中国科学技术大学《代数学基础》期末考试

2025年12月07日19:00–21:00

姓名：_____ 学号：_____ 所在院系：_____

题号	一	二	三	四	五	六	七	总　分
得分								
复查								

本考试不允许使用电子计算工具。如果某一问不会做，可利用该问结果进行后续的推导。

一、(10分) 求整数 1274 和 546 的最大公因子，并求出二元一次不定方程

$$1274x + 546y = (1274, 546)$$

的所有整数解。

Proof. 使用欧几里得算法：

$$1274 = 2 \times 546 + 182$$

$$546 = 3 \times 182 + 0$$

所以$(1274, 546) = 182$。

回代：

$$182 = 1274 - 2 \times 546$$

所以$x = 1, y = -2$。因此，二元一次不定方程

$$1274x + 546y = (1274, 546)$$

的所有整数解为

$$\begin{cases} x = 1 + 3t \\ y = -2 - 7t \end{cases}$$

其中 $t \in \mathbb{Z}$ 为任意整数。 □

二、判断题(20分) 判断正误，并简要说明理由

1). 整系数多项式 $f(x)=x^4+4$ 在有理数域上不可约。

2). 设 p 为素数, n 为正整数，则模 p^n 存在原根。

3). 若 p 为素数且同余方程 $x^2\equiv 2 \pmod p$ 有解，则 $p\equiv \pm 1 \pmod 8$。

4). 设素数 $p\equiv 17(\mathrm{mod}\ 24)$, 则 p 不能写成 x^2+6y^2 的形式和，其中 x,y 为整数。

1. 错误

理由：$x^4+4=(x^2+2x+2)(x^2-2x+2)$，因此在有理数域上可约。

2. 错误

理由：当 $p=2, n\geq 3$ 为正整数，则模 2^n 不存在原根。不妨取 $n=3$，模 8 的缩系为 $\{1,3,5,7\}$, 其元素的阶分别为 $1,2,2,2$, 因此模 2^3 不存在原根。

3. 错误

理由：由二次互反律，$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$，当$p\equiv \pm 1 \pmod 8$ 时，$\frac{p^2-1}{8}$ 为偶数，故$\left(\frac{2}{p}\right)=1$。但是不完整，当 $p=2$ 时同余方程 $x^2\equiv 2 \pmod p$ 有解。

4. 正确

理由：反证，假设素数 $p=x^2+6y^2$，易知 x,y 不能被 p 整除，由二次互反律可得

$$\begin{aligned}1=\left(\frac{x^2}{p}\right)&=\left(\frac{-6y^2}{p}\right)=\left(\frac{-6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\\&=\left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\cdot(-1)^{\frac{3-1}{2}\times\frac{p-1}{2}}=\left(\frac{2}{p}\right)\left(\frac{p}{3}\right).\end{aligned}$$

当 $p\equiv 17(\mathrm{mod}\ 24)$, 则有 $p\equiv 1(\mathrm{mod}\ 8)$ 和 $p\equiv 2(\mathrm{mod}\ 3)$。因此，

$$\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)=1\times(-1)=-1.$$

矛盾！

三、（15分） 求解一次同余方程组：

$$\begin{cases}x\equiv 2 & (\mathrm{mod}\ \ 5)\\ 3x\equiv 1 & (\mathrm{mod}\ \ 7)\\ 2x\equiv 3 & (\mathrm{mod}\ 11)\end{cases}$$

Proof. 化简方程组：

$$\begin{cases} x \equiv 2 \pmod 5 \\ 3x \equiv 1 \pmod 7 \Rightarrow x \equiv 5 \pmod 7 \\ 2x \equiv 3 \pmod{11} \Rightarrow x \equiv 7 \pmod{11} \end{cases}$$

解前两个方程：$x = 2 + 5t \equiv 5 \pmod 7$

$2 + 5t \equiv 5 \pmod 7 \Rightarrow 5t \equiv 3 \pmod 7 \Rightarrow t \equiv 2 \pmod 7$

