Complete Solutions to Exercise 3.4

1. We use the Chines Remainder Theorem to solve the given system of equations. First we check that the given moduli are pairwise prime.

(a) To solve the given system $x \equiv 5 \pmod 7, \quad x \equiv 4 \pmod{11}$ we use the following formula:

(3.23) $$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + \cdots + a_rN_rx_r$$

Provided the gcd of 7 and 11 is 1 which it is.

Firstly what is r equal to in this case?

Because we are given 2 simultaneous equations so $r = 2$ and our solution is given by

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \qquad (\dagger)$$

We need to find each of these components – *a*'s, *N*'s and *x*'s.

Evaluating the *N*'s:

$$N_1 = \frac{n_1 \times n_2}{n_1} = \frac{\cancel{7} \times 11}{\cancel{7}} = 11$$

Similarly $N_2 = 7$.

We also need to solve $N_kx_k \equiv 1 \pmod{n_k}$ for x_k where $k = 1$ and 2:

$$N_1x_1 \equiv 11x_1 \equiv 1 \pmod 7$$

We have $11 \equiv 4 \pmod 7$ so using this in the above equation gives

$$11x_1 \equiv 4x_1 \equiv 1 \pmod 7 \text{ implies } x_1 = 2.$$

Similarly we find x_2:

$$N_2x_2 \equiv 7x_2 \equiv -4x_2 \equiv 1 \pmod{11} \text{ implies } x_2 \equiv -3 \equiv 8 \pmod{11} \text{ so } x_2 = 8.$$

So far we have the *N*'s and *x*'s of (†). *What else do we need to find?*

a's. These are given to us - $a_1 = 5$ and $a_2 = 4$ because we are asked to solve

$$x \equiv 5 \pmod 7, \quad x \equiv 4 \pmod{11}$$

Substituting $a_1 = 5$, $a_2 = 4$, $N_1 = 11$, $N_2 = 7$, $x_1 = 2$ and $x_2 = 8$ into (†) gives

$$\begin{aligned} x &= \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \\ &= \left(5 \times 11 \times 2\right) + \left(4 \times 7 \times 8\right) = 334 \end{aligned}$$

Hence our solution is $x = 334 \equiv 26 \pmod{77}$.

(b) The procedure for solving $x \equiv 0 \pmod 5,\ x \equiv 0 \pmod 6$ is very similar to part (a).

First $\gcd(5,\ 6) = 1$ so we can use the Chinese Remainder Theorem.

We are given two simultaneous equations so the solution x is given by

$$x = (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) \qquad (*)$$

Since we are given $x \equiv 0 \pmod 5,\ x \equiv 0 \pmod 6$ so $a_1 = a_2 = 0$. We don't need to work out the rest of the values because $x = (0)N_1x_1 + (0)N_2x_2 = 0$. Our solution is

$$x = 0 \equiv 0 \pmod{[6 \times 5]} \equiv 0 \pmod{30}$$

This means x is a multiple of 30.

Remember $x \equiv 0 \pmod 5,\ x \equiv 0 \pmod 6$ means that when x is divided by 5 and 6, there is *no* remainder. Clearly 30, 60, 90 … *all* satisfy both these congruences.

(c) We need to solve $x \equiv 3 \pmod 8,\quad x \equiv 5 \pmod{13}$. First we check that 8 and 13 are pairwise prime:

$$\gcd(8,\ 13) = 1$$

Using formula (3.23) with $r = 2$ because we are given two simultaneous equations:

$$x = (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) \qquad (**)$$

We have $a_1 = 3,\quad a_2 = 5$ because we are given $x \equiv 3 \pmod 8,\quad x \equiv 5 \pmod{13}$.

Also

$$N_1 = 13 \text{ and } N_2 = 8$$

We need to find the inverses of $13 \pmod 8$ and $8 \pmod{13}$. Let x_1 be the inverse of $13 \pmod 8$ so

$$N_1x_1 \equiv 13x_1 \equiv 5x_1 \equiv 1 \pmod 8 \text{ gives } x_1 = 5.$$

Similarly let x_2 be the inverse of $8 \pmod{13}$ so

$$N_2x_2 \equiv 8x_2 \equiv 1 \pmod{13} \text{ implies } x_2 = 5.$$

Substituting $a_1 = 3,\quad a_2 = 5,\ N_1 = 13,\ N_2 = 8,\ x_1 = 5$ and $x_2 = 5$ into (**) gives

$$\begin{aligned} x &= (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) \\ &= (3 \times 13 \times 5) + (5 \times 8 \times 5) = 395 \end{aligned}$$

Our solution is $x = 395 \equiv 83 \pmod{104}$.

(d) We need to solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.

Checking that the given moduli are pairwise prime:

$$\gcd(3, 5) = \gcd(3, 7) = \gcd(5, 7) = 1$$

Using formula (3.23)

(3.23) $$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + \cdots + a_rN_rx_r$$

with $r = 3$ gives

$$x = (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) + (a_3 \times N_3 \times x_3) \qquad (*)$$

We need to find all the components on the right - hand side. First we find the N's;

$$N_1 = 5 \times 7 = 35$$
$$N_2 = 3 \times 7 = 21$$
$$N_3 = 3 \times 5 = 15$$

In order to find x_1, x_2 and x_3 we need to solve the equations

$$N_kx_k \equiv 1 \pmod{n_k}.$$

What is n_k equal to?

