MATH10101, for supervision in week 09. Euclid's algorithm. Diophantine equations — SOLUTIONS

($\star$)**Q9**. Let a, b be integers. Use Bezout's Lemma to prove that every common divisor of a and b divides $\gcd(a, b)$.

Q9 - solution. Let c be a common divisor of a and b. This means that $c \mid a$ and $c \mid b$, so by definition $a = ck$, $b = c\ell$ for some integers k, ℓ. By Bezout's Lemma, $\gcd(a, b) = am + bn$ for some integers m, n, which rewrites as $ckm + c\ell n = c(km + \ell n)$ and is divisible by c because $km + \ell n$ is an integer.

Q10. Find the greatest common divisors of the following pairs of integers. In each case write the greatest common divisor as an integral linear combination of the two initial numbers.

(i) $(97, 157)$; (ii) $(2323, 1679)$; (iii) $(10^{10} - 1, 10^9 - 1)$.

Q10 - solution. (i) Answer: $\gcd(97, 157) = 1 = 34 \times 97 - 21 \times 157$.

(ii) Answer: $\gcd(2323, 1679) = 23 = 18 \times 1679 - 13 \times 2323$. See the solution to **Q12** for detailed examples of calculation using Euclid's algorithm.

(iii) Solution: Euclid's algorithm.
$9, 999, 999, 999 = 999, 999, 999 \times 10 + 9$;
$999, 999, 999 = 9 \times 111, 111, 111 + 0$.
Hence the gcd is 9, written as $9 = 1 \times (10^{10} - 1) - 10 \times (10^9 - 1)$.

Of course, in the same way one can show that $\gcd(10^{n+1} - 1, 10^n - 1) = 9$ for all $n \geq 1$.

Remark: given two integers a, b, the gcd of a and b is unique. The integers m, n such that $ma + nb = \gcd(a, b)$ are not unique: one such linear combination can be found by working back up Euclid's algorithm, but there are infinitely many others.

($\star$)**Q11**. (i) Use Euclid's algorithm to show that $\gcd(589, 779) = 19$.

($\star$)(ii) Write 19 as an integral linear combination of 589 and 779.

($\star$)(iii) Find all solutions $(x, y) \in \mathbb{Z}^2$ to the homogeneous equation $589x + 779y = 0$.

($\star$)(iv) Find all solutions $(x, y) \in \mathbb{Z}^2$ to the equation $589x + 779y = 19$.

($\star$)(v) Find all solutions $(x, y) \in \mathbb{Z}^2$ to the equation $589x + 779y = -190$.

($\star$)(vi) Find all solutions $(x, y) \in \mathbb{Z}^2$ to the equation $589x + 779y = 119$.

Q11 - solution. (i) We show the calculation here. Apply Euclid's algorithm to $a = 589$, $b = 779$:

$$\begin{aligned} 589 &= 779 \times 0 + 589 && (\textit{or simply swap } a \textit{ and } b \textit{ if } a < b) \\ 779 &= 589 \times 1 + 190 && (**) \\ 589 &= 190 \times 3 + \mathbf{19} && (*) \\ 190 &= 19 \times 10 + 0 \end{aligned}$$

(ii) To obtain 19 as an integral linear combination of 589 and 779, work back up the algorithm starting from row $(*)$:

$$\begin{aligned} 19 &\underset{(*)}{=} 589 - 190 \times 3 \\ &\underset{(**)}{=} 589 - (779 - 589) \times 3 = 589 \times 4 - 779 \times 3. \end{aligned}$$

Answer: $\gcd(589, 779) = 19 = 527 \times 4 - 779 \times 3$.

(iii) The solutions of the homogeneous equation $589x + 779y = 0$ are pairs $(x, y) = (-\frac{589}{19}k, \frac{779}{19}k) = (-41k,\ 31k)$, $k \in \mathbb{Z}$.

The most straightforward way to solve the equation is to divide through by 19, obtaining an equivalent equation $31x + 41y = 0$, same as $31x = -41y$. Since $-41 \mid 31x$ and -41 is coprime to 31 one has $-41 \mid x$ and so $x = -41k$, $k \in \mathbb{Z}$. Substitution gives $y = 31k$.

(iv) From (ii) we know that $x_0 = 4$, $y_0 = -3$ is a particular solution to the equation $589x + 779y = 19$. The general solution is obtained by adding to it the general solution of the corresponding homogeneous equation, $589x + 779y = 0$. Hence from part (iii), $x = 4 - 41k$, $y = -3 + 31k$, $k \in \mathbb{Z}$ is the general solution.

