NB: Please deposit your solutions in the appropriate box **by 4 p.m. on the due date.** Late assignments or assignments placed into incorrect boxes will not be marked. Use a mathematics department cover sheet. These are available from outside the Resource Centre. PLEASE SHOW ALL WORKING. Also if we believe you have COPIED someone else's script or that you have let someone else COPY YOUR SCRIPT, then you will get NO MARKS.

1. Use the Euclidean algorithm to find a $\gcd(x^4 + 3x^3 - 3x - 1, x^4 + 2x^3 - 2x - 1)$ in $\mathbb{R}[x]$. Show the steps in the calculation.

2. Suppose that a and p are relatively prime numbers in $\mathbb{N}$. We'll write $\overline{a}\overline{b}$ or, sometimes $\overline{a} \cdot \overline{b}$ as a shorthand for $\overline{a} \cdot_p \overline{b}$.

(a) Explain why $\overline{a}, \overline{2}\overline{a}, \cdots, \overline{(p-1)}\overline{a}$ are $p-1$ distinct congruence classes in $\mathbb{Z}_p$.

(b) Conclude that $\{\overline{a}, \overline{2}\overline{a}, \cdots, \overline{(p-1)}\overline{a}\} = \mathbb{Z} \setminus \{\overline{0}\}$.

(c) Show that

$$\overline{a} \cdot \overline{2}\overline{a} \cdot \ \cdots \ \cdot \overline{(p-1)}\overline{a} = \overline{(p-1)}!$$

. (Here $\overline{(p-1)}!$ means $\overline{1} \cdot \overline{2} \cdot \ \cdots \ \cdot \overline{(p-1)}$.)

(d) Deduce that if p is prime then for any non-zero $a \in \mathbb{N}$ we have $\overline{a}^p = \overline{a}$ in $\mathbb{Z}_p$.

3. Let $\mathbb{K}$ mean one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}_p$. Let $a(x)$ and $b(x)$ be polynomials in $\mathbb{K}[x]$. Prove that a lowest degree non-zero polynomial of the form $a(x)u(x) + b(x)v(x)$ (for any $u(x), v(x) \in \mathbb{K}[x]$) is a $\gcd(a(x), b(a))$. (Hint: Follow the idea of the corresponding result for the integers.)