所以$t = 2 + 7s$，$x = 2 + 5(2 + 7s) = 12 + 35s$

再与第三个方程联立：$12 + 35s \equiv 7 \pmod{11}$

$1 + 2s \equiv 7 \pmod{11} \Rightarrow 2s \equiv 6 \pmod{11} \Rightarrow s \equiv 3 \pmod{11}$

所以$s = 3 + 11k$，$x = 12 + 35(3 + 11k) = 117 + 385k$

解为：$x \equiv 117 \pmod{385}$ □

四、(15分)设 $f(x) = x^4 + x^3 + x^2 + x + 1$ 是整系数多项式，

1). 证明 $f(x)$ 为 $\mathbb{Z}[x]$ 中不可约多项式。

2). $f(x)$ 的模 3 约化多项式在 $\mathbb{F}_3[x]$ 中可约吗？为什么？($\mathbb{F}_3 = \mathbb{Z}_3$ 三元有限域)

3). 81 元有限域是否存在，或者说恰好含 81 个元素的整环是否存在？存在的话请构造一个，不存在的话请说明理由。

Proof. 1). 考虑 $f(x+1) = \frac{(x+1)^5 - 1}{(x+1) - 1} = x^4 + 5x^3 + 10x^2 + 10x + 5$，对 $p = 5$ 利用艾森斯坦判别法知 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约，因此 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约。

2). $f(x)$ 的模 3 约化多项式在 $\bar{f}(x) \in \mathbb{F}_3[x]$ 中不可约。因为 $\bar{f}(\bar{0}) = \bar{1}, \bar{f}(\bar{1}) = \bar{2}, \bar{f}(\bar{2}) = \bar{1}$, 所以 $\bar{f}(x)$ 没有一次不可约因子。$\mathbb{F}_3[x]$ 中二次不可约多项式有

$$x^2 + \bar{1}, x^2 + x + \bar{2}, x^2 + 2x + \bar{2}.$$

由带余除法，可得

$$\bar{f}(x) = (x^2 + \bar{1})(x^2 + x) + \bar{1},$$

$$\bar{f}(x) = (x^2 + x + \bar{2})(x^2 + \bar{2}) + \bar{2}x,$$

$$\bar{f}(x) = (x^2 + 2x + \bar{2})(x^2 + \bar{2}x + \bar{1}) + (x + \bar{2}).$$

因此，$\mathbb{F}_3[x]$ 无二次不可约因子。

3). 81 元有限域存在，可取为

$$\mathbb{F}_3[x]/(\bar{f}(x))\mathbb{F}_3[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + (\bar{f}(x))\mathbb{F}_3[x] : a_0, a_1, a_2, a_3 \in \mathbb{F}_3\}.$$

□

五、(10分)设 m, n 为正整数，求复系数多项式 $x^m - 1, x^n - 1 \in \mathbb{C}[x]$ 的最大公因子 $(x^m - 1, x^n - 1)$。

Proof. 不妨设 $n \geq m$, 由带余除法存在整数 q, r 使得 $n = mq + r$，其中$0 \leq r < d$, 则

$$x^n - 1 = x^{mq+r} - 1 = x^r[(x^m)^q - 1] + (x^r - 1).$$

因此， $(x^m - 1, x^n - 1) = (x^n - 1, x^r - 1)$. 利用欧几里得算法或辗转相除法，可得

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

□

六、多项式中的平方和问题（10分）

1). 设 $f(x) \in \mathbb{R}[x]$ 为实系数多项式。证明: 对任意 $c \in \mathbb{R}$ 有 $f(c) \geq 0$ 当且仅当存在实系数多项式 $g(x)$ 和 $h(x)$ 使得

$$f(x) = (g(x))^2 + (h(x))^2.$$

2). 复数中没有大小概念，上述结论无法表面推广。然而请证明：在复系数多项式环 $\mathbb{C}[x]$ 中，任意多项式 $f(x)$ 均可表示为两个复系数多项式的平方和。

