离散数学第二次作业答案

王元叙

2024 年 10 月 20 日

1 作业答案

Problem 1

1. 略。

2. 第二次迭代起 $a > b$ ，每次迭代 $(a, b) \mapsto (b, a \bmod b)$ ，两次迭代后 $(a, b) \mapsto (a \bmod b, b \bmod (a \bmod b))$ 。有 $a \bmod b < b$ 且 $a \bmod b + b \leq a$ 从而 $a \bmod b < \frac{n}{2}$ 。则可以得到结论。

Problem 2

1. 由裴蜀定理，$(a, n) = 1$ 推出 $\exists b, t \in \mathbb{Z}$ 使得 $ab + tn = 1$ 。进而 $ab \equiv 1 \pmod{n}$ 。

   若存在 $b \neq b' \in [n]$ 同时满足条件则 $n | a(b - b')$ 。由于 $(a, n) = 1$ 可得 $n | b - b'$ ，得出矛盾，于是这样的 b 是唯一的。

2. 不妨设 $s, t > 0$ ，若 $x \geq 0$ 则 $a^{sx} \equiv (a^s)^x \equiv 1 \pmod{n}$。

   若 $x < 0$ 则由 $a^{-sx} \equiv 1 \pmod{n}$ 可得 $a^{sx} \equiv b^{-sx} \equiv b^{-sx} \cdot a^{-sx} \equiv 1^{-sx} \equiv 1 \pmod{n}$。

   同理有 $a^{ty} \equiv 1 \pmod{n}$ ，从而 $a^{sx+ty} \equiv 1 \pmod{n}$ 。

3. 若 $d \mid m$ 则存在 t 使得 $m = dt$ ，由第二小题可得 $a^m \equiv 1 \pmod{n}$

   若 $a^m \equiv 1 \pmod{n}$ 且 $d \nmid m$ 则 $(d, m) = d' < d$

   由第二小题结论及裴蜀定理存在 $x, y \in \mathbb{Z}$ 使得 $d' = dx + my$ ，有 $a^{d'} \equiv 1 \pmod{n}$ ，这与 d 最小性矛盾。从而 $d \mid m$ 。

Problem 3

$\Longrightarrow$: 由于 p 是素数，$p \nmid n$ 则 $(p,n)=1$

$$\varphi(pn)=\varphi(p)\varphi(n)=(p-1)\varphi(n)$$

$\Longleftarrow$: 反证法，假设 $n=p^k m$，其中 $k\geq 1$ ，$(p,m)=1$ ，那么

$$\varphi(pn)=\varphi(p^{k+1})\varphi(m)=(p-1)p^k\varphi(m)$$
$$(p-1)\varphi(n)=(p-1)\varphi(p^k)\varphi(m)=(p-1)^2p^{k-1}\varphi(m)$$

比较可知结论 $\varphi(pn)=(p-1)\varphi(n)$ 不成立。

Problem 4

由 $(p,q)=1$ 以及欧拉函数的积性 $\varphi(n)=\varphi(p)\varphi(q)=(p-1)(q-1)$ ，于是

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

中国剩余定理给出

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

Problem 5

计算得到 $\varphi(18)=6$，从而由欧拉定理 $5^6\equiv 1 \pmod{18}$

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

Problem 6

1. 依次验证环的各项定义，略。

2. 构造映射 $N:\mathbb{Z}[\sqrt{-1}]\to \mathrm{N}$ 使得 $a+b\sqrt{-1}\mapsto a^2+b^2$

   可以验证该映射具有的性质：$N(1)=1, N(xy)=N(x)N(Y)$

   根据单位的定义，若 x 是单位则存在 y 使得 $xy=1$ 从而 $N(x)N(y)=1$

   从而 $N(x)=1$ 即 $x=\pm 1,\pm\sqrt{-1}$ 。另一方面，可以验证这四个 x 都是单位，从而给出了 $\mathbb{Z}[\sqrt{-1}]$ 的单位群。

3. 素元一定不可约，只需验证 $1+\sqrt{-1}$ 是素元。首先观察得到 $1+\sqrt{-1} \mid m+n\sqrt{-1}$ 当且仅当 m,n 同奇偶。

