

离散数学（2023 秋）作业二

截止日期：10 月 11 日 11.20

\mathbb{N}^+ , \mathbb{Z} , \mathbb{C} 分别表示正整数集、整数集以及复数集。

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。)

2. (15pt) 考虑如下算法:

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)

证明:

(a) 输出结果 (d, x, y) 满足 $d = ax + by$ 。

(b) 上述算法至多调用函数 EXTENDED-EUCLID $2\lceil \log a \rceil$ 次。

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 $ab \equiv 1 \pmod{n}$.

- (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 均可负数。)
- (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 $d \mid m$. (注意 m 可为负数。)
4. (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。)
5. (10pt) 计算欧拉函数 $\phi(18)$, 以及 5^{2023} 除以 18 所得的余数。
6. (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。)
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 $\pm\sqrt{-1}$.
- (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 $\pm\sqrt{-1}$.

8. (15pt) 考虑集合 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. 证明:

(a) $\mathbb{Z}[\sqrt{-5}]$ 中的单位只有 ± 1 .

(b) 2 是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元但不是素元。