These lower case n's represent the given moduli, so

$$n_1 = 3,\ n_2 = 5 \text{ and } n_3 = 7$$

Solving each of these equations $N_kx_k \equiv 1 \pmod{n_k}$ for $k = 1,\ 2$ and 3:

$$N_1x_1 \equiv 35x_1 \equiv 2x_1 \equiv 1 \pmod{3} \text{ implies } x_1 = 2$$
$$N_2x_2 \equiv 21x_2 \equiv x_2 \equiv 1 \pmod{5} \text{ implies } x_2 = 1$$
$$N_3x_3 \equiv 15x_3 \equiv x_3 \equiv 1 \pmod{7} \text{ implies } x_3 = 1$$

The a's are given by $a_1 = 1,\ a_2 = 2$ and $a_3 = 3$ because we are given

$$x \equiv 1 \pmod{3},\ x \equiv 2 \pmod{5},\ x \equiv 3 \pmod{7}$$

Substituting $a_1 = 1,\ a_2 = 2,\ a_3 = 3,\ N_1 = 35,\ N_2 = 21,\ N_3 = 15,\ x_1 = 2,\ x_2 = 1$ and $x_3 = 1$ into (*) gives

$$\begin{aligned} x &= (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) + (a_3 \times N_3 \times x_3) \\ &= (1 \times 35 \times 2) + (2 \times 21 \times 1) + (3 \times 15 \times 1) = 157 \end{aligned}$$

Our unique solution in modulo $n_1 \times n_2 \times n_3 = 3 \times 5 \times 7 = 105$ is

$$x = 157 \equiv 52 \pmod{105}$$

(e) We are given the simultaneous congruences:

$$x \equiv 1 \pmod{5},\quad x \equiv 3 \pmod{7},\ x \equiv 5 \pmod{11}$$

Checking that the given moduli are pairwise prime we have

$$\gcd\left(5,\ \ 7\right)=\gcd\left(5,\ \ 11\right)=\gcd\left(7,\ \ 11\right)=1$$

We can use formula (3.23):

(3.23) $$x=a_1N_1x_1+a_2N_2x_2+a_3N_3x_3+\cdots+a_rN_rx_r$$

With $r=3$ gives

$$x=\left(a_1\times N_1\times x_1\right)+\left(a_2\times N_2\times x_2\right)+\left(a_3\times N_3\times x_3\right) \qquad (\dagger)$$

Evaluating N's gives

$$N_1=7\times11=77,\ N_2=5\times11=55 \text{ and } N_3=5\times7=35$$

Solving the following equations

$$77x_1\equiv2x_1\equiv1\left(\text{mod }5\right)\ \Rightarrow\ x_1=3$$

$$55x_2\equiv-x_2\equiv1\left(\text{mod }7\right)\ \Rightarrow\ x_2=6$$

$$35x_3\equiv2x_3\equiv1\left(\text{mod }11\right)\ \Rightarrow\ x_3=6$$

What are the values of the a's?

Since we are given $x\equiv1\left(\text{mod }5\right),\ \ x\equiv3\left(\text{mod }7\right),\ x\equiv5\left(\text{mod }11\right)$ so the a's are the integers:

$$a_1=1,\ \ a_2=3 \text{ and } a_3=5$$

Substituting $a_1=1,\ \ a_2=3,\ \ a_3=5$, $N_1=77$, $N_2=55$, $N_3=35$, $x_1=3$, $x_2=6$ and $x_3=6$ into (†) yields

$$\begin{aligned}x&=\left(a_1\times N_1\times x_1\right)+\left(a_2\times N_2\times x_2\right)+\left(a_3\times N_3\times x_3\right)\\&=\left(1\times77\times3\right)+\left(3\times55\times6\right)+\left(5\times35\times6\right)=2271\end{aligned}$$

Our unique solution is given in modular arithmetic with a modulo which is the product of all the given moduli:

$$n=5\times7\times11=385$$

Hence $x=2271\equiv346\left(\text{mod }385\right)$.

2. In each of these cases apart from (d) we need to convert to $x\equiv?\left(\text{mod }n\right)$ because we are given congruences of the form $ax\equiv b\left(\text{mod }n\right)$ where $a>1$.

(a) We are given the system $2x\equiv1\left(\text{mod }3\right),\ \ 5x\equiv2\left(\text{mod }7\right)$. Verifying that $\gcd\left(3,\ \ 7\right)=1$ so the given moduli are pairwise prime.

Solving each of these separately gives

$$2x \equiv 1 \pmod 3 \quad \Rightarrow \quad x \equiv 2 \pmod 3$$
$$5x \equiv 2 \pmod 7 \quad \Rightarrow \quad x \equiv 6 \pmod 7$$

We solve the equivalent system of equations

$$x \equiv 2 \pmod 3, \quad x \equiv 6 \pmod 7$$

by applying the Chinese Remainder Theorem.

The formula in this case is

$$x = (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) \qquad (**)$$

What is N_1 *and* N_2 *equal to?*

$$N_1 = 7 \text{ and } N_2 = 3$$

To find x_1 and x_2 we need to solve

$$N_1 x_1 \equiv 7x_1 \equiv x_1 \equiv 1 \pmod 3 \text{ which gives } x_1 = 1.$$

$$N_2 x_2 \equiv 3x_2 \equiv 1 \pmod 7 \text{ which gives } x_2 = 5.$$

How do we find the a's?

Since we are solving $x \equiv 2 \pmod 3, \quad x \equiv 6 \pmod 7$ so $a_1 = 2, \quad a_2 = 6$.

Substituting $a_1 = 2, \quad a_2 = 6$, $N_1 = 7$, $N_2 = 3$, $x_1 = 1$ and $x_2 = 5$ into (**) yields

$$\begin{aligned} x &= a_1 N_1 x_1 + a_2 N_2 x_2 \\ &= (2 \times 7 \times 1) + (6 \times 3 \times 5) = 104 \end{aligned}$$

Our unique solution modulo $n_1 n_2 = 3 \times 7 = 21$ is

$$x = 104 \equiv 20 \pmod{21}$$

The general solution is given by $x = 21t + 20$ where t is an integer.

The least non-negative integer in $x = 21t + 20$ is when $t = 0$ so $x = 20$.