   若 $1+\sqrt{-1} \mid xy$ ，$x=a+b\sqrt{-1}, y=c+d\sqrt{-1}$ 。从而由前述观察，$ac-bd, ad+bc$ 同奇偶。若 $a \not\equiv b, c \not\equiv d \pmod 2$ 则可以推得矛盾。

4. 素元一定不可约，只需验证 2 不是不可约元。而 $2=(1+\sqrt{-1})(1-\sqrt{-1})$ 。

5. 结论对所有满足不可约元都是素元的整环成立，下面记整环 R 满足这样的性质。

   考虑 p_1 ，有：$p_1 \mid p_1 \cdots p_r = q_1 \cdots q_s$

   由 p_1 不可约，p_1 是素元，根据素元性质可知 $\exists j, 1 \le j \le s$ ，使得 $p_1 \mid q_j$

   不妨假设 $p_1 \mid q_1$ ，使得 $q_1 = u_1 p_1, u_1 \in R$ 。有 q_1, p_1 不可约，所以 $u_1 \in U(R)$，所以 $p_1 \sim q_1$ 。由整环的乘法消去律可得 $a = p_2 \cdots p_r = u_1 q_2 \cdots q_s \in R$ ，再考虑 p_2。

   对 p_2 做同样的论证，又得 $\exists u_2 \in U(R)$，使得 $a = p_3 \cdots p_r = u_1 u_2 q_3 \cdots q_s$ ，如果 $r < s$ ，则到某一步时有 $1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s$ ，故 $q_{r+1} \cdots q_s \in U(R)$，这与 $q_{r+1}, \cdots, q_s$ 不可约矛盾，若 $r > s$ ，则到某一步就得到 $p_{s+1} \cdots p_r = u_1 \cdots u_s$ ，又矛盾。

Problem 7

若 $(m,n)=1$ 根据欧拉定理 $m^{\varphi(n)} \equiv 1 \pmod n$ 从而

$$(m^e)^d = m^{k\varphi(n)+1} \equiv m \pmod n$$

若 $(m,n) \neq 1$ 不妨假设 $p \mid n$ ，设 $m = tp (0 \le t < q)$
由 $m < n$ 可以得到 $(m,q)=1$ ，从而

$$m^{q-1} \equiv 1 \pmod q$$
$$m^{k\varphi(n)} \equiv 1 \pmod q$$

设 $m^{k\varphi(n)} - 1 = hq$ 则

$$m^{k\varphi(n)+1} = tphq + tp \equiv m \pmod n$$

Problem 8

1. 仿照第 6 题的方法构造映射 $N : \mathbb{Z}[\sqrt{5}] \to \mathrm{Z}$ 使得 $a+b\sqrt{5} \mapsto a^2 - 5b^2$ 并验证 $N(xy) = N(x)N(y)$

   可以得到 $\pm 2 \pm \sqrt{5}$ 都是单位。

2. 存在。2 就是 $\mathbb{Z}[\sqrt{5}]$ 一个不可约元。

   设 $2=(a+b\sqrt{5})(c+d\sqrt{5})$ 则 $4=(a^2-5b^2)(c^2-5d^2)$

   由于 $x^2\equiv 0,1,4 \pmod 5$，可得 $(a^2-5b^2)=\pm 1$ 或 $(c^2-5d^2)=\pm 1$ 从而 $(a+b\sqrt{5})$ 或 $(c+d\sqrt{5})$ 是单位。

3. 存在。$\sqrt{5}$ 就是 $\mathbb{Z}[\sqrt{5}]$ 的一个素元。若 $\sqrt{5}\mid(a+b\sqrt{5})(c+d\sqrt{5})$ 有 $\sqrt{5}\mid ac$ 从而 $5\mid ac$。

   由素数性质 $5\mid a$ 或 $5\mid c$ 从而 $\sqrt{5}\mid(a+b\sqrt{5})$ 或 $\sqrt{5}\mid(c+d\sqrt{5})$

   还有更多 $\mathbb{Z}[\sqrt{5}]$ 的素元，同学们可以尝试验证 $4+\sqrt{5},3+2\sqrt{5}$ 也是素元。

4. 不存在。$4=2\times 2=(\sqrt{5}-1)\times(\sqrt{5}+1)$，可以验证 $\sqrt{5}\pm 1$ 同样是不可约元。