SECTION D

Attempted questions: 7

Attached question: 7

$\forall x, y \in \mathbb{Z}$

7\. a. $\wedge\ x \equiv y \pmod{n} \Rightarrow an + x = bn + y$ for some $a, b \in \mathbb{Z}$

$\Rightarrow bn + y = an + x$

$\Rightarrow y \equiv x \pmod{n}$

$\therefore x \equiv y \pmod{n}$ is symmetric

$\forall x \in \mathbb{Z}.\ x = x + 0n$

$\therefore x \equiv x \pmod{n}$

$\therefore x \equiv y \pmod{n}$ is reflexive

$\forall x, y, z \in \mathbb{Z}.\ x \equiv y \pmod{n} \wedge y \equiv z \pmod{n}$

$\Rightarrow an + x = bn + y \wedge cn + y = dn + z$ for some $a, b, c, d \in \mathbb{Z}$

$\Rightarrow (a + c - b)n + x = cn + y = dn + z$

$\Rightarrow (a + c - b)n + x = dn + z$

$(a + c - b) \in \mathbb{Z}$

$\therefore x \equiv z \pmod{n}$

$\therefore x \equiv y \pmod{n}$ is transitive

$\therefore x \equiv y \pmod{n}$ is an equivalence relation

b. Given a pair of positive natural numbers (m, n) (without loss of generality, take $m > n$), write m as a multiple p of n plus some remainder r such that $r < n$. Repeat this with n and r in place of m and n respectively. Continue iterating until $r = 0$. The last non-zero value of r (equivalently, the last value of m) is $\gcd(m, n)$. Rearrange this equation from the form $m = pn + r$ to $r = m - pn$. Substitute n for the previous value of r, for which you must rearrange the previous equation in a similar manner. The equation will be of the form: $r_k = m_k - p_k(m_{k-1} - p_{k-1} m_k)$ so expand and group the m_k terms to get $r_k = (1 + p_k p_{k-1}) m_k - p_k m_{k-1}$. Repeatedly substitute m_k, until you are left with $\gcd(m, n) = am + bn$ for some $a, b \in \mathbb{Z}$

c i. Let $m_1 = m^{-1} \pmod n$
$n_1 = n^{-1} \pmod m$
which must exist since m and n are coprime.

Let $x = rnn_1 + smm_1$

RTP: ~~...~~ $x \equiv r \pmod m \wedge x \equiv s \pmod n$

1) RTP: $x \equiv r \pmod m$

$$x \equiv (rnn_1 + smm_1) \pmod m$$
$$\equiv rnn_1 \pmod m$$
$$\equiv r \cdot 1 \pmod m \text{ since } n \cdot n_1 \equiv 1 \pmod m \text{ by definition}$$
$$\equiv r \pmod m \text{ as required}$$

2) RTP: $x \equiv s \pmod n$

$$x \equiv (rnn_1 + smm_1) \pmod n$$
$$\equiv smm_1 \pmod n$$
$$\equiv s \cdot 1 \pmod n \text{ since } mm_1 \equiv 1 \pmod n \text{ by definition}$$
$$\equiv s \pmod n \text{ as required}$$

$\square$

ii. Let x, y such that $x \equiv r \pmod m \wedge x \equiv s \pmod n \wedge$
$y \equiv r \pmod m \wedge y \equiv s \pmod n$

RTP: $x \equiv y \pmod{mn}$

$x \equiv y \pmod m$
$\therefore (x-y) = am$ for some $a \in \mathbb{Z}$
$x \equiv y \pmod n$
$\therefore (x-y) = bn$ for some $b \in \mathbb{Z}$
m and n are coprime,
$\therefore (x-y) = abmn$.
$ab \in \mathbb{Z}$, $\therefore x - y \equiv 0 \mod (mn) \therefore x \equiv y \mod (mn)$
as required.