(b) We are required to solve $2x \equiv 1 \pmod{13}, \ 3x \equiv 2 \pmod{19}$. First we need to convert these into $x \equiv ? \pmod n$. Solving each of these equations separately

$$2x \equiv 1 \pmod{13} \quad \text{implies that} \quad x \equiv 7 \pmod{13}$$
$$3x \equiv 2 \pmod{19} \quad \text{implies that} \quad x \equiv 7 \pmod{19}$$

We solve the equivalent system

$$x \equiv 7 \pmod{13}, \ x \equiv 7 \pmod{19}$$

We have $\gcd(13, \ 19) = 1$ so the given moduli 13 and 19 are relatively prime.

Using formula:

(3.23) $$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$$

with $r = 2$ gives

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \qquad (\dagger)$$

First finding the *N*'s:

$$N_1 = \frac{13 \times 19}{13} = 19, \;\; N_2 = \frac{13 \times 19}{19} = 13$$

How do we determine x_1 *and* x_2*?*

Need to solve $N_1 x_1 \equiv 1 \left(\text{mod } n_1\right)$ and $N_2 x_2 \equiv 1 \left(\text{mod } n_2\right)$ where $n_1 = 13, \;\; n_2 = 19$:

$$19x_1 \equiv 6x_1 \equiv 1 \left(\text{mod } 13\right) \text{ gives } x_1 = 11$$

$$13x_2 \equiv -6x_2 \equiv 1 \left(\text{mod } 19\right) \text{ gives } x_2 = 3$$

The *a*'s are given by $a_1 = a_2 = 7$ because we are solving

$$x \equiv 7 \left(\text{mod } 13\right), \;\; x \equiv 7 \left(\text{mod } 19\right).$$

Substituting $a_1 = a_2 = 7$, $N_1 = 19, \;\; N_2 = 13$, $x_1 = 11$ and $x_2 = 3$ into (†) yields

$$\begin{aligned} x &= a_1 N_1 x_1 + a_2 N_2 x_2 \\ &= \left(7 \times 19 \times 11\right) + \left(7 \times 13 \times 3\right) = 1736 \end{aligned}$$

Writing this number x congruent to modulo $n_1 \times n_2 = 13 \times 19 = 247$:

$$x = 1736 \equiv 7 \left(\text{mod } 247\right)$$

The least non-negative integer which satisfies the given system is 7.

The general solution is given by $x = 7 + 247t$.

(c) We need to solve the system:

$$3x \equiv 5 \left(\text{mod } 7\right), \;\; 5x \equiv 2 \left(\text{mod } 11\right), \;\; 9x \equiv 1 \left(\text{mod } 5\right).$$

Firstly we can simplify the last congruence because $9 \equiv 4 \left(\text{mod } 5\right)$ so this congruence is equivalent to $4x \equiv 1 \left(\text{mod } 5\right)$.

Next we solve each of these equations:

$$\begin{aligned} 3x \equiv 5 \left(\text{mod } 7\right) &\;\; \Rightarrow \;\; x \equiv 4 \left(\text{mod } 7\right) \\ 5x \equiv 2 \left(\text{mod } 11\right) &\;\; \Rightarrow \;\; x \equiv 7 \left(\text{mod } 11\right) \\ 4x \equiv 1 \left(\text{mod } 5\right) &\;\; \Rightarrow \;\; x \equiv 4 \left(\text{mod } 5\right) \end{aligned}$$

We solve the equivalent system:

$$x \equiv 4 \left(\text{mod } 7\right), \quad x \equiv 7 \left(\text{mod } 11\right), \quad x \equiv 4 \left(\text{mod } 5\right)$$

In order to use the Chinese Remainder Theorem we have to check that the given moduli are pairwise prime:

$$\gcd\left(5, \;\; 7\right) = \gcd\left(5, \;\; 11\right) = \gcd\left(7, \;\; 11\right) = 1$$

Now we can use the Chinese Remainder formula:

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right) \qquad (**)$$

Evaluating N_1, N_2 and N_3:

$$N_1 = \frac{\cancel{7} \times 11 \times 5}{\cancel{7}} = 55$$

$$N_2 = \frac{7 \times 11 \times 5}{11} = 35$$

$$N_3 = \frac{7 \times 11 \times \cancel{5}}{\cancel{5}} = 77$$

Solving the equations $N_k x_k \equiv 1 \left(\text{mod } n_k\right)$:

$$55x_1 \equiv -x_1 \equiv 1 \left(\text{mod } 7\right) \text{ implies that } x_1 = 6$$

$$35x_2 \equiv 2x_2 \equiv 1 \left(\text{mod } 11\right) \text{ implies that } x_2 = 6$$

$$77x_3 \equiv 2x_3 \equiv 1 \left(\text{mod } 5\right) \text{ implies that } x_3 = 3$$

What are the a's equal to?

We are solving $x \equiv 4 \left(\text{mod } 7\right)$, $x \equiv 7 \left(\text{mod } 11\right)$, $x \equiv 4 \left(\text{mod } 5\right)$ so

$$a_1 = 4, \; a_2 = 7, \; a_3 = 4$$

Substituting $a_1 = 4$, $a_2 = 7$, $a_3 = 4$, $N_1 = 55$, $N_2 = 35$, $N_3 = 77$, $x_1 = 6$, $x_2 = 6$ and $x_3 = 3$ into (**) yields

$$\begin{aligned} x &= \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right) \\ &= \left(4 \times 55 \times 6\right) + \left(7 \times 35 \times 6\right) + \left(4 \times 77 \times 3\right) = 3714 \end{aligned}$$

We write this congruent to modulo $n_1 n_2 n_3 = 7 \times 11 \times 5 = 385$ therefore we have

$$x = 3714 \equiv 249 \left(\text{mod } 385\right)$$

The general solution is given by $x = 249 + 385t$ and least non-negative integer is 249.

