Words before the solution: As information provided to us could have been in error, it is very important for us to have the capability to tell whether the information might have been incorrect, and when this happens and if we can, find the correct statement or information. This exercise will help us to get such training, and to understand the CRT better.

(2.20) Let $a, b, m, n$ be integers with $gcd(m, n) = 1$. Let
\[ c \equiv (b - a)m^{-1} \pmod{n}. \]
Prove that $x = a + cn$ is a solution to
\[ x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}, \]
and that every solution to this system has the form $x = a + cn + umn$, for some $y \in \mathbb{Z}$.

Solution: This is not a correct statement. Here is an example to indicate that the exercise is not right. Let $m = 3$, $n = 5$, $a = 2$ and $b = 4$. Then $gcd(3, 5) = 1$. Moreover, the Euclidean Algorithm computation tells us that $1 = (2)(3) + (-1)(5)$, and so $m^{-1} \equiv 3^{-1} \equiv 2 \pmod{5}$. Hence $c = (b - a)m^{-1} = (4 - 2)(2) = 4 \pmod{5}$. Let $x = a + cn = 2 + 4 \cdot 5 = 22$. But $x = 22 \equiv 1 \pmod{3}$ and $x \equiv 2 \pmod{5}$, not a solution to
\[ x \equiv 2 \pmod{3} \text{ and } x \equiv 4 \pmod{5}. \]
Therefore, this statement is false.

What is the correct statement? Please review what we have discussed in class on the Chinese Remainder Theorem, before answering this question. One of the key point in the discussion is that we can first use Euclidean Algorithm to compute integers $u$ and $v$ such that $um + vn = 1$, and then obtain that $x = bum + avn$ is the only solution of
\[ x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}, \]
for $x$ with $0 \leq x < mn$.

Correct Exercise: Let $a, b, m, n$ be integers with $gcd(m, n) = 1$. Let $u \equiv m^{-1} \pmod{n}$, and let $c = (b - a)u$. Prove that $x = a + cm$ is a solution to
\[ x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}, \]
and that every solution to this system has the form $x = a + cm + umn$, for some $y \in \mathbb{Z}$. 

1
Solution: Since $\gcd(m, n) = 1$, the Euclidean Algorithm tells us that there will be integers $u$ and $v$ such that $mu + nv = 1$. In particular, $m^{-1} \equiv u \pmod{n}$. Let $c = (b - a)u$ and $x = a + cm$.

Then $x_0 = a + cn = a + (b - a)um = a + bum - aum = a + bum - a(1 - vn) = a + bum - a + avn = bum + avn$. Therefore, (as discussed in class), $x_0$ is a solution of the system

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}.$$ 

Let $x$ be any solution to the system. Then $x - x_0 \equiv a - a \equiv 0 \pmod{m}$, and $x - x_0 \equiv b - b \equiv 0 \pmod{n}$. It follows that $m|(x - x_0)$ and $n|(x - x_0)$. Since $\gcd(m, n) = 1$ and by the Fundamental Theorem of Arithmetic (Theorem 1.21 of the text on Page 27), the unique factorization of $x - x_0$ must have $mn$ as a factor, and so for some integer $y$, $x - x_0 = ymn$. Substitute $x_0 = a + cm$, we have $x = a + cm + ymn$, as desired.