Proof. **(1)**考虑$f(x)$ 的标准分解式:

$$f(x) = a\varphi(x)\psi(x),$$

其中$a \in \mathbb{R}$，而

$$\varphi(x) = (x - a_1)^{k_1}(x - a_2)^{k_2} \cdots (x - a_s)^{k_s},$$

$$\psi(x) = \prod_{j=1}^{t}(x^2 + p_jx + q_j)^{r_j},$$

这里，$k_1, k_2, \cdots, k_s, r_1, r_2, \cdots, r_t$ 是正整数，而$p_j^2 - 4q_j < 0, 1 \le j \le t$。由于$\psi(x)$ 没有实根，而实系数多项式的复根必成对出现，所以存在多项式$\psi_1(x), \psi_2(x) \in \mathbb{R}[x]$，使得

$$\psi(x) = [\psi_1(x) + i\psi_2(x)][\psi_1(x) - i\psi_2(x)] = [\psi_1(x)]^2 + [\psi_2(x)]^2.$$

对于$\varphi(x)$，不妨设$a_1 < a_2 < \cdots < a_s$，下证$k_1, k_2, \cdots, k_s$ 均为偶数。假设某个k_i 是奇数，则x 在a_i 的附近变化时$f(x)$ 变号，但$f(c) \ge 0$ 对一切$c \in \mathbb{R}$ 成立，矛盾。于是$\varphi(x) = [\varphi_1(x)]^2$，其中

$$\varphi_1(x) = (x - a_1)^{\frac{k_1}{2}}(x - a_2)^{\frac{k_2}{2}} \cdots (x - a_s)^{\frac{k_s}{2}} \in \mathbb{R}[x].$$

再由题设条件，$f(c) \ge 0$ 对一切$c \in \mathbb{R}$ 成立，可知$a \ge 0$。因此，有

$$f(x) = (g(x))^2 + (h(x))^2,$$

其中

$$g(x) = \sqrt{a}\varphi_1(x)\psi_1(x), \quad h(x) = \sqrt{a}\varphi_1(x)\psi_2(x) \in \mathbb{R}[x].$$

(2)设$f(x) \in \mathbb{C}[x]$ 是任意多项式。定义：

$$g(x) = \frac{1 + f(x)}{2}, \quad h(x) = \frac{1 - f(x)}{2i}$$

则$g(x)$ 和$h(x)$ 都是复系数多项式，且直接计算可得：

$$\begin{aligned} g(x)^2 + h(x)^2 &= \left(\frac{1 + f(x)}{2}\right)^2 + \left(\frac{1 - f(x)}{2i}\right)^2 \\ &= \frac{(1 + f(x))^2}{4} + \frac{(1 - f(x))^2}{-4} \quad (\text{因为} i^2 = -1) \\ &= \frac{(1 + f(x))^2 - (1 - f(x))^2}{4} \\ &= \frac{4f(x)}{4} = f(x) \end{aligned}$$

因此，$f(x) = g(x)^2 + h(x)^2$。

□

七、模 pq 的二次剩余(20分) 设 p, q 为不同的奇素数，$n = pq$，引入雅可比符号

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p}\right)\left(\frac{a}{q}\right),$$

其中右侧的 $\left(\frac{a}{p}\right)$ 和 $\left(\frac{a}{q}\right)$ 为勒让德符号。

1). 证明：若 $\left(\frac{a}{n}\right)=-1$，则 a 不是模 n 的二次剩余。

2). 举例说明：存在整数 a 满足 $\left(\frac{a}{n}\right)=1$，但 a 不是模 n 的二次剩余。

3). 上一问说明雅可比符号并不是判别合数模二次剩余的正确符号。请写出 a 为模 n 二次剩余的判别准则(充要条件)，并给出证明。

4). 证明

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}},\quad \left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}.$$

5). 设 $P=p_1p_2\cdots p_s$, 推广雅可比符号

$$\left(\frac{a}{P}\right):=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right).$$

设奇数 $P\geq 3$ 和奇数 $Q\geq 3$, 且 $(P,Q)=1$, 则有以下互反律成立

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{(P-1)/2\cdot(Q-1)/2}.$$

Proof. **(1)**

若$\left(\frac{a}{n}\right)=-1$，则$\left(\frac{a}{p}\right)$ 与$\left(\frac{a}{q}\right)$ 中至少有一个为-1。