(d) Since 7 and 11 are relatively prime so we can use the Chinese Remainder Theorem with $r = 2$:

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \qquad (\dagger)$$

We have $N_1 = 11$ and $N_2 = 7$. The inverse of $N_1 = 11$ and $N_2 = 7$ modulo 7 and 9 respectively is given by x_1 and x_2 such that

$$11x_1 \equiv 1 \;\Rightarrow\; 4x_1 \equiv 1 \left(\text{mod } 7\right) \;\Rightarrow\; x_1 = 2$$

$$7x_2 \equiv 1 \;\Rightarrow\; -4x_2 \equiv 1 \;\Rightarrow\; x_2 \equiv -3 \left(\text{mod } 11\right) \;\Rightarrow\; x_2 = 8$$

Substituting $a_1 = 3$, $a_2 = 9$, $N_1 = 11$, $N_2 = 7$, $x_1 = 2$ and $x_2 = 8$ into (†) gives

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right)$$
$$= \left(3 \times 11 \times 2\right) + \left(9 \times 7 \times 8\right) = 570$$

Our unique solution is given by $x = 570 \equiv 31 \left(\text{mod } 77\right)$. Our general solution is $x = 31 + 77t$ where t is any integer and the least positive integer is 31.

3. Let x be the least positive integer which leaves remainder 2 when divided by 7, remainder 3 when divided by 9 and remainder 6 when divided by 11. We can write this in modular arithmetic as:

$$x \equiv 2 \left(\text{mod } 7\right),\ x \equiv 3 \left(\text{mod } 9\right),\ x \equiv 6 \left(\text{mod } 11\right)$$

The given moduli 7, 9 and 11 are pairwise prime so we can use the Chinese Remainder Theorem:

(3.23) $$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$$

Since we have 3 simultaneous equations so in the formula $r = 3$:

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right) \qquad (\dagger)$$

Using the procedure in all the above solutions we have

$$N_1 = \frac{\cancel{7} \times 9 \times 11}{\cancel{7}} = 99$$
$$N_2 = \frac{7 \times \cancel{9} \times 11}{\cancel{9}} = 77$$
$$N_3 = \frac{7 \times 9 \times \cancel{11}}{\cancel{11}} = 63$$

The x_1, x_2 and x_3 satisfy

$$99x_1 \equiv x_1 \equiv 1 \left(\text{mod } 7\right) \text{ gives } x_1 = 1$$
$$77x_2 \equiv 5x_2 \equiv 1 \left(\text{mod } 9\right) \text{ gives } x_2 = 2$$
$$63x_3 \equiv -3x_3 \equiv 1 \left(\text{mod } 11\right) \text{ gives } x_3 = 7$$

Since we need to solve $x \equiv 2 \left(\text{mod } 7\right),\ x \equiv 3 \left(\text{mod } 9\right),\ x \equiv 6 \left(\text{mod } 11\right)$ so

$$a_1 = 2,\ a_2 = 3,\ a_3 = 6$$

Putting all these numbers $a_1 = 2,\ a_2 = 3,\ a_3 = 6$, $N_1 = 99$, $N_2 = 77$, $N_3 = 63$, $x_1 = 1$, $x_2 = 2$ and $x_3 = 7$ into (†) gives

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right)$$
$$= \left(2 \times 99 \times 1\right) + \left(3 \times 77 \times 2\right) + \left(6 \times 63 \times 7\right) = 3306$$

We need to write x in modulo $n_1 \times n_2 \times n_3 = 7 \times 9 \times 11 = 693$:

$$x = 3306 \equiv 534 \left(\text{mod } 693\right)$$

The least positive integer which satisfies the remainders given in the question is 534.

4. The least positive integer x which leaves remainder 1 when divided by 5, remainder 2 when divided by 7, remainder 3 when divided by 9 and remainder 4 when divided by 11 satisfies the following congruent equations:

$$x \equiv 1 \left(\text{mod } 5\right),\ x \equiv 2 \left(\text{mod } 7\right),\ x \equiv 3 \left(\text{mod } 9\right),\ x \equiv 4 \left(\text{mod } 11\right)$$

We need to find the integer x which satisfies all these equations. Checking the given moduli are pairwise prime:

$$\gcd\left(5,\ \ 7\right) = \gcd\left(5,\ \ 9\right) = \gcd\left(5,\ \ 11\right) = \gcd\left(7,\ \ 9\right) = \gcd\left(7,\ \ 11\right) = \gcd\left(9,\ \ 11\right) = 1$$

Hence the given moduli are pairwise prime so we can apply the Chinese Remainder Theorem. We use

(3.23) $$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$$

Since we have 4 simultaneous equations so in the formula $r = 4$:

$$x = \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right) + \left(a_4 \times N_4 \times x_4\right) \qquad (\dagger\dagger)$$

Evaluating various components of this (††):

$$N_1 = \frac{\cancel{5} \times 7 \times 9 \times 11}{\cancel{5}} = 693$$

$$N_2 = \frac{5 \times \cancel{7} \times 9 \times 11}{\cancel{7}} = 495$$

$$N_3 = \frac{5 \times 7 \times \cancel{9} \times 11}{\cancel{9}} = 385$$

$$N_4 = \frac{5 \times 7 \times 9 \times \cancel{11}}{\cancel{11}} = 315$$

We need to solve the equations $N_k x_k \equiv 1 \left(\text{mod } n_k\right)$ for $k = 1,\ 2,\ 3,\ 4$. The lower case n's are the given moduli, that is $n_1 = 5,\ n_2 = 7,\ n_3 = 9$ and $n_4 = 11$. We have

$$693x_1 \equiv 3x_1 \equiv 1 \left(\text{mod } 5\right) \text{ gives } x_1 = 2$$

$$495x_2 \equiv 5x_2 \equiv 1 \left(\text{mod } 7\right) \text{ gives } x_2 = 3$$

$$385x_3 \equiv 7x_3 \equiv 1 \left(\text{mod } 9\right) \text{ gives } x_3 = 4$$

$$315x_4 \equiv 7x_4 \equiv 1 \left(\text{mod } 11\right) \text{ gives } x_4 = 8$$

