4. **[6 marks] Number theory.**

(a) **[3 marks]** Prove the following statement:

$$\forall m \in \mathbb{Z}^+,\ \forall c \in \mathbb{Z},\ c \equiv c \pmod{m}$$

Your proof must use the definitions of modular equivalence and divisibility, and may **not** use any theorems found on the Reference Sheets, nor any other theorems/properties of divisibility or modular equivalence. We have left space for rough work here, but please write your formal proof in the box below.

Proof.

Definition of modular equivalence: $a \equiv b \pmod{m} \iff m \mid a-b \iff m \mid b-a$

Definition of divisibility: $d \mid n \iff \exists k \in \mathbb{Z},\ n = kd$ (where $d, n \in \mathbb{Z}$)

Let m be an arbitrary positive integer

Let c be an arbitrary integer

Want to show: $c \equiv c \pmod{m}$ equivalent to $m \mid c-c$ or $m \mid 0$ (using definition of modular equivalence)

Now $m \mid 0$ is equivalent to $\exists k \in \mathbb{Z},\ 0 = k(m)$, where $m, 0 \in \mathbb{Z}$

Take k to be 0, which $\in \mathbb{Z}$

Thus $0 = 0(m) \Rightarrow 0 = 0$, which is a fact.

Therefore $m \mid 0$ and thus $c \equiv c \pmod{m}$.

Hence Proved.

(b) **[3 marks]** Prove the following statement:

$$\forall n, m, d \in \mathbb{Z}, \big((n \neq 0 \vee m \neq 0) \wedge d \mid m \wedge d \mid n\big) \Rightarrow d \mid \gcd(n, m)$$

Your proof **may** use any definitions and theorems provided on the Reference Sheets, but no other theorems/properties of divisibility or modular equivalence.

We have left space for rough work here, but please write your formal proof in the box below.

Proof.

Let $n, m, d \in \mathbb{Z}$

what to show: $((n \neq 0 \vee m \neq 0) \wedge d \mid m \wedge d \mid n) \Rightarrow d \mid \gcd(n, m)$

Assume that $(n \neq 0 \vee m \neq 0) \wedge d \mid m \wedge d \mid n$

Since $m, n \in \mathbb{Z}$ and at least one of them is non zero, using GCD characterization Theorem, $\gcd(m, n)$ is the smallest positive integer that is a linear combination of m and n. Equivalently $\exists p, q \in \mathbb{Z}$ such that $\gcd(n, m) = pn + qm$

Since $d, m, n, p, q \in \mathbb{Z}$ and $d \mid m$ and $d \mid n$, using Divisibility of Linear Combinations Theorem $d \mid pn + qm$. Equivalently $d \mid \gcd(n, m)$.

Hence proved. ∎