

ENT Practice

悔教

目录

1 作业 1 (2026 年 3 月 11 日)	1
2 作业 2 (2026 年 4 月 16 日)	2
3 作业 3 (2026 年 5 月 6 日)	4
4 作业 4 (2026 年 5 月 29 日)	6
5 参考练习 (2026 年 6 月 4 日)	7

1 作业 1 (2026 年 3 月 11 日)

问题 1.1. 设 n 为正整数, 证明:

(1) $\gcd(a^n, b^n) = \gcd(a, b)^n$;

(2) 设 a, b 是互素的正整数, 且 $ab = c^n$, 其中 c 也是正整数, 则 a, b 都是整数的 n 次方幂。

问题 1.2. 设 a, b 是互素的正整数。证明: 当 $n > ab - a - b$ 时, 方程

$$ax + by = n$$

有非负整数解; 当 $n = ab - a - b$ 时, 上述方程无非负整数解。

问题 1.3. 令 Prim 是所有正素数构成的集合。对 Prim 的任意有限子集 S , 令

$$f_S(x) = |\{a \in \mathbb{Z} : 1 \leq a \leq x \text{ 且 } a \text{ 的所有素因子都在 } S \text{ 中}\}|.$$

(1) 证明 $f_S(x) \leq 2^{|S|} \sqrt{x}$ 。提示: 每个正整数可以分解为一个平方数和一个无平方因子的数的乘积。

(2) 证明不等式

$$x - f_S(x) \leq \sum_{\substack{p \in \text{Prim} \setminus S \\ p \leq x}} \left\lfloor \frac{x}{p} \right\rfloor$$

成立;

(3) 利用上面的结论证明级数 $\sum_p \frac{1}{p}$ 发散。

问题 1.4. 设 n 是正整数。令 $v(n) = \sum_{d|n} 1$, 即 n 的所有正因子的个数。证明:

(1) n 是平方数当且仅当 $v(n)$ 是奇数;

(2) $v(n) \leq 2\sqrt{n} + 1$;

(3) n 的所有正因子的乘积等于 $n^{v(n)/2}$ 。

问题 1.5. 对正整数 n , 令 $T(n)$ 是其十进制下数码的交错和。例如 $T(1234) = 4 - 3 + 2 - 1$; 又例如 $T(987) = 7 - 8 + 9$ 。证明:

$$T(n) \equiv n \pmod{11}.$$

问题 1.6. 证明方程

$$7x^3 + 2 = y^3$$

没有整数解。

问题 1.7. 设 p 是一个正素数。证明:

(1) (Wilson 定理) 我们总有

$$(p-1)! \equiv -1 \pmod{p};$$

(2) 下面的和式

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

的分子可以被 p 整除。

2 作业 2 (2026 年 4 月 16 日)

问题 2.1. 设 p 是奇素数, 证明: 模 p 的任意两个原根之积不是模 p 的原根。

问题 2.2. 设 n, a 都是正整数且 $a > 1$, 证明:

$$n \mid \varphi(a^n - 1),$$

其中 φ 是 Euler 函数。

问题 2.3. 设 p 与 $q = 2p + 1$ 都是素数。证明：

- (1) 当 $p \equiv 1 \pmod{4}$ 时, 2 是模 q 的原根;
- (2) 当 $p \equiv 3 \pmod{4}$ 时, -2 是模 q 的原根。

问题 2.4. 设 p 是素数, $p \equiv 1 \pmod{4}$ 。证明：

(1)

$$\sum_{\substack{1 \leq r \leq p-1 \\ \left(\frac{r}{p}\right)=1}} r = \frac{p(p-1)}{4};$$

(2)

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) = 0;$$

(3)

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{k^2}{p} \right\rfloor = \frac{(p-1)(p-5)}{24}.$$

问题 2.5. 设 p 是素数, $p \equiv 3 \pmod{4}$, 且 $p > 3$ 。证明：

(1)

$$\sum_{\substack{1 \leq r \leq p-1 \\ \left(\frac{r}{p}\right)=1}} r \equiv 0 \pmod{p};$$

(2)

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv 0 \pmod{p}.$$

问题 2.6. 设 p 是奇素数, a 是整数。

(1) 证明：同余方程

$$x^2 - y^2 \equiv a \pmod{p}$$

必有解；

(2) 若 (x, y) 和 (x', y') 均是上述同余方程的解, 当

$$x \equiv x' \quad \text{且} \quad y \equiv y' \pmod{p}$$

时, 我们把 (x, y) 和 (x', y') 看成是同一组解。证明：(1) 中同余方程的解的个数是 $p-1$ (若 $p \nmid a$) 或 $2p-1$ (若 $p \mid a$)。