The last ingredients we need for (††) are the a's. These are the right hand values of the above congruences:

$$a_1 = 1,\ \ a_2 = 2,\ \ a_3 = 3,\ a_4 = 4$$

Because we are solving the following system of equations

$$x \equiv 1 \left(\text{mod } 5\right),\ x \equiv 2 \left(\text{mod } 7\right),\ x \equiv 3 \left(\text{mod } 9\right),\ x \equiv 4 \left(\text{mod } 11\right)$$

Substituting $a_1 = 1,\ \ a_2 = 2,\ \ a_3 = 3,\ a_4 = 4$, $N_1 = 693$, $N_2 = 495$, $N_3 = 385$, $N_4 = 315$, $x_1 = 2$, $x_2 = 3$, $x_3 = 4$ and $x_4 = 8$ into (††) yields

$$\begin{aligned} x &= \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) + \left(a_3 \times N_3 \times x_3\right) + \left(a_4 \times N_4 \times x_4\right) \\ &= \left(1 \times 693 \times 2\right) + \left(2 \times 495 \times 3\right) + \left(3 \times 385 \times 4\right) + \left(4 \times 315 \times 8\right) = 19056 \end{aligned}$$

We need to evaluate x modulo $n_1 \times n_2 \times n_3 \times n_4 = 5 \times 7 \times 9 \times 11 = 3465$:

$$x = 19056 \equiv 1731 \left(\text{mod } 3465\right)$$

The least positive integer is 1731.

5. We need to show the given linear system

$$x \equiv 1 \left(\text{mod } 2\right) \text{ and } x \equiv 2 \left(\text{mod } 4\right)$$

cannot be solved. From the first equation $x \equiv 1 \left(\text{mod } 2\right)$ we have $x - 1 = 2k$ for some integer k. Therefore $x = 1 + 2k$. Similarly for the second equation we have $x = 2 + 4c$ for some integer c. Equating these equations gives

$$x = 1 + 2k = 2 + 4c$$

Re-arranging this we have

$$2k - 4c = 1$$

This is a Diophantine equation. By Proposition (1.17):

> Let $\gcd\left(a,\ \ b\right) = g$. The equation $ax + by = c$ has integer solutions $\Leftrightarrow$ $g \mid c$.

We can say that $2k - 4c = 1$ has *no* solutions because $\gcd\left(2,\ \ -4\right) = 2$ and $2 \not| 1$.

Note that the given moduli 2 and 4 are *not* pairwise prime we *cannot* use Chinese Remainder Theorem.

6. We can write the given information in modular arithmetic. Let x be the number of soldiers. Then we have

2 left over when in rows of 5 $\Rightarrow$ $x \equiv 2 \left(\text{mod } 5\right)$

4 left over when in rows of 6 $\Rightarrow$ $x \equiv 4 \left(\text{mod } 6\right)$

1 left over when in rows of 7 $\Rightarrow$ $x \equiv 1 \pmod 7$

7 left over when in rows of 11 $\Rightarrow$ $x \equiv 7 \pmod{11}$

We solve this $x \equiv 2 \pmod 5,\ x \equiv 4 \pmod 6,\ x \equiv 1 \pmod 7,\ x \equiv 7 \pmod{11}$ by using the formula

$$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4 \qquad (*)$$

Provided the moduli 5, 6, 7 and 11 are pairwise prime. Check that these are actually pairwise prime.

We have

$$N_1 = \frac{\cancel{5} \times 6 \times 7 \times 11}{\cancel{5}} = 462$$

$$N_2 = \frac{5 \times \cancel{6} \times 7 \times 11}{\cancel{6}} = 385$$

$$N_3 = \frac{5 \times 6 \times \cancel{7} \times 11}{\cancel{7}} = 330$$

$$N_4 = \frac{5 \times 6 \times 7 \times \cancel{11}}{\cancel{11}} = 210$$

The x_k's satisfy $N_kx_k \equiv 1 \pmod{n_k}$ for $k = 1,\ 2,\ 3,\ 4$. Lower case n's are the values of the given moduli

$$n_1 = 5,\ n_2 = 6,\ n_3 = 7,\ n_4 = 11$$

Solving $N_kx_k \equiv 1 \pmod{n_k}$ for each k:

$$462x_1 \equiv 2x_1 \equiv 1 \pmod 5 \text{ implies } x_1 = 3$$

$$385x_2 \equiv x_2 \equiv 1 \pmod 6 \text{ implies } x_2 = 1$$

$$330x_3 \equiv x_3 \equiv 1 \pmod 7 \text{ implies } x_3 = 1$$

$$210x_4 \equiv x_4 \equiv 1 \pmod{11} \text{ implies } x_4 = 1$$

The a's are $a_1 = 2,\ a_2 = 4,\ a_3 = 1,\ a_4 = 7$ because we are solving

$$x \equiv 2 \pmod 5,\ x \equiv 4 \pmod 6,\ x \equiv 1 \pmod 7,\ x \equiv 7 \pmod{11}$$

Substituting $a_1 = 2,\ a_2 = 4,\ a_3 = 1,\ a_4 = 7$, $N_1 = 462$, $N_2 = 385$, $N_3 = 330$, $N_4 = 210$, $x_1 = 3$, $x_2 = 1$, $x_3 = 1$ and $x_4 = 1$ into (*) gives

$$\begin{aligned} x &= a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4 \\ &= (2 \times 462 \times 3) + (4 \times 385 \times 1) + (1 \times 330 \times 1) + (7 \times 210 \times 1) = 6112 \end{aligned}$$

Evaluating x modulo $n_1 \times n_2 \times n_3 \times n_4 = 5 \times 6 \times 7 \times 11 = 2310$:

$$x = 6112 \equiv 1492 \pmod{2310}$$

The minimum number of soldiers in his battalion is 1492.