若$\left(\frac{a}{p}\right)=-1$，则$a$ 在模p 下不是二次剩余；若$\left(\frac{a}{q}\right)=-1$，则$a$ 在模q 下不是二次剩余。

因此a 在模p 或模q 下不是二次剩余，从而不可能是模n 的二次剩余。

(2)

取$p=3,q=5,n=15$。考虑$a=2$:

计算勒让德符号:

$$\left(\frac{2}{3}\right)=-1,\quad \left(\frac{2}{5}\right)=-1$$

因此雅可比符号:

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)\times(-1)=1$$

但2 不是模15 的二次剩余，因为:

- 模3 的二次剩余为$\{1\}$，$2\not\equiv 1 \pmod 3$
- 模5 的二次剩余为$\{1,4\}$，$2\not\equiv 1,4 \pmod 5$

所以2 在模3 和模5 下都不是二次剩余，从而不可能是模15 的二次剩余。

(3)

a是模$n = pq$的二次剩余当且仅当$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) = 1$。

若a 是模n 的二次剩余，则存在x 使得

$$x^2 \equiv a \pmod{n}$$

由于$p \mid n$，有$x^2 \equiv a \pmod{p}$，所以$\left(\frac{a}{p}\right) = 1$。同理$\left(\frac{a}{q}\right) = 1$。

若$\left(\frac{a}{p}\right) = 1$ 且$\left(\frac{a}{q}\right) = 1$，则存在$u, v$ 使得

$$u^2 \equiv a \pmod{p}, \quad v^2 \equiv a \pmod{q}$$

由中国剩余定理，存在x 同时满足

$$x \equiv u \pmod{p}, \quad x \equiv v \pmod{q}$$

则$x^2 \equiv a \pmod{p}$ 且$x^2 \equiv a \pmod{q}$，从而$x^2 \equiv a \pmod{n}$。

因此a 是模n 的二次剩余。

(4)

由 $n = pq$ 可知 $n - 1 = (p - 1) + (q - 1) + (p - 1)(q - 1)$, 从而

$$\frac{n-1}{2} \equiv \frac{p-1}{2} + \frac{q-1}{2} \pmod{2}, \quad \frac{n^2-1}{8} \equiv \frac{p^2-1}{8} + \frac{q^2-1}{8} \pmod{8}.$$

因此，有

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}} = (-1)^{\frac{n-1}{2}}$$

以及

$$\left(\frac{2}{n}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{n^2-1}{8}}.$$

(5) 令$Q = q_1 q_2 \cdots q_r$. 由雅可比符号的定义及二次剩余勒让德符号的二次互反律

知

$$\begin{aligned}\left(\frac{Q}{P}\right) &= \prod_{j=1}^{s}\left(\frac{Q}{p_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)\\ &= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)(-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}}\\ &= \left(\frac{P}{Q}\right)\prod_{j=1}^{s}\prod_{i=1}^{r}(-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}}\\ &= \left(\frac{P}{Q}\right)\prod_{j=1}^{s}(-1)^{\frac{p_j-1}{2}\cdot\sum_{i=1}^{r}\frac{q_i-1}{2}}.\end{aligned}$$

由(4)及数学归纳法知

$$\sum_{i=1}^{r}\frac{q_i-1}{2} \equiv \frac{Q-1}{2}(\text{mod } 2).$$

因此，

$$\begin{aligned}\left(\frac{Q}{P}\right) &= \left(\frac{P}{Q}\right)\prod_{j=1}^{s}(-1)^{\frac{p_j-1}{2}\cdot\frac{Q-1}{2}}.\\ &= \left(\frac{P}{Q}\right)(-1)^{\sum_{j=1}^{s}\frac{p_j-1}{2}\cdot\frac{Q-1}{2}}\\ &= \left(\frac{P}{Q}\right)(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\end{aligned}$$

由 P,Q 互素，知 $\left(\frac{Q}{P}\right) = \pm 1$. 因此，

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{(P-1)/2\cdot(Q-1)/2}.$$

□