问题 2.7. 试求所有素数 p , 使得 $x^2 - 15$ 在 $\mathbb{F}_p[x]$ 中可约。

问题 2.8. 设 $p = 4k + 1$ 是素数, a 是 k 的约数。证明:

$$\left(\frac{a}{p}\right) = 1.$$

问题 2.9. 设 $n > 1$, 且 $p = 2^n + 1$ 是素数。证明: 模 p 的原根之集与模 p 的二次非剩余之集相同; 进而证明 3, 7 都是模 p 的原根。

问题 2.10. 设 p 是奇素数, 证明: 在 $\mathbb{F}_p[x]$ 中, 形如

$$x^2 + \alpha x + \beta$$

的二次多项式中, 共有 $\frac{p(p-1)}{2}$ 个不可约多项式。

3 作业 3 (2026 年 5 月 6 日)

问题 3.1. 设 m, d 为正整数, 且 $d \mid m$ 。证明: 对于任意和 d 互素的整数 a_0 , 都存在 $a \in \mathbb{Z}$, 使得

$$a \equiv a_0 \pmod{d} \quad \text{且} \quad \gcd(a, m) = 1.$$

(不使用 Dirichlet 定理!)

问题 3.2. 设 $m = p^\ell$ 是素数 p 的幂次, a 是正整数且与 p 互素。记 f 是 a 模 m 的阶。证明: 当 χ 遍历所有模 m Dirichlet 特征时, $\chi(a)$ 遍历所有 f 次单位根。更进一步, 能否确定每个单位根被取到几次?

问题 3.3. 任意给定两个 (在 $\mathbb{C}$ 中取值的) 数列 $A = \{a_n\}_{n=1}^\infty$, $B = \{b_n\}_{n=1}^\infty$, 我们定义一个新数列 $A * B = \{c_n\}_{n=1}^\infty$, 其中

$$c_n = \sum_{d \mid n} a_d b_{n/d}.$$

称 $A * B$ 为 A, B 的 Dirichlet 卷积。证明:

(1) 给定任意三个数列 A, B, C , 都有结合律成立:

$$(A * B) * C = A * (B * C).$$

(2) 给定任意两个数列 A, B , 都有交换律成立:

$$A * B = B * A.$$

(3) 给定任意三个数列 A, B, C , 都有分配律成立:

$$(A + B) * C = A * C + B * C;$$

这里 $A + B = \{a_n + b_n\}_{n=1}^\infty$ 。

问题 3.4. 考虑以下三个数列:

- $\mathcal{E} = \{e_n\}_{n=1}^{\infty}$, 其中 $e_1 = 1$, 且对任意 $n > 1$ 有 $e_n = 0$;
- $\mathcal{I} = \{i_n\}_{n=1}^{\infty}$, 其中对任意 $n \geq 1$ 有 $i_n = 1$;
- $\mu = \{u_n\}_{n=1}^{\infty}$, 其中

$$u_n = \begin{cases} 1, & n = 1, \\ 0, & n \text{ 有平方因子}, \\ (-1)^r, & n = p_1 p_2 \cdots p_r \text{ 是 } r \text{ 个不同素数的乘积}. \end{cases}$$

证明:

- (1) 对任意数列 A , 都有

$$A * \mathcal{E} = \mathcal{E} * A = A.$$

数列 $A = \{a_n\}_{n=1}^{\infty}$ 在 Dirichlet 卷积下可逆 (即, 存在数列 B , 使得 $A * B = \mathcal{E}$) 当且仅当 $a_1 \neq 0$;

- (2) $\mathcal{I}$ 和 μ 在 Dirichlet 卷积下互为逆, 即:

$$\mathcal{I} * \mu = \mu * \mathcal{I} = \mathcal{E}.$$

此关系称为 Möbius 反演;

- (3) 若数列 $F = \{f_n\}_{n=1}^{\infty}$ 和 $G = \{g_n\}_{n=1}^{\infty}$ 满足

$$f_n = \sum_{d|n} g_d,$$

则有

$$g_n = \sum_{d|n} u_d f_{n/d}.$$

问题 3.5. 设

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

是正整数 m 的素因子分解。证明 Euler 函数 $\varphi(m)$ 满足

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

问题 3.6. 考虑有限域 $\mathbb{F}_p$ 上的一元多项式环 $\mathbb{F}_p[x]$ 。对每个正整数 $n \in \mathbb{Z}_{>0}$, 令 M_n 是 $\mathbb{F}_p[x]$ 中 n 次首一不可约多项式的个数。

