 有 $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$ 。 $(\phi(n))$ 为欧拉函数。)

证明: 引理证明, $\begin{cases} x \equiv r \pmod{m_1} & \text{且 } (m_1, m_2) = 1, \text{ 且 } \\ x \equiv r \pmod{m_2} \end{cases} \Rightarrow x \equiv r \pmod{m_1 m_2}$

则 $m_1 | x-r, m_2 | x-r, \because (m_1, m_2) = 1$, 由裴蜀定理的推广
 $\therefore m_1 m_2 | x-r$
 $\therefore x \equiv r \pmod{m_1 m_2}$

已知 $a^{\phi(n)} \equiv 1 \pmod{n}$

$\because (a, n) = 1$, $n = pq$ 且 p, q 为素数 如果一个数与因子的乘积都互质, 那么它与各因数都互质

$\therefore (a, p) = 1, (a, q) = 1$

则有 $a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}, a^{\phi(q)} \equiv a^{q-1} \equiv 1 \pmod{q}$,

$$\because k = \text{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \frac{\phi(n)}{d}$$

且有 $\begin{cases} a^k \equiv 1 \pmod{p}, & \text{由于 } (p, q) = 1, \\ a^k \equiv 1 \pmod{q}, \end{cases}$

根据已证明的引理即可得到。

$$a^k \equiv 1 \pmod{(pq)}$$

6. (10pt) 计算欧拉函数 $\phi(18)$, 以及 5^{2023} 除以 18 所得的余数。

$$C_{18} = \{1, 5, 7, 11, 13, 17\}, \therefore \phi(18) = 6$$

$$5^{2023} \equiv (5^6)^{337} \cdot 5 \pmod{18} \equiv 1^{337} \cdot 5 \pmod{18} \equiv 5 \pmod{18}$$

$\therefore 5^{2023}$ 除以 18 所得余数为 5

7. (25pt) 考虑集合 $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$. 证明:

- (a) $\mathbb{Z}[\sqrt{-1}]$ 构成一个环 (参考讲义定义)。
- (b) $\mathbb{Z}[\sqrt{-1}]$ 中的单位只有 ± 1 以及 $\pm\sqrt{-1}$. (环的单位指其倒数也在该环中)
- (c) $1 + \sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中既是不可约元又是素元。
- (d) 2 在 $\mathbb{Z}[\sqrt{-1}]$ 中既不是不可约元也不是素元。
- (e) 已知 $\mathbb{Z}[\sqrt{-1}]$ 的任意不可约元都是素元。对于 $x \in \mathbb{Z}[\sqrt{-1}]$ 且 $x \neq 0, \pm 1, \pm\sqrt{-1}$, 若有 $x = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ 其中 $p_i (1 \leq i \leq k), q_j (1 \leq j \leq \ell)$ 均为 $\mathbb{Z}[\sqrt{-1}]$ 的不可约元。证明: $k = \ell$ 且适当交换乘积 $q_1 q_2 \cdots q_\ell$ 的顺序后, 对任意 $1 \leq i \leq k$, 有 $p_i = \epsilon_i q_i$ 其中 $\epsilon_i = \pm 1$ or $\pm\sqrt{-1}$.

解: (a) ① 封闭性 $\forall A = a_1 + b_1\sqrt{-1}, B = a_2 + b_2\sqrt{-1}, a_1, a_2, b_1, b_2 \in \mathbb{Z}$

$$A+B = (a_1+a_2) + (b_1+b_2)\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$$

$$A \cdot B = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$$

② 零元: $\exists a=b=0$, 则得 $0 \in \mathbb{Z}[\sqrt{-1}]$

单位元: 取 $a=1, b=0$ 则得 $1 \in \mathbb{Z}[\sqrt{-1}]$

③ $\forall a, b \in \mathbb{Z}$, 有 $-a, -b \in \mathbb{Z}$, 且 $-a - b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$

综上 $\mathbb{Z}[\sqrt{-1}]$ 构成一个环

(b) 取 $A = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}], a, b \in \mathbb{Z}$

$$\text{则 } \frac{1}{A} = \frac{1}{a+b\sqrt{-1}} = \frac{a-b\sqrt{-1}}{(a+b\sqrt{-1})(a-b\sqrt{-1})} = \frac{a-b\sqrt{-1}}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\sqrt{-1}$$

$$\text{要使 } \frac{1}{A} \in \mathbb{Z}[\sqrt{-1}], \text{ 则要满足 } \begin{cases} \frac{a}{a^2+b^2} \in \mathbb{Z} \\ \frac{-b}{a^2+b^2} \in \mathbb{Z} \end{cases} \quad \because a, b \in \mathbb{Z}$$

$$\therefore a^2+b^2 \geq a, a^2+b^2 \geq -b$$

$$a^2 \geq a, b^2 \geq -b$$

则仅有以下情况满足:

$$\textcircled{1} a=0, b=1 \quad \textcircled{2} a=0, b=-1 \quad \textcircled{3} a=1, b=0 \quad \textcircled{4} a=-1, b=0$$

对应元素 $\sqrt{-1}, -\sqrt{-1}, 1, -1$

而 $\mathbb{Z}[\sqrt{-1}]$ 中的单位仅有 $\pm 1, \pm\sqrt{-1}$

(c) 素元一定不可约元，只需验证 $1+\sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中是素元。

反证法：设 $k_1 = a_1 + b_1\sqrt{-1}$, $k_2 = a_2 + b_2\sqrt{-1}$,

$$\text{已知 } 1+\sqrt{-1} \mid k_1 k_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{-1}$$

