中国科学技术大学《代数学基础》期末考试

2023年03月02日，8：30–10：30

姓名：__________ 学号：__________ 所在院系：__________

题号	一	二	三	四	五	六	七	八	总 分
得分									
复查									

一、(10分) 设 $n \in \mathbb{Z}$ 有标准素因子分解 $n = \varepsilon \prod_{i=1}^{k} p_i^{e_i}$, 其中 $\varepsilon = \pm 1$ 以及 p_i 为两两不同的素数。定义 $\nu_{p_i}(n) = e_i$, 并且令 $\nu_{p_i}(0) = +\infty$. 证明：当 $a, b \in \mathbb{Z}$, 对任意素数 p, 以下结论成立：

(1) 当 $\nu_p(a) \neq \nu_p(b)$, 则有 $\nu_p(a+b) = \min\{\nu_p(a), \nu_p(b)\}$;

(2) 若 $a^p \equiv b^p \pmod p$, 则有 $a^p \equiv b^p \pmod{p^2}$.

二、(15分)

(1) 解一次同余方程 $2^{2023}x \equiv 61 \pmod{221}$. (10分)

(2) 求出一个次数最低的多项式 $f(x) \in \mathbb{F}_5[x]$, 使得 $f(\bar{0}) = f(\bar{1}) = f(\bar{4}) = \bar{1}$, 以及 $f(\bar{2}) = f(\bar{3}) = \bar{3}$.

三、（共10分） 设 $f(x) = x^7 + x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ 和 $g(x) = x^4 + x^2 + x \in \mathbb{F}_2[x]$, 求 $f(x)$ 与 $g(x)$ 的最大公因式 $(f(x), g(x))$, 并求出 $s(x), t(x) \in \mathbb{F}_2[x]$ 使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

四、(20分)设第 n 个费马(Fermat)数 $F_n = 2^{2^n} + 1$. 证明：

(1) 2 模 F_n 的阶为 2^{n+1};

(2) F_n 的素因子 p 满足 $p \equiv 1 (\bmod 2^{n+1})$;

(3) 若 F_n 是素数，则模 F_n 的二次非剩余必为 F_n 的原根；

(4) 若 F_n 是素数，则 ± 3 是模 F_n 的原根。

五、(10分)

(1) 求使得勒让德符号 $\left(\frac{-2}{p}\right) = 1$ 的全体素数 p.

(2) 二元二次不定方程 $x^2 + 2y^2 = 2023$ 是否有整数解？为什么？

六、(20分) 设 $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[x]$ 在复数域 $\mathbb{C}$ 中有一个根为 α, 证明：

(1) $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约，并且 $f(x)$ 没有重根； 4+4

(2) $\alpha^2 - 2$ 也是 $f(x)$ 的根，并求出 $f(x)$ 的全部复根； 4+5+3

(3) $f(x)$ 模 2 约化多项式是 $\mathbb{F}_2[x]$ 中不可约多项式； 5

(4) 8 元有限域是否存在？存在的话请构造说明，不存在的话解释原因。5

1+4

七、（共10分）

(1) 证明 $f(x) = x^6 + 12x^5 + 18x^4 + 24x^3 + 9x^2 + 36x + 6$ 在 $\mathbb{Z}[x]$ 中不可约。

(2) 如果 $f(x)$ 是 $\mathbb{Z}[x]$ 中首一多项式，而 $g(x) \in \mathbb{Q}[x]$ 是 $f(x)$ 的首一多项式因子，那么

$$g(x) \in \mathbb{Z}[x].$$