(1) 证明: $z \in \mathbb{C}$ 且 $|z| < 1/p$ 时, 有

$$\sum_{n=1}^{\infty} p^n z^n = \prod_{n=1}^{\infty} \left(\frac{1}{1 - z^n} \right)^{M_n}.$$

提示: 注意 $\mathbb{F}_p[x]$ 中所有 n 次首一多项式恰有 p^n 个, 利用 $\mathbb{F}_p[x]$ 的唯一因子分解性质。

(2) 利用上述关系式与 Möbius 反演计算 M_n 。

问题 3.7. 若一个 (在 $\mathbb{C}$ 中取值的) 数列 $A = \{a_n\}_{n=1}^{\infty}$ 满足对任意的互素正整数 k, ℓ , 都有

$$a_{k\ell} = a_k a_{\ell},$$

则称 A 是积性的。证明:

(1) 若 A 是积性的且不是零数列 (即 a_n 不全为 0), 则必有 $a_1 = 1$;

(2) 给定任意两个非零积性数列 A, B , 则它们的 Dirichlet 卷积 $A * B$ 也是积性的。

问题 3.8. 设 $F = \{f_n\}_{n=1}^{\infty}$ 是非零积性数列。对任意 $A = \{a_n\}_{n=1}^{\infty}$, 记 $F \cdot A = \{f_n a_n\}_{n=1}^{\infty}$ 。证明:

- 若 F 完全积性 (即, 对于任意正整数 k, ℓ 都有 $f_{k\ell} = f_k f_{\ell}$), 则对任意数列 A, B 都有

$$F \cdot (A * B) = (F \cdot A) * (F \cdot B).$$

- F 是完全积性的当且仅当

$$F^{-1} = F \cdot \mu,$$

其中 F^{-1} 是 F 关于 Dirichlet 卷积的逆。

4 作业 4 (2026 年 5 月 29 日)

问题 4.1. 设 p 为奇素数, $\zeta_p = e^{2\pi\sqrt{-1}/p}$ 。回忆: 二次 Gauss 和定义为

$$g = \sum_{x=1}^{p-1} \left(\frac{x}{p} \right) \zeta_p^x.$$

另定义

$$G = \sum_{x=0}^{p-1} \zeta_p^{x^2}.$$

证明: $G = g$ 。

问题 4.2. 设素数 $p \equiv 1 \pmod{4}$ 。令 χ 为模 p 的一个四次乘法特征, 即 $\chi^4 = \chi_0$ 且 $\chi^2 \neq \chi_0$ (这里 χ_0 表示平凡特征)。回忆: Jacobi 和定义为

$$J(\chi, \chi) = \sum_{x \in \mathbb{F}_p} \chi(x) \chi(1-x).$$

(1) 证明 $J(\chi, \chi) \in \mathbb{Z}[\sqrt{-1}]$;

(2) 若记 $J(\chi, \chi) = a + b\sqrt{-1}$ (其中 $a, b \in \mathbb{Z}$), 则 $p = a^2 + b^2$, 且 a 为奇数, b 为偶数。

问题 4.3. 给定奇素数 p 以及整数 a , $p \nmid a$ 。求

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x^2 - ax}{p} \right).$$

问题 4.4. 证明不定方程

$$x^2 + 5y^2 = 3z^2$$

没有非零整数解, 即不存在整数解 (x_0, y_0, z_0) 满足 $x_0 y_0 z_0 \neq 0$ 。

问题 4.5. 求不定方程

$$x^2 - 2y^2 = 1$$

的全部正整数解。

问题 4.6. 求不定方程

$$x^2 + y^2 + z^2 = 2xyz$$

的全部整数解。

5 参考练习 (2026 年 6 月 4 日)