7. We do *not* have $x \equiv ? \pmod{m}$ but $ax \equiv ? \pmod{m}$. *How do we solve these?*

We convert them into $x \equiv ? \pmod{m}$ by multiplying by an appropriate factor.

Multiply the first linear congruence $2x \equiv 1 \pmod{5}$ by 3:

$$6x \equiv x \equiv 3 \pmod{5} \quad \left[\text{Because } 6 \equiv 1 \pmod{5}\right]$$

We can simplify the second $3x \equiv 9 \pmod{6}$ by dividing through by $\gcd(3, 6) = 3$:

$$x \equiv 3 \pmod{2} \equiv 1 \pmod{2}$$

We multiply the third $4x \equiv 1 \pmod{7}$ by 2:

$$8x \underbrace{\equiv}_{\text{Because } 8 \equiv 1 \pmod{7}} x \equiv 2 \pmod{7}$$

Finally we multiply the last given congruence $5x \equiv 9 \pmod{11}$ by 9:

$$45x \underbrace{\equiv}_{\text{Because } 45 \equiv 1 \pmod{11}} x \equiv 81 \equiv 4 \pmod{11}$$

This last congruence is $x \equiv 4 \pmod{11}$.

We solve the equivalent system:

$$x \equiv 3 \pmod{5},\ x \equiv 1 \pmod{2},\ x \equiv 2 \pmod{7} \text{ and } x \equiv 4 \pmod{11}$$

Checking the given moduli are pairwise prime:

$$\gcd(2, 5) = \gcd(2, 7) = \gcd(2, 11) = \gcd(5, 7) = \gcd(5, 11) = \gcd(7, 11) = 1$$

Hence the moduli are pairwise prime so we can use formula (3.23):

(3.23) $$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$$

We are given 4 equations so we use this formula with $r = 4$:

$$x = (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) + (a_3 \times N_3 \times x_3) + (a_4 \times N_4 \times x_4) \qquad (\dagger\dagger)$$

Evaluating each of the N's which are given by $N_k = \dfrac{n_1 n_2 \cdots n_r}{n_k}$ with $n_1 = 5$, $n_2 = 2$, $n_3 = 7$ and $n_4 = 11$:

$$N_1 = \frac{2 \times \cancel{5} \times 7 \times 11}{\cancel{5}} = 154$$

$$N_2 = \frac{\cancel{2}\times 5\times 7\times 11}{\cancel{2}} = 385$$

$$N_3 = \frac{2\times 5\times \cancel{7}\times 11}{\cancel{7}} = 110$$

$$N_4 = \frac{2\times 5\times 7\times \cancel{11}}{\cancel{11}} = 70$$

We need to find the x_k's which are given by $N_k x_k \equiv 1 \pmod{n_k}$ for $k = 1,\ 2,\ 3$ and 4:

$$N_1 x_1 \equiv 154 x_1 \equiv 1 \pmod 5 \qquad [\text{Remember } n_1 = 5]$$

$$N_2 x_2 \equiv 385 x_2 \equiv 1 \pmod 2 \qquad [\text{Remember } n_2 = 2]$$

$$N_3 x_3 \equiv 110 x_3 \equiv 1 \pmod 7 \qquad [\text{Remember } n_3 = 7]$$

$$N_4 x_4 \equiv 70 x_4 \equiv 1 \pmod{11} \qquad [\text{Remember } n_4 = 11]$$

Solving each of these equations gives:

$$154x_1 \underbrace{\equiv}_{\text{Because } 154\equiv 4\equiv -1 \pmod 5} -x_1 \equiv 1 \pmod 5 \quad \text{implies} \quad x_1 = 4$$

$$385x_2 \underbrace{\equiv}_{\text{Because } 385\equiv 1 \pmod 2} x_2 \equiv 1 \pmod 2 \text{ implies } x_2 = 1$$

$$110x_3 \underbrace{\equiv}_{\text{Because } 110\equiv 5 \pmod 7} 5x_3 \equiv 1 \pmod 7 \quad \text{implies} \quad x_3 = 3$$

$$70x_4 \underbrace{\equiv}_{\text{Because } 70\equiv 4 \pmod{11}} 4x_4 \equiv 1 \pmod{11} \text{ implies } x_4 = 3$$

The given a's are $a_1 = 3,\ a_2 = 1,\ a_3 = 2$ and $a_4 = 4$ because we are solving

$$x \equiv 3 \pmod 5,\ x \equiv 1 \pmod 2,\ x \equiv 2 \pmod 7 \text{ and } x \equiv 4 \pmod{11}$$

Putting all these numbers $a_1 = 3,\ a_2 = 1,\ a_3 = 2,\ a_4 = 4$, $N_1 = 154$, $N_2 = 385$, $N_3 = 110$, $N_4 = 70$, $x_1 = 4,\ x_2 = 1,\ x_3 = 3$ and $x_4 = 3$ into (††) gives:

$$\begin{aligned} x &= (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) + (a_3 \times N_3 \times x_3) + (a_4 \times N_4 \times x_4) \\ &= (3\times 154\times 4) + (1\times 385\times 1) + (2\times 110\times 3) + (4\times 70\times 3) = 3733 \end{aligned}$$

Remember the modulus n is the product of the given moduli:

$$n = 5\times 2\times 7\times 11 = 770$$

We have $x = 3733 \equiv 653 \pmod{770}$. The least positive integer is 653.

Check in your own time that this solution is correct, that is $x \equiv 653 \pmod{770}$ satisfies all 4 given congruences.

