Alex Valentino Assignment 11 problem 5
300H

Lemma: $Mult(m_1, \ldots, m_k)$ is an ideal.
Suppose $m_1, \ldots, m_k \in \mathbb{Z}$. We must show $Mult(m_1, \ldots, m_k)$ is an ideal. By definition we must show that $Mult(m_1, \ldots, m_k)$ is closed under addition and integer multiplication.

- We must show that $Mult(m_1, \ldots, m_k)$ is closed under addition. Suppose $a, b \in Mult(m_1, \ldots, m_k)$. We must show that $a + b \in Mult(m_1, \ldots, m_k)$. By definition of being members of $Mult(m_1, \ldots, m_k)$, for all $i \in [k], m_i \mid a, m_i \mid b$. By definition of division there exists $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$ such that $m_i a_i = a, m_i b_i = b$ for all $i \in [k]$. Adding both equations together yields $m_i(a_i + b_i) = a + b$. Therefore by definition of divides $m_i \mid a + b$ for all $i \in [k]$. Therefore by definition $a + b \in Mult(m_1, \ldots, m_k)$.

- We must show that $Mult(m_1, \ldots, m_k)$ is closed under integer multiplication. Suppose $j \in Z, a \in Mult(m_1, \ldots, m_k)$. We must show $ja \in Mult(m_1, \ldots, m_k)$. By definition of being a member of $Mult(m_1, \ldots, m_k)$, for all $i \in [k], m_i \mid a$. Therefore by definition of divides there exists $a_1, \ldots, a_k \in \mathbb{Z}$ such that $m_i a_i = a$ for all $i \in [k]$. Multiplying both sides by j yields $m_i j a_i = ja$. Since $\mathbb{Z}$ is closed under multiplication $ja_i \in \mathbb{Z}$. Therefore by the definition of division $m_i \mid ja$. By the definition of being a member of $Mult(m_1, \ldots, m_k)$, $ja \in Mult(m_1, \ldots, m_k)$.

Let $(b_1, \ldots, b_k)$ and $(m_1, \ldots, m_k)$ be two sequences of integers where all of the m_i are positive. Let S be the set of integers n such that for all $i \in \{1, \ldots, k\}$, $n \equiv_{m_i} b_i$. Suppose $n_0 \in S$. Prove that $S = \{n_0 + j * lcm(m_1, \ldots, m_k) : j \in \mathbb{Z}\}$. Suppose $a \in S$. We must show that $a = n_0 + j * lcm(m_1, \ldots, m_k)$. By definition of being a member of S, for all $i \in [k], a \equiv_{m_i} b_i$. Since n_0 also has this property, then for all $i \in [k], a \equiv_{m_i} n_0$. Therefore we have by algebraic manipulation $a - n_0 \equiv_{m_i} 0$. Therefore $a - n_0$ is a multiple of every $m_1, \ldots, m_k$. Therefore $a - n_0 \in Mult(m_1, \ldots, m_k)$. Since $Mult(m_1, \ldots, m_k) = Mult(lcm(m_1, \ldots, m_k))$ as $Mult(m_1, \ldots, m_k)$ is an ideal and $lcm(m_1, \ldots, m_k)$ is it's smallest element, then there exists a $j \in \mathbb{Z}$ such that $a - n_0 = j * lcm(m_1, \ldots, m_k)$. Therefore by algebraic manipulation $a = n_0 + j * lcm(m_1, \ldots, m_k)$.