问题 5.1. 设 p 为奇素数。对于正整数 $1 \leq i \leq p-1$, 令 a_i 是一个满足

$$ia_i \equiv 1 \pmod{p}$$

的正整数。

(1) 证明该和 $\sum_{i=1}^{p-1} a_i \equiv 0 \pmod{p}$ 。

(2) 设 S 为前 $p-1$ 个正整数之和: $1 + 2 + \cdots + (p-1)$ 。证明对于所有素数 $p > 3$ 都有

$$(p-1)! \not\equiv -1 \pmod{S}.$$

问题 5.2. 设 p 和 q 为奇素数。假设 q 能整除梅森数 $M_p = 2^p - 1$ 。证明 $q > p$ 。

问题 5.3. 考虑二次同余式

$$x^2 \equiv a \pmod{p^2},$$

其中 p 为奇素数且 $\gcd(a, p) = 1$ 。

- (1) 设 x_0 是 $x^2 \equiv a \pmod{p}$ 的一个解。证明存在模 p 下唯一的整数 t , 使得 $x_1 = x_0 + tp$ 是该同余式模 p^2 的解。
- (2) 证明: 对任意正整数 k , 方程 $x^2 \equiv a \pmod{p^k}$ 都有解。

问题 5.4. 考虑不定方程

$$x^3 + 2y^3 = 7z^3.$$

- (1) 证明任意整数的立方模 7 必然同余于 0, 1 或 -1。
- (2) 证明方程 $x^3 + 2y^3 = 7z^3$ 仅有平凡解 $x = y = z = 0$ 。

问题 5.5. 考虑方程

$$x^2 - 3y^2 = 1.$$

- (1) 求此方程最小的正整数解 (x_1, y_1) 。

- (2) 通过

$$x_n + y_n\sqrt{3} = (x_1 + y_1\sqrt{3})^n$$

定义解序列 (x_n, y_n) 。证明 x_n 始终为奇数。

- (3) 证明 $\{(x_n, y_n) : n \in \mathbb{Z}_{>0}\}$ 即是此方程所有的正整数解。

问题 5.6. 设 $\mu(n)$ 表示莫比乌斯函数, $\Phi_n(x)$ 表示第 n 个分圆多项式。我们有

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

- (1) 将 $\Phi_n(x)$ 表示为 $x^d - 1$ 的有理函数。
- (2) 设 p 为素数。证明

$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}).$$

问题 5.7. 求 7^{7^7} 除以 100 的余数。

问题 5.8. 设 $a \in \mathbb{Z}$ 和 10 互素。证明

$$a^{20} \equiv 1 \pmod{100}.$$

问题 5.9. 设 $p > 3$ 为素数。假设存在整数 a , 使得 a 在模 p 下的 (乘法) 阶为 3。

- (1) 证明: $p \equiv 1 \pmod{3}$ 。

(2) 证明: $a^2 + a + 1 \equiv 0 \pmod{p}$ 。

(3) 确定 $a + 1$ 模 p 的 (乘法) 阶, 并给出证明。

问题 5.10. 设 p 是一个奇素数, 且 $p \nmid 2026$ 。当 p 满足什么条件时, 同余方程

$$x^2 \equiv 2026 \pmod{p}$$

有解?

问题 5.11. 解不定方程

$$x^2 + y^2 + z^2 = 615.$$

问题 5.12. (1) 证明对于任意素数 p 和正整数 k , 方程

$$x^2 \equiv x \pmod{p^k}$$

只有两个解, 并写出这两个解。

(2) 求同余方程 $x^2 \equiv x \pmod{100}$ 在模 100 意义下的所有解。

问题 5.13. 设 p 为奇素数。

(1) 证明对于任意整数 $0 \leq k \leq p-1$, 组合数 $\binom{p-1}{k}$ 满足同余式

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

(2) 计算

$$\sum_{k=0}^{p-1} \binom{p-1}{k}^2$$

模 p 的余数。

问题 5.14. 考虑有限域 $\mathbb{F}_p$ 上的线性方程组 (其中 $p > 3$ 为素数):

$$\begin{cases} ax + 2y \equiv 3 \pmod{p}, \\ x + ay \equiv 5 \pmod{p}. \end{cases}$$

对于哪些 $a \in \mathbb{F}_p$, 上述方程组有解?

