This problem set is about the Chinese Remainder Theorem.

1. Prove the following propositions.

(a) Assume $p, q \in \mathbb{N}$ are coprime. Given any $m, n \in \mathbb{Z}$, there exists a unique $l \in \mathbb{Z}$ with $0 \leq l < pq$, such that, for any $x \in \mathbb{Z}$,

$$\begin{aligned} x &\equiv m \mod p \\ x &\equiv n \mod q \end{aligned}$$

if and only if

$$x \equiv l \mod pq.$$

(*Hint.* Define $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$ by $f(n + pq\mathbb{Z}) = (n + p\mathbb{Z}, n + q\mathbb{Z})$. Check that f is a well defined function and a group isomorphism.)

(b) (Chinese Remainder Theorem) Assume $p_1, \cdots, p_k \in \mathbb{N}$ are pairwise coprime. Given any $n_1, \cdots, n_k \in \mathbb{Z}$, there exists a unique $l \in \mathbb{Z}$ with $0 \leq l < p_1 \cdots p_k$, such that, for any $x \in \mathbb{Z}$,

$$\begin{aligned} x &\equiv n_1 \mod p_1 \\ \cdots &\quad \cdots \quad \cdots \\ x &\equiv n_k \mod p_k \end{aligned}$$

if and only if

$$x \equiv l \mod p_1 \cdots p_k.$$

(*Hint.* Use part (a), and do a mathematical induction on k.)

2. Prove the following propositions, (which tell you how to find the l in the Chinese Remainder Theorem.)

(a) If $p_1, \cdots, p_k \in \mathbb{N}$ are pairwise coprime, then there exits $a_1, \cdots, a_k \in \mathbb{N}$ such that, for $i = 1, 2, \cdots, k$,

$$a_i(p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k) \equiv 1 \mod p_i.$$

(b) If $p_1, \cdots, p_k$ and $a_1, \cdots, a_k$ are as in part (a), for any $n_1, \cdots, n_k \in \mathbb{Z}$,

$$\begin{aligned} x &\equiv n_1 \mod p_1 \\ \cdots &\quad \cdots \quad \cdots \\ x &\equiv n_k \mod p_k \end{aligned}$$

if and only if

$$x \equiv \sum_{i=1}^{k} n_i a_i (p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k) \mod p_1 \cdots p_k.$$

3. Find the set of all integers x satisfying

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$