(v) We could multiply the particular solution found in (ii) by -10 to obtain a particular solution of $589x + 779y = -190$. However, in this case it is easy to notice that $589 - 779 = -190$. Hence $x_0 = 1$, $y_0 = -1$ is a particular solution. Adding to this the solution of the homogeneous equation, we obtain the general solution $(x, y) = (1 - 41k,\ -1 + 31k)$, $k \in \mathbb{Z}$.

Attention: a common mistake in this case is to take the general solution to (iv), multiply it by -10 and claim that $(-40 + 410k,\ 30 - 310k)$, $k \in \mathbb{Z}$, is the general solution to $589x + 779y = -190$. This is incorrect: this formula gives *some* of the solutions to the equation but not all, because it only generates solutions where both x and y are divisible by 10.

(vi) Since $\gcd(589, 779) = 19$ and $19 \nmid 119$, this Diophantine equation has no solutions.

Q12. Find the greatest common divisors of (i) 15691 and 44517, (ii) 173417 and 159953.

Q12 - solution. Part (i):

$$\begin{aligned}
44517 &= 2 \times 15691 + 13135 \\
15691 &= 1 \times 13135 + 2556 \\
13135 &= 5 \times 2556 + 355 \\
2556 &= 7 \times 355 + 71 \\
355 &= 5 \times 71 + 0.
\end{aligned}$$

Hence $\gcd(44517, 15691) = 71$, the last non-zero remainder.

Working back up:

$$\begin{aligned}
71 &= 2556 - 7 \times 355 \\
&= 2556 - 7 \times (13135 - 5 \times 2556) \\
&= 36 \times 2556 - 7 \times 13135 \\
&= 36 \times (15691 - 1 \times 13135) - 7 \times 13135 \\
&= 36 \times 15691 - 43 \times 13135 \\
&= 36 \times 15691 - 43 \times (44517 - 2 \times 15691) \\
&= 122 \times 15691 - 43 \times 44517.
\end{aligned}$$

Part (ii):

$$\begin{aligned}
173417 &= 1 \times 159953 + 13464 \\
159953 &= 11 \times 13464 + 11849 \\
13464 &= 1 \times 11849 + 1615 \\
11849 &= 7 \times 1615 + 544 \\
1615 &= 2 \times 544 + 527 \\
544 &= 1 \times 527 + 17 \\
527 &= 31 \times 17 + 0.
\end{aligned}$$

Hence $\gcd(173417, 159953) = 17$, the last non-zero remainder.

Working back up:

$$\begin{aligned}
17 &= 544 - 1 \times 527 \\
&= 544 - 1 \times (1615 - 2 \times 544) \\
&= 3 \times 544 - 1 \times 1615 \\
&= 3 \times (11849 - 7 \times 1615) - 1 \times 1615 \\
&= 3 \times 11849 - 22 \times 1615 \\
&= 3 \times 11849 - 22 \times (13464 - 1 \times 11849) \\
&= 25 \times 11849 - 22 \times 13464 \\
&= 25 \times (159953 - 11 \times 13464) - 22 \times 13464 \\
&= 25 \times 159953 - 297 \times 13464 \\
&= 25 \times 159953 - 297 \times (173417 - 1 \times 159953) \\
&= 322 \times 159953 - 297 \times 173417.
\end{aligned}$$

Q13. For further practice, find **all** solutions $(x, y) \in \mathbb{Z}^2$ to the following equations.

Reminder *In each case, start by finding a particular solution, either by inspection or by Euclid's algorithm. Then write down the general solution. You should* **check** *your answer.*

(i) $3x + 5y = 1$;
(ii) $2x + 15y = 4$;
(iii) $31x + 385y = 1$;
(iv) $41x + 73y = 20$;
(v) $93x + 81y = 3$;
(vi) $533x + 403y = 52$.

Q13 - solution. If $\gcd(a, b) \,|\, c$, the process of solving $ax + by = c$ leads to general solution in the form

$$\left(x_0 - \frac{bk}{\gcd(a,b)},\ y_0 + \frac{ak}{\gcd(a,b)}\right) \quad \text{for } k \in \mathbb{Z}.$$

where (x_0, y_0) is (any) particular solution. We will make use of this formula.

(i) By observation $m = 2$, $n = -1$ is a solution. Also, $\gcd(3, 5) = 1$ so the general solution is

$$m = 2 - 5k, \qquad n = -1 + 3k, \qquad k \in \mathbb{Z}.$$

Check it!

(ii) Without thinking we can use Euclid's algorithm to solve $2x + 15y = \gcd(2, 15) = 1$, finding $2 \times (-7) + 15 \times 1 = 1$. Multiply through by 4 to get the particular solution $x_0 = -28$, $y_0 = 4$.

Alternatively you could stare at $2x+15y = 4$ for a minute to see that $x_0 = 2$, $y_0 = 0$ is a solution.