由观察可知， $a_1 a_2 - b_1 b_2$ 与 $a_1 b_2 + a_2 b_1$ 同奇偶

假设 $1+\sqrt{-1} \mid k_1$ 且 $1+\sqrt{-1} \mid k_2$

则有 $a_1 \not\equiv b_1 \pmod{2}$, $a_2 \not\equiv b_2 \pmod{2}$

这与上面观察到的结论矛盾

故假设错误

从而得 $1+\sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中是素元，则其也为不可约元。

(d) $\because 2 = (1+\sqrt{-1})(1-\sqrt{-1})$, 且 $1+\sqrt{-1}$ 与 $1-\sqrt{-1}$ 都不是单位。

$\therefore 2$ 不是不可约元

素元一定是不可约元

故 2 不是素元

(e) 已知 $\mathbb{Z}[\sqrt{-1}]$ 的任意不可约元都是素元。对于 $x \in \mathbb{Z}[\sqrt{-1}]$ 且 $x \neq 0, \pm 1, \pm \sqrt{-1}$, 若有 $x = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ 其中 $p_i (1 \leq i \leq k)$, $q_j (1 \leq j \leq \ell)$ 均为 $\mathbb{Z}[\sqrt{-1}]$ 的不可约元。证明： $k = \ell$ 且适当交换乘积 $q_1 q_2 \cdots q_\ell$ 的顺序后，对任意 $1 \leq i \leq k$, 有 $p_i = \epsilon_i q_i$ 其中 $\epsilon_i = \pm 1$ or $\pm \sqrt{-1}$.

8. (10pt) 考虑一套 RSA 密钥体系，其中设 $n = pq$ 为两个素数的乘积， $\phi(n)$ 为欧拉函数，公钥 e 是与 $\phi(n)$ 互素的数，私钥 d 为同余方程 $ed \equiv 1 \pmod{\phi(n)}$ 的解。证明对于任意整数 m , $(m^e)^d \equiv m \pmod{n}$ 。即对消息 m 先用公钥 e 加密后再用私钥 d 解密，在模 n 取余数的意义下，得到的还是原来的消息 m 。
(注意这里 m 可能与 n 不互素。)

模 n 同余 m

解：① $(m, n) = 1$

$$\because ed \equiv 1 \pmod{\phi(n)}, \exists k \in \mathbb{Z}, \text{s.t. } ed = k\phi(n) + 1$$

$$\text{则 } (m^e)^d \equiv m^{k\phi(n)+1} \equiv (m^{\phi(n)})^k \cdot m \equiv 1^k \cdot m \equiv m \pmod{n} \quad (\text{应用欧拉定理})$$

② $(m, n) \neq 1$

$\because n = pq$ 且 p, q 均为素数

则当 $(m, p) = 1$ 时, $q | m$

$$\text{则 } (m^e)^d \equiv (m^{p-1})^{k(q-1)} \cdot m \equiv 1^{k(q-1)} \cdot m \equiv m \pmod{p}$$

$$(m^e)^d \equiv 0 \equiv m \pmod{q}$$

由中国剩余定理得 $(m^e)^d \equiv m \pmod{(pq)}$

同理可证 $(m, q) = 1$, $p | m$ 的情况 和 $p | m$, $q | m$ 的情况

综上 $(m^e)^d \equiv m \pmod{n}$ 成立

9. (15pt) 考虑集合 $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

- 找出一个 $\mathbb{Z}[\sqrt{5}]$ 中除 ± 1 之外的单位。
- $\mathbb{Z}[\sqrt{5}]$ 中是否存在不可约元？若存在请找出一个，若不存在请证明。
- $\mathbb{Z}[\sqrt{5}]$ 中是否存在素元？若存在请找出一个，若不存在请证明。
- $\mathbb{Z}[\sqrt{5}]$ 是否存在唯一分解？请证明你的结果。

解：(a) $k = a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, $a, b \in \mathbb{Z}$,

$$\text{则 } \frac{1}{k} = \frac{1}{a+b\sqrt{5}} = \frac{a-b\sqrt{5}}{(a+b\sqrt{5})(a-b\sqrt{5})} = \frac{a-b\sqrt{5}}{a^2-5b^2} = \frac{a}{a^2-5b^2} - \frac{b}{a^2-5b^2}\sqrt{5}$$

要满足 $\begin{cases} \frac{a}{a^2-5b^2} \in \mathbb{Z} \\ \frac{-b}{a^2-5b^2} \in \mathbb{Z} \end{cases}$ 取 $a=2, b=1$, 则 $\frac{a}{a^2-5b^2} = -2, \frac{-b}{a^2-5b^2} = 1$ 均属于 \mathbb{Z}

即 $2+\sqrt{5}$ 为 $\mathbb{Z}[\sqrt{5}]$ 的一个单位

(b) 存在不可约元 2。

反证：若 $2 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{5}]$ 且 α, β 都不为单位，

$$\text{设规范数 } N(2) = 4 = N(\alpha)N(\beta)$$

且 $|N(\alpha)| \neq 1, |N(\beta)| \neq 1$, $|N(\alpha)|$ 与 $|N(\beta)|$ 是 4 的因子，只可能为 2

$$\text{若 } |N(\alpha)| = 2, \text{ 则 } |N(a_1 + b_1\sqrt{5})| = 2, \text{ 则 } a_1^2 - 5b_1^2 = \pm 2$$

$$\text{则 } a_1^2 \equiv 2 \pmod{5}, \text{ 无解,}$$

$$a_1^2 \equiv -2 \pmod{5}, \text{ 无解}$$

故方程 $a^2 - 5b^2 = 2$ 无整数解

则该假设不成立。

故 2 为不可约元

(c) 存在 $\sqrt{5}$ 。

(d) 不存唯一分解。