Solution Sheet 3

1. (i)★ By observation $m = -3, n = 2$ is a solution, so the general solution is
$$m = -3 + 5k, \quad n = 2 - 3k \quad \text{for } k \in \mathbb{Z}.$$

   (ii) The particular solution previously found was $m = -28, n = 4$. The general solution is
$$m = -28 + 15k, \quad n = 4 - 2k \ \text{ for } k \in \mathbb{Z}.$$

   Note, you might have observed that $2m + 15n = 4$ has a particular solution $m = 2, n = 0$. This leads to the general solution
$$m = 2 + 15\ell, n = -2\ell \text{ for } \ell \in \mathbb{Z}.$$

   This is the same *set* of solutions as above, simply map between them by $\ell \leftrightarrow k - 2$.

   (iii)★ The particular solution previously found was $m = -149, n = 12$. The general solution follows from
$$1 = (12 - 31k) \times 385 + (-149 + 385k) \times 31$$

   for $k \in \mathbb{Z}$, hence
$$m = -149 + 385k, \quad n = 12 - 31k \ \text{ for } k \in \mathbb{Z}.$$

   (iv) The particular solution previously found was $m = -320, n = 180$. The general solution follows from
$$20 = (180 - 41k) \times 73 + (-320 + 73k) \times 41$$

   for $k \in \mathbb{Z}$, hence
$$m = -320 + 73k, n = 180 - 41k \quad \text{for } k \in \mathbb{Z}.$$

   (v)★ The particular solution previously found was $m_0 = 7, n_0 = -8$. If (m, n) is the general solution we have both
$$93m + 81n = 3 \ \text{ and } \ 93m_0 + 81n_0 = 3.$$

Subtract and rearrange to get

$$93(m - m_0) = 81(n_0 - n).$$

At this stage divide through by $\gcd(93, 81) = 3$ to get

$$31(m - m_0) = 27(n_0 - n).$$

Then 31 divides the left hand side so it divides the right hand side.

Recall, if $\gcd(a, b) = d$ then $\gcd(a/d, b/d) = 1$. Hence $\gcd(31, 27) = 1$.

Recall, if $a|bc$ and $\gcd(a, b) = 1$ then $a|c$. Hence $31|(n_0 - n)$.

Thus $n_0 - n = 31k$, i.e. $n = n_0 - 31k$ for some $k \in \mathbb{Z}$. This is substituted back to give $m - m_0 = 27k$. Therefore the general solution is

$$m = 7 + 31k, \quad n = -8 - 41k \text{ for } k \in \mathbb{Z}.$$

(vi) From Question 2(ii) on Sheet 2 we know that $\gcd(527, 697) = 17$. Since $17 \nmid 13$ the Diophantine Equation has no solutions.

(vii)★ The particular solution previously found was $m_0 = -12, n_0 = 16$. If (m, n) is the general solution we have both

$$533m + 403n = 52 \text{ and } 533m_0 + 403n_0 = 52.$$

Subtract and rearrange to get

$$533(m - m_0) = 403(n_0 - n).$$

At this stage divide through by $\gcd(533, 403) = 13$ to get

$$41(m - m_0) = 31(n_0 - n).$$

Then 41 divides the left hand side so it divides the right hand side.

Recall, if $\gcd(a, b) = d$ then $\gcd(a/d, b/d) = 1$. Hence $\gcd(41, 31) = 1$.

Recall, if $a|bc$ and $\gcd(a, b) = 1$ then $a|c$. Hence $41|(n_0 - n)$.

Thus $n_0 - n = 41k$, i.e. $n = n_0 - 41k$ for some $k \in \mathbb{Z}$. This is substituted back to give $m - m_0 = 31k$. Therefore the general solution is

$$m = -12 + 31k, \quad n = 16 - 41k \text{ for } k \in \mathbb{Z},$$

(Recall that the general solution of $am + bn = c$ is

$$\left(m_0 + \frac{bk}{\gcd(a, b)}, n_0 - \frac{ak}{\gcd(a, b)}\right)$$

for $k \in \mathbb{Z}$.)

