Mario Sai

CS 155 Problem Set 9

I pledge my honor that I have abided by the Stevens Honor System. MSai

1. If each m_i divides A, this means that each m_i is a factor of A. Multiplying factors of A together will yield other factors of A as long as the product is less than A, as shown below:

$$m_1 \mid A \Rightarrow xm_1 = A \Rightarrow m_1 = \frac{A}{x} \quad \wedge \quad x \mid A$$
$$m_2 \mid A \Rightarrow ym_2 = A \quad m_2 = \frac{A}{y} \quad y \mid A \quad (x \text{ and } y \text{ are all factors of } A)$$
$$A_1 m_2 = \frac{A}{x} \cdot \frac{A}{y}$$
$$m_1 m_2 = \frac{A^2}{xy}$$
$$\left(\frac{xy}{A}\right) m_1 m_2 = A$$

$m_1 m_2$ divides A as long as $\frac{xy}{A}$ is an integer. Because x and y are factors of A, $\frac{xy}{A} \in \mathbb{Z}$ if $xy \geq A$, which can only happen if $m_1, m_2 \leq A$. Therefore, $m_1 m_2 \mid A$ only if $m_1, m_2 < A$, and applying this repetitively gives $m < A \Rightarrow m \mid A$.

Thus, as long as $m < A$, $m \mid A$. This is true because $m_i \; \forall i < n$ are all relatively prime. Because they are pairwise relatively prime and are factors of A as established earlier, then $m_i \; \forall i < n$ either represents the prime factorization of A or a subset of the prime factorization, e.g. for 56, 7 and 4 represents $7 \cdot 2^2$. Thus, the product can never exceed A, and $m < A$ fulfills $m \mid A$.

2. If X and Y are the solutions to the system of congruences, then

$$X \equiv Y \equiv a_i \bmod m_i \text{ for all } i, \; 1 \leq i \leq n$$

This means that $Y - X \equiv 0 \bmod m_i$,

which implies that $m_i \mid (Y - X) \; \forall i : 1 \leq i \leq n$.

From the previous problem, the m_i's are also pairwise relatively prime and $m_i \mid (Y - X)$, so we can say the product divides $(Y - X)$.

Thus, $m \mid (Y - X)$, which means $Y - X \equiv 0 \bmod m$.

Addition gives $Y \equiv X \bmod m$, therefore any two solutions are congruent mod m.

3. $x \equiv 2 \bmod 4$
$x \equiv 4 \bmod 5$
$x \equiv 3 \bmod 9$
$m = 9 \cdot 5 \cdot 9 = 180$

$m_1 = 45$
$45^{-1} \bmod 4 \equiv 1^{-1} \bmod 4 \equiv 1 \bmod 4$

$m_2 = 36$
$36^{-1} \bmod 5 \equiv 1^{-1} \bmod 5 \equiv 1 \bmod 5$

$m_3 = 20$
$20^{-1} \bmod 9 \equiv 2^{-1} \bmod 9 \equiv 5 \bmod 9$

$x = 2 \cdot 1 \cdot 45 + 4 \cdot 1 \cdot 36 + 3 \cdot 20 \cdot 5$
$90 + 144 + 300$
$x = 534 \bmod 180$
$x \equiv 174 \bmod 180$

EC. $x \equiv r_1 \bmod m_1 \iff x = q_1 m_1 + r_1$ for some $q_1 \in \mathbb{Z}$
$x \equiv r_2 \bmod m_2 \iff x = q_2 m_2 + r_2$ for some $q_2 \in \mathbb{Z}$.

$q_1 m_1 + r_1 = q_2 m_2 + r_2$

$\gcd(m_1, m_2) = d \iff \frac{m_1}{y_1} = d \iff m_1 = d y_1$
$\frac{m_2}{y_2} = d \iff m_2 = d y_2$

$q_1 y_1 d + r_1 = q_2 y_2 d + r_2$
$r_1 = q_2 y_2 d - q_1 y_1 d + r_2$
$r_1 = (q_2 y_2 - q_1 y_1) d + r_2$
let $(q_2 y_2 - q_1 y_1) = c$, $c \in \mathbb{Z}$

$r_1 = cd + r_2 \iff r_1 \equiv r_2 \bmod d$