1. (a) (**4 marks**) Suppose φ is one-to-one. Then $\varphi(\bar{x}) \neq \varphi(\bar{y})$ for distinct $\bar{x}, \bar{y} \in \mathbb{Z}_n$, so that the image $\varphi(\mathbb{Z}_n)$ contains n elements. But $\varphi(\mathbb{Z}_n)$ is a subset of $\mathbb{Z}_n$ and $\mathbb{Z}_n$ has n elements, so $\varphi(\mathbb{Z}_n) = \mathbb{Z}_n$ and φ is onto.

(b) (**4 marks**) Suppose φ is onto. If φ is not one-to-one, then $\varphi(\bar{x}) = \varphi(\bar{y})$ for some $\bar{x} \neq \bar{y}$, so that the number of elements in $\varphi(\mathbb{Z}_n)$ is less than n and φ is not onto. This contradiction implies that φ is one-to-one.

(c) (**7 marks**) Suppose $\gcd(a, n) = 1$. Then $\bar{a}$ is invertible in $\mathbb{Z}_n$, that is, there is some $\bar{b} \in \mathbb{Z}_n$ such that $\bar{a} \cdot_n \bar{b} = \bar{1}$.

Suppose $\psi(\bar{c}) = \psi(\bar{d})$ for some $\bar{c}, \bar{d} \in \mathbb{Z}_n$. Then $\bar{a} \cdot_n \bar{c} = \bar{a} \cdot_n \bar{d}$, so $\bar{b} \cdot_n \bar{a} \cdot_n \bar{c} = \bar{b} \cdot_n \bar{a} \cdot_n \bar{d}$, that is, $\bar{1} \cdot_n \bar{c} = \bar{1} \cdot_n \bar{d}$ and $\bar{c} = \bar{d}$, it follows that ψ is one-to-one and by (a) above it is onto.

2. (**3 marks**) For $n \in \mathbb{N}$, $7 \mid 3^{4n+1} + 4^{n+1} \iff 3^{4n+1} + 4^{n+1} \equiv 0 \pmod 7$.

Now (**7 marks**)

$$\begin{aligned} 3^{4n+1} + 4^{n+1} &\equiv (3^4)^n \cdot 3 + 4^n \cdot 4 \\ &\equiv ((9)^2)^n \cdot 3 + 4^n \cdot 4 \\ &\equiv (2^2)^n \cdot 3 + 4^n \cdot 4 \\ &\equiv 4^n \cdot 3 + 4^n \cdot 4 \\ &\equiv 4^n \cdot 7 \\ &\equiv 0 \pmod 7, \end{aligned}$$

so $7 \mid 3^{4n+1} + 4^{n+1}$.

3. (a) (**6 marks**) $4x^2 - x + 2 \equiv 0 \pmod 5 \iff 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{0}$ in $\mathbb{Z}_5$. Now

$$\begin{aligned} \bar{x} = \bar{0} &\implies 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{2} \\ \bar{x} = \bar{1} &\implies 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{0} \\ \bar{x} = \bar{2} &\implies 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{3} \\ \bar{x} = \bar{3} &\implies 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{0} \\ \bar{x} = \bar{4} &\implies 4\bar{x}^2 - \bar{x} + \bar{2} = \bar{2}. \end{aligned}$$

Thus $\bar{x} = \bar{1}$ and $\bar{3}$ are the solutions in $\mathbb{Z}_5$, and so (**2 marks**) $x \in \bar{1} \cup \bar{3}$ are solutions, that is, $x \in \{5k+1, 5k+3 : k \in \mathbb{Z}\}$.

(b) (**3 marks**) $25x \equiv 10 \pmod{30} \iff 25x + 30y = 10$ for some $y \in \mathbb{Z} \iff 5x + 6y = 2$ for some $y \in \mathbb{Z} \iff 5x \equiv 2 \pmod 6$. $\iff \bar{5} \cdot_6 \bar{x} = \bar{2}$ in $\mathbb{Z}_6$.

(**4 marks**) Now

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{5} \cdot_6 \bar{x}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Thus $5x \equiv 2 \pmod 6$. $\iff \bar{x} = \bar{4} \iff x \in \bar{4}$, that is, $x \in \{6k + 4 : k \in \mathbb{Z}\}$.

4. (a) (**5 marks**) Note

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{3} \cdot_5 \bar{x}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$

Thus $3^{-1} = 2$ in $\mathbb{Z}_5$, and $f(x) = (3x^2+2)(2x^3+2x+4) + (2x+1)$. So $q(x) = 2x^3+2x+4$, $r(x) = 2x+1$.

(b) (**5 marks**)

$$f(x) = g(x)(x-2) + (x^2+2)$$
$$g(x) = (x^2+2)(x^2+2x+2) + 0.$$

Thus (x^2+2) is a greatest common divisor.