2022–2023 学年《代数学基础》期末考试

一、求证：

(a) $v_p(a) \neq v_p(b)$ 时，有 $v_p(a+b) = \min\{v_p(a), v_p(b)\}$；

(b) 若 p 为素数，且 $a^p \equiv b^p \pmod{p}$，则 $a^p \equiv b^p \pmod{p^2}$。

二、

(a) 解方程：$2^{2023}x \equiv 61 \pmod{221}$；

(b) 设 $F(x) \in \mathbb{F}_5[x]$，且 $F(\bar{0}) = F(\bar{1}) = F(\bar{4}) = \bar{1}$，$F(\bar{2}) = F(\bar{3}) = \bar{3}$，求次数最小的 F。

三、设 $f(x), g(x) \in \mathbb{F}_2[x]$，$f(x) = x^7 + x^5 + x^2 + 1$，$g(x) = x^4 + x^2 + x$。

(a) 求 $(f(x), g(x))$；

(b) 求 $s(x), t(x) \in \mathbb{F}_2[x]$，使得 $s(x)f(x) + t(x)g(x) = (f(x), g(x))$。

四、记 Fermat 数 $F_n = 2^{2^n} + 1$（$n > 1$），求证：

(a) 2 模 F_n 的阶为 2^{n+1}；

(b) 记 p 为 F_n 的素因子，则 $p \equiv 1 \pmod{2^{n+1}}$；

(c) 若 F_n 为素数，则其二次非剩余均为原根；

(d) 若 F_n 为素数，则 ± 3 为其原根。

五、设 $f(x) = x^3 + x^2 - 2x - 1$，其一个复根为 α，求证：

(a) $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约，且无重根；

(b) $\alpha^2 - 2$ 也是 $f(x)$ 的根，并求出所有根；

(c) 考虑 $f(x)$ 在 $\mathbb{F}_2[x]$ 上的约化多项式 $g(x)$，证明其不可约；

(d) 是否存在八元有限域？若存在，请构造说明；若不存在，请给出理由。

六、

(a) 求所有素数 p 使得 $\left(\dfrac{-2}{p}\right) = 1$；

(b) 不定方程 $x^2 + 2y^2 = 2023$ 是否有整数解？

七、设 $f(x)$ 为 $\mathbb{Z}[x]$ 中的首一多项式，$g(x) \in \mathbb{Q}[x]$ 为其一个首一因子，求证：$g(x) \in \mathbb{Z}[x]$。