8. (a) We need to show that if $x \equiv M \pmod{p}$ and $x \equiv M \pmod{q}$ then $x \equiv M \pmod{p \times q}$.

Proof.

From $x \equiv M \pmod{p}$ we have $x - M = kp$ and from $x \equiv M \pmod{q}$ we have

$$x - M = cq$$

Hence $x - M$ is a multiple of distinct primes p and q. We are given p and q are *distinct* primes so they are *relatively* prime which implies by Proposition (2.10):

> Let a and b be relatively prime positive integers then $\left[a, \quad b\right] = a \times b$.

That the smallest multiple (LCM) of p and q is $p \times q$. Hence we have

$$x - M \equiv 0 \pmod{p \times q} \quad \Rightarrow \quad x \equiv M \pmod{p \times q}$$

This completes our proof.

■

(b) We are asked to prove that if $p_1, \ p_2, \ p_3, \ \cdots, \ p_k$ be distinct primes such that $x \equiv M \pmod{p_j}$ for $j = 1, \ 2, \ 3, \ \cdots, \ k$ then $x \equiv M \pmod{p_1 \times p_2 \times p_3 \times \cdots \times p_k}$.

How do we prove this?

By mathematical induction.

Proof.

If $k = 2$ then by part (a) we have our result $x \equiv M \pmod{p_1 \times p_2}$.

Assume the result is true for $k = m$, that is

$$x \equiv M \pmod{p_1 \times p_2 \times \cdots \times p_m} \qquad (\ddagger)$$

Required to prove the result for $k = m + 1$:

$$x \equiv M \pmod{p_1 \times p_2 \times \cdots \times p_m \times p_{m+1}}$$

We consider the two simultaneous equations

$$x \equiv M \pmod{p_1 \times p_2 \times \cdots \times p_m} \text{ which implies } \left(p_1 \times p_2 \times \cdots \times p_m\right) \mid \left(x - M\right)$$

$$x \equiv M \pmod{p_{m+1}} \text{ which implies } p_m \mid \left(x - M\right)$$

By Question 12 (i) of Exercises 1.3:

> If $a \mid c$ and $b \mid c$, and $\gcd\left(a, \quad b\right) = 1$ then $\left(a \times b\right) \mid c$

Since the given primes are *distinct* so $\gcd\left(p_1 \times p_2 \times \cdots \times p_m, \quad p_{m+1}\right) = 1$. We can apply this result to $\left(p_1 \times p_2 \times \cdots \times p_m\right) \mid \left(x - M\right)$ and $p_m \mid \left(x - M\right)$. We have

$$\left(p_1 \times p_2 \times \cdots \times p_m \times p_{m+1}\right) \mid \left(x - M\right)$$

By the definition of congruence we conclude that

$$x \equiv M \left(\text{mod } p_1 \times p_2 \times \cdots \times p_m \times p_{m+1}\right)$$

By mathematical induction we have our result.

■

(c) Now we have to prove $a \equiv b \left(\text{mod } m_k\right) \Leftrightarrow a \equiv b \left(\text{mod } \left[m_1,\ m_2,\ \cdots,\ m_n\right]\right)$.

Proof.

$(\Leftarrow)$. We assume $a \equiv b \left(\text{mod } \left[m_1,\ m_2,\ \cdots,\ m_n\right]\right)$ where the notation

$$\left[m_1,\ m_2,\ \cdots,\ m_n\right] \text{ is the LCM of } m_1, m_2, \cdots, m_n .$$

Since m_k must be present in $\left[m_1,\ m_2,\ \cdots,\ m_n\right]$ so $m_k \mid \left(a-b\right)$ because we are assuming $a \equiv b \left(\text{mod } \left[m_1,\ m_2,\ \cdots,\ m_n\right]\right)$. From $m_k \mid \left(a-b\right)$ we obtain $a \equiv b \left(\text{mod } m_k\right)$.

$(\Rightarrow)$. Now we assume $a \equiv b \left(\text{mod } m_k\right)$ and we need to deduce

$$a \equiv b \left(\text{mod } \left[m_1,\ m_2,\ \cdots,\ m_n\right]\right)$$

We prove this part by mathematical induction on k.

We consider the base case $k = 2$ which is $a \equiv b \left(\text{mod } m_1\right)$ and $a \equiv b \left(\text{mod } m_2\right)$.

We need to prove $a \equiv b \left(\text{mod } \left[m_1,\ m_2\right]\right)$.

From the base case congruent results we have $a = b + m_1 s$ and $a = b + m_2 t$ where s and t are integers. Equating these gives

$$b + m_1 s = b + m_2 t \ \Rightarrow\ m_1 s = m_2 t \ \Rightarrow\ s = \frac{m_2}{m_1} t$$

Remember s and t are integers so if we chose $t = m_1$ then we have an integer solution for $s = \dfrac{m_2}{\cancel{m_1}} \cancel{m_1} = m_2$.

Substituting this $s = m_2$ into the above equations $a = b + m_1 s$ yields

$$a = b + m_1 m_2 \text{ which implies } a \equiv b \left(\text{mod } m_1 m_2\right)$$

By question 18 of Exercises 2.4:

Let n be a common multiple of x and y. Then $\left[x,\ y\right] \mid n$.

Applying this to $m_1 m_2$ because $m_1 m_2$ is a common multiple of m_1 and m_2 so we have $\left[m_1,\ m_2\right] \mid \left(m_1 m_2\right)$. Using this $\left[m_1,\ m_2\right] \mid \left(m_1 m_2\right)$ and $a \equiv b \left(\text{mod } m_1 m_2\right)$ we

deduce that $a \equiv b \left(\text{mod } \left[m_1, \quad m_2\right]\right)$. Hence we have our result for the base case $k = 2$.

