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.

1. (**15 marks**) Let $n \in \mathbb{N}$ and let $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ be a function from $\mathbb{Z}_n$ to itself.

(a) If φ is one-to-one, then show that φ is onto.

(b) If φ is onto, then show that φ is one-to-one.

(c) Define $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\psi(\bar{x}) = \bar{a} \cdot_n \bar{x}$. Suppose a and n are relatively prime. Show that ψ is one-to-one and onto.

2. (**10 marks**) Use congruence to show that for every $n \in \mathbb{N}$, $3^{4n+1} + 4^{n+1}$ is divisible by 7.

3. (**15 marks**)

(a) Find all integers $x \in \mathbb{Z}$ such that

$$4x^2 - x + 2 \equiv 0 \pmod{5}.$$

(b) Find all integers $x \in \mathbb{Z}$ such that

$$25x \equiv 10 \pmod{30}.$$

4. (**10 marks**) Let $f(x), g(x)$ and $h(x)$ be polynomials in $\mathbb{Z}_5[x]$ defined by

$$f(x) = x^5 + 2x^2 + x + 4, \quad g(x) = x^4 + 2x^3 + 4x^2 + 4x - 1, \quad h(x) = 3x^2 + 2.$$

Here for simple, we denote $\bar{a}$ by a for $\bar{a} \in \mathbb{Z}_5$.

(a) Find quotient $q(x)$ and remainder $r(x)$ when $f(x)$ is divided by $h(x)$.

(b) Find a greatest common divisor $d(x)$ of $f(x)$ and $g(x)$,