问题 5.15. 设 p 为奇素数, g 是模 p 的一个原根。

(1) 证明: $g^{(p-1)/2} \equiv -1 \pmod{p}$ 。

(2) 对于哪些奇素数 p , $-g$ 仍然是模 p 的原根? 请给出证明。

问题 5.16. 设 n 是严格大于 1 的整数。证明 $n^4 + 4^n$ 一定不是素数。提示：利用恒等式 $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$ 。

问题 5.17. 求方程

$$x^2 + y^2 = 2$$

的所有有理数解。提示：换元 $u = \frac{x+y}{2}$, $v = \frac{x-y}{2}$ 。

问题 5.18. 设 p 为奇素数，且 a 是一个不能被 p 整除的整数。

(1) 证明：

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = -1,$$

其中括号代表 Legendre 符号。提示：利用

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = \sum_{z=0}^{p-1} \left(\frac{z + a}{p} \right) \left(1 + \left(\frac{z}{p} \right) \right)$$

以及 Jacobi 和。

(2) 计算同余方程

$$x^2 - y^2 \equiv a \pmod{p}$$

在模 p 下的解 (x_0, y_0) 的个数。

问题 5.19. 考虑不定方程

$$x^2 + y^2 = z^3.$$

(1) 证明：如果上述方程有整数解 (x_0, y_0, z_0) ，满足 x_0, y_0 互素，那么 x_0 是奇数，且 y_0 是偶数。

(2) 证明在 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 中， $x_0 + y_0\sqrt{-1}$ 和 $x_0 - y_0\sqrt{-1}$ 互素。

(3) 证明存在整数 a, b ，使得

$$\begin{cases} x_0 = a(a^2 - 3b^2), \\ y_0 = b(3a^2 - b^2), \\ z_0 = a^2 + b^2. \end{cases}$$

问题 5.20. 考虑以下线性同余方程组：

$$\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv a \pmod{18}. \end{cases}$$

(1) 证明该方程组有解当且仅当 $a \equiv 5 \pmod{6}$ 。

(2) 设 $a = 11$, 求该方程组的所有解。

问题 5.21. 求所有大于 7 的奇素数, 使得 105 是模 p 的二次剩余。这样的素数的 Dirichlet 密度是多少?

问题 5.22. 记 p 的所有二次剩余为 $a_1, a_2, \dots, a_{(p-1)/2}$ 。证明

$$(x - a_1)(x - a_2) \cdots (x - a_{(p-1)/2}) \equiv x^{(p-1)/2} - 1 \pmod{p}.$$

问题 5.23. 证明不定方程

$$(x^2 - 2)(x^2 - 3)(x^3 - 6) = 0$$

没有整数解, 但对于任意素数 p , 此方程模 p 都有解。

问题 5.24. 考虑三次分圆整数环 $\mathbb{Z}[\omega]$, 其中 $\omega = e^{2\pi\sqrt{-1}/3}$ 。对于任意 $x = a + b\omega \in \mathbb{Z}[\omega]$, 定义其范数为

$$N(x) = a^2 - ab + b^2.$$

设 $\alpha, \beta \in \mathbb{Z}[\omega]$, 且它们的范数 $N(\alpha)$ 与 $N(\beta)$ 都不能被 3 整除。假设 α 和 β 在环 $\mathbb{Z}[\omega]$ 中是互素的。

(1) α, β 在 $\mathbb{Z}$ 中的范数 $N(\alpha)$ 和 $N(\beta)$ 是否一定互素? 如果为真, 请证明; 如果为假, 请提供一个反例。

(2) 设正整数 g 为 $N(\alpha)$ 和 $N(\beta)$ 在 $\mathbb{Z}$ 中的最大公约数。证明 $g \equiv 1 \pmod{3}$ 。

问题 5.25. 证明: 对于任意给定的正整数 k , 都存在无穷多个素数, 其十进制表示的最后 k 位数字全为 1。

问题 5.26. 设 A 为满足 $p \equiv 1 \pmod{3}$ 的素数集合, B 为满足 $p \equiv 3 \pmod{4}$ 的素数集合。分别求集合 A 、集合 B 、集合 $A \cap B$ 的 Dirichlet 密度。

问题 5.27. 证明任意一个等差数列

$$a, a + d, a + 2d, \dots, a + kd, \dots$$

都必定包含一个非素数。

问题 5.28. (1) 设 m 是一个正整数。证明: 若 $p = 2^m + 1$ 是一个素数, 则 m 是 2 的方幂。

(2) 对 $n \geq 0$, 记 $F_n = 2^{2^n} + 1$, 称为 Fermat 数。证明: 若 $m > n$, 则 $F_n \mid (F_m - 2)$ 。

(3) 证明: 若 $m \neq n$, 则 $\gcd(F_m, F_n) = 1$ 。利用这个结论证明素数有无穷多个。

问题 5.29. 求 2026^{618} 在十进制下的最后两位数。

问题 5.30. 设 p 是一个奇素数。证明所有模 p 原根都是模 p 的二次非剩余。对于哪些奇素数 p ，所有的模 p 二次非剩余都是原根？