2. If the number of large boxes is x and small boxes y we must have $90x + 70y = 1100$ (all prices in pennies). Divide by 10 to get $9x + 7y = 110$. Euclid's Algorithm applied to 9 and 7 gives

$$\begin{aligned} 9 &= 1 \times 7 + 2, \\ 7 &= 3 \times 2 + 1. \end{aligned}$$

Work back to get

$$\begin{aligned} 1 &= 7 - 3 \times 2 = 7 - 3 \times (9 - 1 \times 7) \\ &= 4 \times 7 - 3 \times 9. \end{aligned}$$

Multiply by 110 to get $110 = 9 \times (-330) + 7 \times (440)$. Thus a particular solution is $x = -330$ and $y = 440$. This can not be a solution to our problem since the number of large boxes is negative!

Instead we look at the general solution that follows from

$$110 = 9 \times (-330 + 7t) + 7 \times (440 - 9t)$$

for $t \in \mathbb{Z}$.Thus the general solution is

$$x = -330 + 7t, y = 440 - 9t, t \in \mathbb{Z}.$$

We wish to find a solution in which both x and y are non-negative, i.e.

$$-330 + 7t \geq 0 \text{ and } 440 - 9t \geq 0.$$

These rearrange to

$$\frac{440}{9} \geq t \geq \frac{330}{7}, \text{ i.e. } 48.88... \geq t \geq 47.142...$$

From this we see only one possible value for t, namely $t = 48$, for which $x = 6$ and $y = 8$. So the unique answer is 6 large boxes and 8 small boxes.

3. Always check your answers by substituting back into the question.

(i) Euclid's Algorithm gives

$$\begin{aligned} 41 &= 31 + 10 \\ 31 &= 3 \times 10 + 1 \end{aligned}$$

Working back gives

$$1 = 4 \times 31 - 3 \times 41.$$

Multiply through by 4 to find

$$\begin{aligned} 4 &= 16 \times 31 - 12 \times 41 \\ &= (16 + 41k) \times 31 - (12 + 31k) \times 41 \end{aligned}$$

for all $k \in \mathbb{Z}$. Thus the general solution is $16 + 41k, k \in \mathbb{Z}$, written as $\mathbf{x \equiv 16 \bmod 41}$.

(ii) Euclid's Algorithm gives

$$\begin{aligned} 157 &= 97 + 60 \\ 97 &= 60 + 37 \\ 60 &= 37 + 23 \\ 37 &= 23 + 14 \\ 23 &= 14 + 9 \\ 14 &= 9 + 5 \\ 9 &= 5 + 4 \\ 5 &= 4 + 1. \end{aligned}$$

I leave it to the student to reverse this and derive

$$1 = 34 \times 97 - 21 \times 157. \quad (1)$$

Multiplying through by 2 we see that

$$\begin{aligned} 2 &= 68 \times 97 - 42 \times 157 \\ &= (68 + 157k) \times 97 - (42 + 97k) \times 157 \end{aligned}$$

for all $k \in \mathbb{Z}$. Thus the general solution is $68 + 157k, k \in \mathbb{Z}$, written as $\mathbf{x \equiv 68 \bmod 157}$.

Note that (1) was seen in the solution to Question 2(i), Sheet 2.

(iii)★ Note that 1679 and 2323 were seen earlier in Question 2(iii), Sheet 2, where the greatest common divisor of 23 was found. Since 23 does not divide 21 the congruence $1679x \equiv 21 \bmod 2323$ has **no solutions**.

(iv)★ Apply Euclid's algorithm to 87 and 105 to find that $\gcd(87, 105) = 3$. Since $3|57$ the congruence has solutions. Divide through the original congruence to get $29x \equiv 19 \bmod 35$.

