These solutions are written at the request of students. Please let me know if you don't understand these solutions; I'm happy to expand on them if necessary.

1. **An Expanded Chinese Remainder Theorem:** Given $x \in M_m$ and $y \in M_n$ where $\gcd(m, n) = 1$, there is a unique $z \in M_{mn}$ such that

$$z \equiv x \bmod m$$
$$z \equiv y \bmod n.$$

Prove this statement as follows:

(a) Prove that $z = xnn^{-1} + ymm^{-1}$, where n^{-1} is the inverse of n modulo m and m^{-1} is the inverse of m modulo n, satisfies the equations.

Solution: We need to see that $z \equiv x \bmod m$ and $z \equiv y \bmod n$. These are both more or less the same, so we'll only show the first one: $z \equiv x \bmod m$. Recall that n^{-1} is the inverse of n modulo m. That is, n^{-1} is the integer so that $nn^{-1} \equiv 1 \bmod m$. This means that $xnn^{-1} \equiv x \bmod m$. On the other hand, $ymm^{-1} \equiv 0 \bmod m$, as it is a multiple of m. Thus $z = xnn^{-1} + ymm^{-1} \equiv x + 0 \equiv x \bmod m$.

(d) Can you state (and prove?) a general Chinese remainder theorem?

Solution: The general version simply takes more values of x (and y) and more values of m (and n). We number them, and state the theorem as follows:

> Given $m_1, m_2, \ldots, m_k$ all pair-wise relatively prime (that is, $\gcd(m_i, m_j) = 1$ if $i \neq j$) and $x_1, x_2, \ldots, x_k$ so that $\gcd(x_j, m_j) = 1$ (so that x_j represents an element of M_{m_j}), then there is a unique $z \in M_{m_1 m_2 \cdots m_k}$ such that
>
> $$z \equiv x_j \bmod m_j, \qquad j = 1, \ldots, k.$$

The proof is similar, except now each term has an inverse for every other m_j. That is, the first term is $x_1 m_2 m_2^{-1} m_3 m_3^{-1} \cdots m_k m_k^{-1}$, where each of these inverses is in M_{m_1} (that is, the inverse of m_3 is the integer m_3^{-1} such that $m_3 m_3^{-1} \equiv 1 \bmod m_1$). The next term has x_2 and inverses of all m_j *except* m_2, and here the inverses are with respect to m_2. This is, of course, complicated to write down without notation. I would probably write this as

$$z = \sum_{j=1}^{k} x_j \prod_{i \neq j} m_i m_i^{-1},$$

where $\prod$ is a product sign (as $\sum$ is a summation sign), and m_i^{-1} means the multiplicative inverse of m_i modulo m_j. This seems fairly complicated though.