Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 points]** State the Chinese Remainder Theorem (CRT).

Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime

The system of congruences

$$x \equiv a_1 \mod m_1$$
$$x \equiv a_2 \mod m_2$$
$$\vdots$$
$$x \equiv a_k \mod m_k$$

has a solution, and this solution is unique modulo M, where $M = m_1 m_2 \cdots m_k$.

2. **[3 points]** Give the correspondence between $\mathbb{Z}_{12}$ and the set $\{(a_1, a_2)\colon\ a_1 \in \mathbb{Z}_4 \text{ and } a_2 \in Z_3\}$ implied by the CRT.

Z_{12}	Pairs
0	(0, 0)
1	(1, 1)
2	(2, 2)
3	(3, 0)
4	(0, 1)
5	(1, 2)
6	(2, 0)
7	(3, 1)
8	(0, 2)
9	(1, 0)
10	(2, 1)
11	(3, 2)

3. **[5 points]** Find a solution to the following system of congruences, if one exists.

$$\begin{aligned} 12x &\equiv 50 \pmod{77} \\ x &\equiv 4 \pmod{9} \\ x &\equiv 21 \pmod{40} \end{aligned}$$

$77 = 7 \cdot 11$, $9 = 3^2$, $40 = 2^3 \cdot 5$ — pairwise relatively prime

$M = 77 \cdot 9 \cdot 40 = 27720$.

In $\mathbb{F}_{77}$: find $(12)^{-1}$.

$77 = 6 \cdot 12 + 5$

$12 = 2 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12$

$= 5(77 - 6 \cdot 12) - 2 \cdot 12 = 5 \cdot 77 - 32 \cdot 12$

So $(12)^{-1} \equiv -32 \equiv 45$ and $12x \equiv 50$ is equiv to $x \equiv (50)(45) \equiv 17 \pmod{77}$

no longer needed after change in problem

i	m_i	z_i	y_i	a_i
1	77	360	$(52)^{-1} = -37$	17
2	9	3080	$(2)^{-1} = 5$	4
3	40	693	$(13)^{-1} = -3$	21

$(52)^{-1}$:

$77 = 1 \cdot 52 + 25$

$52 = 2 \cdot 25 + 2$

$25 = 12 \cdot 2 + 1$

$1 = 25 - 12 \cdot 2 = 25 - 12 \cdot (52 - 2 \cdot 25) = 25 \cdot 25 - 12 \cdot 52$

$= 25(77 - 1 \cdot 52) - 12 \cdot 52 = 25 \cdot 77 - 37 \cdot 52$

So $(52)^{-1} = -37 \pmod{77}$

$(13)^{-1}$: $40 = 3 \cdot 13 + 1$, $1 = 40 - 3 \cdot 13$, so $(13)^{-1} = -3 \pmod{40}$.

By CRT: $x = a_1 z_1 y_1 + a_2 z_2 y_2 + a_3 z_3 y_3$

$= 17 \cdot 360 \cdot (-37) + 4 \cdot 3080 \cdot 5 + 21 \cdot 693 \cdot (-3)$

$= -226440 + 61600 - 43659 = -208499 \equiv \boxed{13261 \bmod M}$