Euclid's algorithm then gives

$$1 = -6 \times 29 + 5 \times 35.$$

Multiply through by 19 to find

$$\begin{aligned} 19 &= -114 \times 29 + 95 \times 35 \\ &= (-114 + 35k) \times 29 + (95 - 29k) \times 35 \end{aligned}$$

for all $k \in \mathbb{Z}$. Thus the general solution is $x \equiv -114 \equiv 26 \bmod 35$, or, in terms of the initial modulus,

$$\mathbf{x} \equiv \mathbf{26}, \mathbf{61} \text{ or } \mathbf{96} \bmod \mathbf{105}.$$

(v)★ Instead of repeating work already done, look back at Question 1(iii) to find

$$31 \times (-149) \equiv 1 \bmod 385.$$

Multiply through by 4 to find the general solution of the present question is

$$\mathbf{x} \equiv 4 \times (-149) = -596 \equiv \mathbf{174} \bmod \mathbf{385}.$$

(vi) Recall, if $ab \equiv ac \bmod m$ and $\gcd(a, m) = 1$ then $b \equiv a \bmod m$. Use this with the observation that the congruence is unaltered by the addition of multiples of the modulus to any of the numbers.

In particular,

$$32x \equiv 47 \equiv 47 + 385 \bmod 385,$$

which gives an even number on the right hand side and thus the possibility of cancelling a factor of 2. In fact $47 + 385 = 432 = 16 \times 27$ so we can divide both sides by 16 to get $2x \equiv 27 \bmod 385$.

Apply the same idea again, so $2x \equiv 27 + 385 = 412 \bmod 385$. Divide through by 2 to get $\mathbf{x} \equiv \mathbf{206} \bmod \mathbf{385}$.

(vii) Apply the idea seen in part vi to the coefficient of x, so

$$13 \equiv 47x \equiv (47 - 73)\, x = -26x \bmod 73.$$

Divide through by 13 to get $1 \equiv -2x \bmod 73$. Perhaps now use the method from (vi) and write $-2x \equiv 1 + 73 = 74 \bmod 73$, thus $-x \equiv 37 \bmod 73$. Then multiply by -1 to finish $\mathbf{x} \equiv \mathbf{-37} \equiv \mathbf{36} \bmod \mathbf{73}$.

(viii) Observe that all the integers are divisible by 6, so divide through by 6 to get $7x \equiv 15 \bmod 26$. Looking at a few small x we come across $7 \times 3 \equiv -5 \bmod 26$. Multiplying by -3 we see that $7 \times (-9) \equiv 15 \bmod 26$ and so the solution to the congruence is $x \equiv -9 \equiv 17 \bmod 26$.

There will be 6 solutions to the original congruence, all incongruent modulo 156, yet all congruent modulo 26. Thus in terms of the original modulus, the solutions are

$$\mathbf{x} \equiv \mathbf{17}, \mathbf{43}, \mathbf{69}, \mathbf{95}, \mathbf{121}, \mathbf{147} \bmod \mathbf{156}.$$

4. i) Solve $5x \equiv 1 \bmod 43$ to find that the inverse is **26**.

   ii) a) Multiply both sides by 26 to get $26 \times 5x \equiv 26 \times 17 \bmod 43$, i.e. $x \equiv 12 \bmod 43$.

   b) Since $25 = 5^2$ multiply both sides by 26^2 to get $x \equiv 26^2 \times 13 \equiv 16 \bmod 43$.

   c) Since 26 is the inverse of $5 \bmod 43$ then 5 is the inverse of 26. So multiply both sides by 5 to get $5 \times 26x \equiv 5 \times 41 \bmod 43$, i.e. $x \equiv 33 \bmod 43$.

