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. **soln:**

$$x^4+3x^3-3x-1 = 1(x^4+2x^3-2x-1)+(x^3-x)$$

$$x^4+2x^3-2x-1 = (x+2)(x^3-x)+(x^2-1)$$

$$x^3-x = x(x^2-1).$$

So x^2-1 (or any real multiple of this) is a gcd. [4 marks]

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 $\overline{a},\overline{2a},\cdots,\overline{(p-1)a}$ are $p-1$ distinct congruence classes in $\mathbb{Z}_p$.
soln: Since a and p are relatively prime $\overline{a}$ is invertible in $\mathbb{Z}_p$. Thus $\overline{ab}=\overline{ac}$ is equivalent to $\overline{b}=\overline{c}$. [2 marks]

(b) Conclude that $\{\overline{a},\overline{2a},\cdots,\overline{(p-1)a}\}=\mathbb{Z}\setminus\{\overline{0}\}$.
soln: None of $\overline{a},\overline{2a},\cdots,\overline{(p-1)a}$ is $\overline{0}$ since $\overline{a}$ is invertible and none of $\overline{1},\overline{2},\cdots,\overline{p-1}$ is zero in $\mathbb{Z}_p$. So $\{\overline{a},\overline{2a},\cdots,\overline{(p-1)a}\}$ is a subset of $\mathbb{Z}\setminus\{\overline{0}\}$. Since both sets have cardinality $p-1$ we are done. [3 marks]

(c) Show that

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

. (Here $\overline{(p-1)!}$ means $\overline{1}\cdot\overline{2}\cdot\quad\cdots\quad\cdot\overline{(p-1)}$.)
soln: Since $\{\overline{a},\overline{2a},\cdots,\overline{(p-1)a}\}=\mathbb{Z}\setminus\{\overline{0}\}$ multiplying out the elements of $\{\overline{a},\overline{2a},\cdots,\overline{(p-1)a}\}$ is the same as multiplying out the elements of $\mathbb{Z}\setminus\{\overline{0}\}$. [2 marks]

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

$$\overline{a}^{p-1}\cdot\overline{(p-1)!}=\overline{(p-1)!}.$$

If p is prime then p and $(p-1)!$ are relatively prime. So $(p-1)!$ is invertible in $\mathbb{Z}_p$. Thus we can 'cancel' it from each side to get

$$\overline{a}^{p-1}=\overline{1}.$$

Now mulitplying both sides by $\overline{a}$ gives

$$\overline{a}^p=\overline{a}.$$

[4 marks]
Well done you've just proved Fermat's "little" theorem.

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.)
soln: By the division algorithm we have

$$a(x) = [a(x)u(x) + b(x)v(x)]q(x) + r(x),$$

where $q(x), r(x) \in \mathbb{K}[x]$ with deg$r(x)$ <deg$(a(x)u(x) + b(x)v(x))$. But $r(x) = a(x)(1 - u(x)q(x)) - b(x)v(x)$ so it must vanish otherwise it will contradict the assumption that there are no non-zero polynomials of the form $a(x)s(x) + b(x)t(x)$ with degree less than the degree of $a(x)u(x) + b(x)v(x)$. So $r(x) = 0$ which means $a(x)u(x) + b(x)v(x)$ divides $a(x)$. An almost identical argument shows that $a(x)u(x)+b(x)v(x)$ also divides $b(x)$. On the other hand if $c(x) \in \mathbb{K}[x]$ divides $a(x)$ and $b(x)$ then this means $a(x) = d(x)c(x)$ and $b(x) = e(x)c(x)$, for some $d(x), e(x) \in \mathbb{K}[x]$, and so $a(x)u(x) + b(x)v(x) = [d(x)u(x) + e(x)v(x)]c(x)$. That is $c(x) \mid a(x)u(x) + b(x)v(x)$. Thus $a(x)u(x) + b(x)v(x)$ is a greatest common divisor.

[8 marks]