[Induction Hypothesis]. Assume it is true for $k = \ell$:

$$a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_\ell\right]\right) \qquad (*)$$

We have to prove the result for $k = \ell + 1$:

$$a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_\ell, \ m_{\ell+1}\right]\right)$$

From (*) we have

$$a = b + \left[m_1, \ m_2, \ \cdots, \ m_\ell\right] s_1$$

As we are assuming $a \equiv b \left(\text{mod } m_k\right)$ so $a \equiv b \left(\text{mod } m_{\ell+1}\right)$. Therefore

$$a = b + m_{\ell+1} t_1$$

Equating these last two equations gives

$$\left[m_1, \ m_2, \ \cdots, \ m_\ell\right] s_1 = m_{\ell+1} t_1 \ \Rightarrow \ s_1 = \frac{m_{\ell+1}}{\left[m_1, \ m_2, \ \cdots, \ m_\ell\right]} t_1$$

Choosing $t_1 = \left[m_1, \ m_2, \ \cdots, \ m_\ell\right]$ gives $s_1 = m_{\ell+1}$. Substituting this $s_1 = m_{\ell+1}$ into the above equation $a = b + \left[m_1, \ m_2, \ \cdots, \ m_\ell\right] s_1$ gives

$a = b + \left[m_1, \ m_2, \ \cdots, \ m_\ell\right] m_{\ell+1}$ which implies $a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_\ell\right] m_{\ell+1}\right)$

Now as for above case we have

$$\left[m_1, \ m_2, \ \cdots, \ m_\ell\right] m_{\ell+1} \text{ is a multiple of } \left[m_1, \ m_2, \ \cdots, \ m_\ell, \ m_{\ell+1}\right].$$

Therefore $a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_\ell\right] m_{\ell+1}\right)$ implies

$$a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_\ell, \ m_{\ell+1}\right]\right)$$

By mathematical induction we conclude that

$$a \equiv b \left(\text{mod } m_k\right) \ \Rightarrow \ a \equiv b \left(\text{mod } \left[m_1, \ m_2, \ \cdots, \ m_n\right]\right)$$

This completes our proof.

■

9. We need to prove the following:

Let $n_1, \ n_2, \ n_3, \ \cdots, \ n_r$ be positive integers which are pairwise prime. Also integers c_k's satisfy $\gcd\left(c_k, \quad n_k\right) = 1$. Then the simultaneous linear congruences

$$\begin{aligned} c_1 x &\equiv b_1 \pmod{n_1} \\ c_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ c_r x &\equiv b_r \pmod{n_r} \end{aligned}$$

has a solution satisfying all these equations.

Moreover the solution is *unique* modulo $n_1 \times n_2 \times n_3 \times \cdots \times n_r$.

Proof.

Since we are given that $\gcd(c_k, n_k) = 1$ so the equation

$$c_k x \equiv b_k \pmod{n_k}$$

has a unique solution. *Why?*

Because by Corollary (3.19):

$ax \equiv b \pmod{n}$ has unique solution provided $g = \gcd(a, n) = 1$

Let the solution be x. Therefore for each $k = 1, 2, 3, \cdots, r$ we have

$$x \equiv d_k \pmod{n_k}$$

Applying the Chinese Remainder Theorem to this system of equations $x \equiv d_k \pmod{n_k}$ yields a unique solution modulo $n_1 \times n_2 \times n_3 \times \cdots \times n_r$.

This completes our proof.

■

10. We are given that $P(x) \equiv 0 \pmod{n}$ where $n = n_1 \times n_2 \times \cdots \times n_r$ and $n_1, n_2, \cdots, n_r$ are pairwise prime integers.

We need to show that $P(x) \equiv 0 \pmod{n_k}$.

Proof.

From $P(x) \equiv 0 \pmod{n}$ we have

$$P(x) \equiv 0 \pmod{n_1 \times n_2 \times \cdots \times n_r} \quad [\text{Because } n = n_1 \times n_2 \times \cdots \times n_r]$$

This means that $P(x) = k(n_1 \times n_2 \times \cdots \times n_r)$ where k is an integer. Rearranging this

$$P(x) = n_1(k n_2 \times \cdots \times n_r) = n_1 \times (\text{integer})$$

Since $P(x)$ is a multiple of n_1 so

$$P(x) \equiv 0 \pmod{n_1}$$

Similarly, we can show that $P\left(x\right) \equiv 0 \left(\text{mod } n_j\right)$ for $j = 2,\ 3, \cdots,\ r$. This completes our proof.

■

11. We need to show that the simultaneous linear congruences:

$$x \equiv a \left(\text{mod } m\right)$$
$$x \equiv b \left(\text{mod } n\right)$$

Have a solution $\Leftrightarrow$ $\gcd\left(m,\ \ n\right) \Big| \left(a - b\right)$.

Proof.

From the definition of congruence we have

$$x \equiv a \left(\text{mod } m\right) \ \Leftrightarrow\ x - a = km \ \Leftrightarrow\ x = a + km$$
$$x \equiv b \left(\text{mod } n\right) \ \Leftrightarrow\ \ \ x - b = cn \ \Leftrightarrow\ x = b + cn$$

where k and c are integers. Putting $x = a + km$ into the bottom equation gives

$$x = a + km = b + cn$$

Re-arranging this gives

$$a - b = cn - km = cn + \left(-k\right)m$$

This $cn + \left(-k\right)m = a - b$ is a Diophantine equation with the unknowns as m and n. Now using the criteria for a solution to the Diophantine equation (1.16) of chapter 1:

Equation $ax + by = c$ has integer solutions $\Leftrightarrow$ $g \Big\vert\ c$ where $\gcd\left(a,\ \ b\right) = g$.

Hence $cn + \left(-k\right)m = a - b$ has a solution $\Leftrightarrow$ $\gcd\left(m,\ \ n\right) \Big| \left(a - b\right)$. This is our required result.

■