5. (i) Write the two congruences as $x = 3 + 11k$ and $x = 4 + 13\ell$ for integers k, ℓ. Equate to get $3 + 11k = 4 + 13\ell$. Thus we get a linear Diophantine equation $11k - 13\ell = 1$. Use Euclid's Algorithm to find

$$\begin{aligned} 1 &= 11 \times 6 - 13 \times 5 \\ &= 11 \times (6 + 13t) - 15 \times (5 + 11t) \end{aligned}$$

   for all $t \in \mathbb{Z}$. Thus the general solution for k is $k = 6 + 13t$, which gives

$$x = 3 + 11\,(6 + 13t) = 69 + 143t$$

   for any $t \in \mathbb{Z}$. Expressed as a congruence the general solution is $\mathbf{x} \equiv \mathbf{69} \bmod \mathbf{143}$.

   (ii)★ Solve both congruences individually. For example, multiply the first congruence by 4 (since $4 \times 2 \equiv 1 \bmod 7$) and the second by 3 (since $3 \times 4 \equiv 1 \bmod 11$). We then have

$$\begin{aligned} x &\equiv 4 \bmod 7, \\ x &\equiv 18 \equiv 7 \bmod 11. \end{aligned}$$

Write $x = 4 + 7k$ and $x = 7 + 11\ell$. As before set $4 + 7k = 7 + 11\ell$ or $7k - 11\ell = 3$. If you **simply look** at this you should see a solution,

$$\begin{aligned} 3 &= 7 \times 2 - 11 \times 1 \\ &= 7 \times (2 + 11t) - 11 \times (1 + 7t) \end{aligned}$$

for all $t \in \mathbb{Z}$. Thus the general solution for k is $k = 2 + 11t$, which gives

$$x = 4 + 7(2 + 11t) = 18 + 77t$$

for any $t \in \mathbb{Z}$. Expressed as a congruence the general solution is $\mathbf{x \equiv 18 \bmod 77}$.

(iii)★ Write $x = 432 + 527k$ and $x = 324 + 697\ell$ so

$$697\ell - 527k = 432 - 324 = 108.$$

For this to have solutions we need $\gcd(697, 527) | 108$. Looking back to Question 2(ii), Sheet2, we see that $\gcd(697, 527) = 17$. Since $17 \nmid 108$ there are **no** solutions of the system.

(iv) Solve both congruences individually. But there is no need to do any work for this since we have seen both congruences previously.

From the solution to Question 3i, we can replace $31x \equiv 4 \bmod 41$ by $x \equiv 16 \bmod 41$. From the solution to Question 3(vii), we can replace $47x \equiv 13 \bmod 73$ by $x \equiv 36 \bmod 73$. Thus we have the system

$$\begin{aligned} x &\equiv 16 \bmod 41, \\ x &\equiv 36 \bmod 73. \end{aligned}$$

Write $x = 16 + 41k$ and $x = 36 + 73\ell$ and so $41k - 73\ell = 20$. We have seen this Diophantine Equation in Question 5(iv), Sheet 2. The general solution was found to be

$$(k, \ell) = (-320 + 73t, 180 + 41t),$$

$t \in \mathbb{Z}$. Thus the general solution for x is

$$\begin{aligned} x &= 16 + 41(-320 + 73t) \\ &= -13104 + 2993t, \end{aligned}$$

$t \in \mathbb{Z}$. Expressed as a congruence the general solution is

$$\mathbf{x \equiv -13104 \equiv 1861 \bmod 2993}.$$

(v)★ The methods from the course only work for pairs of congruences, so we first look at

$$\begin{aligned} x &\equiv 1 \bmod 4 \\ x &\equiv 2 \bmod 3. \end{aligned}$$

Equating $1 + 4k = 2 + 3\ell$ we find a solution of $k = 1, \ell = 1$ and so the general solution is $x \equiv 5 \bmod 12$. Thus we get a second pair of congruences

$$\begin{aligned} x &\equiv 5 \bmod 12, \\ x &\equiv 3 \bmod 7. \end{aligned}$$

Equating $5 + 12m = 3 + 7n$ we find a solution of $m = 1$, $n = 2$ and thus the general solution $\mathbf{x} \equiv \mathbf{17} \bmod \mathbf{84}$.

