注意事项：

（1）试卷共 2 页，共 10 题，1-6 题每题各 10 分，其中第 1 题到第 3 题仅选做 1 题，第 7 题到第 10 题每题 15 分，满分 100 分；

（2）证明题要求逻辑严密，计算题要求有计算步骤；

（3）$\mathbf{Z}$ 表示整数集，$\mathbf{Z}^{+}$ 表示正整数集；

（4）试题中的概念、方法、结论与所学课程内容一致。

---

1 试叙述良序性公理（*The Well-Ordering Property*），并用它证明$\sqrt{11}$是无理数(*Irrational*)。

2 证明：设 $a\in\mathbf{Z}$，$b\in\mathbf{Z}^{+}$，存在唯一的 $q,r\in\mathbf{Z}$，使得 $a=bq+r,(0\le r\le b-1)$。

3 设 $a,b,m\in\mathbf{Z}$，$m\in\mathbf{Z}^{+}$，$(a,m)=d$，若 $d\nmid b$，则 $ax\equiv b\,(\mathrm{mod}\,m)$ 无解，若 $d\,|\,b$，则 $ax\equiv b\,(\mathrm{mod}\,m)$ 恰有 d 个模(*Modulo*) m 互不同余的解(*Incongruent Solutions*)。

4 证明：如果 a 和 b 是不全为 0 的整数，那么正整数 d 是 a，b 的最大公因子(*Greatest Common Divisor*)当且仅当(*IF and Only IF*)

[1]. $d\,/\,a$ 且 $d\,/\,b$,

[2]. 如果 c 是整数且 c/a, c/b, 则 c/d。

5 叙述中国剩余定理（*The Chinese Remainder Theorem*），并给出解的表达式，并用它解同余方程（*Solving the congruence*）

$$2x^{3}+7x-4\equiv 0\,(\mathrm{mod}\,200)$$。

6 [1]. 证明同余方程组

$$x\equiv a_1(mod\ m_1)$$
$$x\equiv a_2(mod\ m_2)$$

有解，当且仅当$(m_1,\ m_2)|(a_1-a_2)$。若有解，则模$[m_1,\ m_2]$的解唯一。

[2]. 证明：设 a, b, $c\in\mathbf{Z}$，$m\in\mathbf{Z}^{+}$，$d=(c,\ m)$，$ac\equiv bc(\mathrm{mod}\ m)$

则 $a \equiv b \pmod{m/d}$。

7 √[1]. 证明：若 $r_1, r_2, \ldots, r_{\phi(n)}$ 是一个模 n 的既约剩余系（*Reduced Residue System*），且正整数 a 使得 $(a,n)=1$，那么集合 $ar_1, ar_2, \ldots, ar_{\phi(n)}$ 也是模 n 的既约剩余系。

√[2]. 若 $m \in Z^+$，$a \in Z$，若（a，m）=1，则 $a^{\phi(m)} \equiv 1 \mod m$。

√[3]. 如果 a 和 b 为互素的正整数，那么 $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$。

8 √[1]. 设 f 是积性函数（*Multiplicative Function*），若有素幂分解 $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$ 则：$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_s^{a_s})$。

√[2]. 证明：如果 a 和 b 是正整数，那么 $\emptyset(ab) = (a,b)\emptyset(a)\emptyset(b)/\emptyset((a,b))$ 从而推出当 $(a,b) > 1$ 时，有 $\emptyset(ab) > \emptyset(a)\emptyset(b)$。

9 √[1]. 证明：如果 n 是正整数，且 a 和 b 均是与 n 互素的整数，且 $(\mathrm{ord}_n a,\ \mathrm{ord}_n b) = 1$，那么 $\mathrm{ord}_n(ab) = \mathrm{ord}_n a \times \mathrm{ord}_n b$。

√[2]. 设 m 是一个有原根（*Primitive Roots*）r 的正整数，并且 a 和 b 均是与 m 互素的整数。则有：

（i） $ind_r 1 \equiv 0 (mod \phi(m))$，

（ii） $ind_r(ab) \equiv ind_r a + ind_r b (mod \phi(m))$，

（iii） $ind_r a^k \equiv k \cdot ind_r a (mod \phi(m))$，其中 k 为正整数。

10 √[1]. 设 p 是奇素数，n 是正奇数，且 a 和 b 是整数不被 p 整除，$(a,n)=(b,n)=1$ 那么 若 $a \equiv b \pmod{p}$，那么 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$；若 $a \equiv b \pmod{n}$，则 $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$。

√[2]. 计算 Jacobi 符号 $(\frac{5}{21})$，$\left(\frac{27}{101}\right)$。

√[3]. 设 p 是奇素数，$a \in Z$，且 p 不能整除 a，那么 $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$。