(vi) First, solve each congruence individually to get

$$\begin{aligned} x &\equiv 3 \bmod 7, \\ x &\equiv 9 \bmod 11, \\ x &\equiv 12 \bmod 13. \end{aligned}$$

Next, solve *any* pair. For example solve $x \equiv 3 \bmod 7$ and $x \equiv 12 \bmod 13$ to get $x \equiv 38 \bmod 91$.

Finally, introduce the unused congruence and solve the resulting pair $x \equiv 9 \bmod 11$ and $x \equiv 38 \bmod 91$. The solution of the triplet is $\mathbf{x} \equiv \mathbf{493} \bmod \mathbf{1001}$.

6. a) Squaring,

$$\begin{aligned} & 5^2 &=& \ 25 \equiv -16 \bmod 41, \\ \text{i)}\ & 5^4 &\equiv& \ (16)^2 \equiv \mathbf{10} \bmod 41, \\ & 5^8 &\equiv& \ 10^2 \equiv 18 \bmod 41, \\ \text{ii)}\ & 5^{16} &\equiv& \ 18^2 \equiv \mathbf{37} \equiv -4 \bmod 41, \\ & 5^{32} &\equiv& \ 4^2 \equiv 16 \bmod 41, \\ \text{iii)}\ & 5^{64} &=& \ 16^2 \equiv \mathbf{10} \bmod 41. \end{aligned}$$

b) From this list we note that $5^{64} \equiv 10 \equiv 5^4 \bmod 41$, and so on dividing through by 5^4 (coprime to 41) gives $5^{60} \equiv 1 \bmod 41$.

OR you might note from the list that

$$5^{16} \times 5^4 \equiv -4 \times 10 \equiv 1 \bmod 41.$$

So $5^{20} \equiv 1 \bmod 41$.

c) Multiply both sides of $5^2 x \equiv 7 \bmod 41$ by 5^{58} to get $5^{60} x \equiv 7 \times 5^{58}$ i.e. $x \equiv 7 \times 5^{58} \bmod 41$. Here

$$\begin{aligned} 7 \times 5^{58} &= 7 \times 5^{32} \times 5^{16} \times 5^8 \times 5^2 \\ &\equiv 7 \times 16 \times (-4) \times 18 \times (-16) \bmod 41 \\ &\equiv 38 \bmod 41. \end{aligned}$$

7. Squaring,

$$\begin{aligned} 3^2 &= 9 \equiv -2 \bmod 11, \\ 3^4 &\equiv (-2)^2 \equiv 4 \bmod 11, \\ 3^8 &\equiv 4^2 \equiv 5 \bmod 11, \\ 3^{16} &\equiv 5^2 \equiv 3 \bmod 11, \\ 3^{32} &\equiv 9 \bmod 11. \end{aligned}$$

So $3^{40} = 3^{32} 3^8 \equiv 9 \times 5 \equiv 1 \bmod 11$.

Note that $40^{35} \equiv 7^{35} \equiv (-4)^{35} \equiv -(4^{35}) \bmod 11$. Also, from this list we see that $4 \equiv 3^4 \bmod 11$ so we can read off the first few lines below from the list above.

$$\begin{aligned} 4^2 &\equiv 3^8 \equiv 5 \bmod 11, \\ 4^4 &\equiv 3^{16} \equiv 3 \bmod 11, \\ 4^8 &\equiv 3^{32} \equiv 9 \equiv -2 \bmod 11, \\ 4^{16} &\equiv (-2)^2 \equiv 4 \bmod 11, \\ 4^{32} &\equiv 4^2 \equiv 5 \bmod 11. \end{aligned}$$

Thus $40^{35} \equiv -(4^{32} \times 4^2 \times 4) \equiv -(5 \times 5 \times 4) \equiv 10 \bmod 11$.

Finally, $3^{40} + 40^{35} \equiv 1 + 10 \equiv 0 \bmod 11$.