Then the general solution is

$$x = 2 - 15k, \qquad y = 2k, \qquad k \in \mathbb{Z}.$$

Check it!

(iii) Euclid's Algorithm gives

$$\begin{aligned} 385 &= 12 \times 31 + 13 \\ 31 &= 2 \times 13 + 5 \\ 13 &= 2 \times 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Working back we find that

$$1 = 31(-149) + 385 \times 12.$$

So a particular solution is $x_0 = -149$, $y_0 = 12$.

We demonstrated that $\gcd(31, 385) = 1$, so the general solution is

$$x = -149 - 385k, \qquad y = 12 + 31k \qquad \text{for } k \in \mathbb{Z}.$$

Check:

$$1 = 31\,(-149 - 385k) + 385\,(12 + 31k)\,.$$

(iv) Euclid's Algorithm gives

$$\begin{aligned}
73 &= 41 + 32 \\
41 &= 32 + 9 \\
32 &= 3 \times 9 + 5 \\
9 &= 5 + 4 \\
5 &= 4 + 1.
\end{aligned}$$

Working back we find that

$$1 = 41(-16) + 73 \times 9.$$

Multiply by 20 to get

$$20 = 41(-320) + 73 \times 180.$$

So a particular solution is $x_0 = -320$, $y_0 = 180$.

The general solution is then

$$x = -320 - 73k, \qquad y = 180 + 41k \qquad \text{for } k \in \mathbb{Z}.$$

(v) With these small coefficients it is easy to see that both 93 and 81 are multiples of 3. Start by dividing through by 3 to get $31m + 27n = 1$.

We quickly find by Euclid's Algorithm that $1 = 31 \times 7 + 27(-8)$ (confirming that $\gcd(31, 27) = 1$) so a particular solution is $x_0 = 7$, $y_0 = -8$.

Here is a detailed argument to derive the general solution. (These steps are not necessary if we simply use the formula above.) If (x, y) is a solution we have both

$$93x + 81y = 3 \quad \text{and} \quad 93x_0 + 81y_0 = 3.$$

Subtract and rearrange to get

$$93\,(x_0 - x) = 81\,(y - y_0)\,.$$

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

$$31\,(x_0 - x) = 27\,(y - y_0)\,.$$

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

Recall that $\gcd(31, 27) = 1$. Recall also the Coprime Factor Lemma which says that if $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$. Hence $31 \mid (y - y_0)$.

Thus $y - y_0 = 31k$, i.e. $y = y_0 + 31k$ for some $k \in \mathbb{Z}$. This is substituted back to give $x - x_0 = -27k$. Therefore the general solution is

$$x = 7 - 27k, \qquad y = -8 + 31k \qquad \text{for } k \in \mathbb{Z}.$$

(vi) Euclid's Algorithm gives

$$\begin{aligned} 533 &= 403 + 130, \\ 403 &= 3 \times 130 + 13, \\ 130 &= 10 \times 13. \end{aligned}$$

Hence $\gcd(533, 403) = 13$. Since $13 \mid 52$ the equation has solutions.

Working back we find that

$$13 = 533(-3) + 403 \times 4.$$

Multiply through by 4 to get

$$52 = 533(-12) + 403 \times 16,$$

giving a particular solution of $x_0 = -12$, $y_0 = 16$.

Therefore the general solution is

$$x = -12 - 31k, \qquad y = 16 + 41k \qquad \text{for } k \in \mathbb{Z}.$$

Here $31 = \frac{403}{13}$ and $41 = \frac{533}{13}$ with $13 = \gcd(533, 403)$. Check the solution!

Q14. Let $a, b \in \mathbb{Z}$. Prove formally: a, b are coprime $\iff \exists m, n \in \mathbb{Z}$: $am + bn = 1$.

Q14 - solution. Recall "a and b are coprime" by definition means $\gcd(a, b) = 1$.

$\implies$: assume that $\gcd(a, b) = 1$. Then by Bezout's lemma there exist $m, n \in \mathbb{Z}$ such that $am + bn = 1$, as required.

$\impliedby$: assume that $am + bn = 1$ for integers m, n, and let $d = \gcd(a, b)$. Note that $\gcd$ is always non-negative (it is zero in the $\gcd(0, 0)$ and is ≥ 1 otherwise because 1 is a common divisor).

Since d is a common divisor of a and b, we have $a = dk$, $b = d\ell$ for some integers k, ℓ. Then $1 = dkm + d\ell n = d(km + \ell n)$ so $d \mid 1$. The only non-negative integer which divides 1 is 1. So $d = 1$ meaning a, b are coprime.

Q15. Continuing on from the previous question, find m and n to show that (i) 41 and 68 are coprime; (ii) 71 and 118 are coprime.

More generally, prove that $3k + 2$ and $5k + 3$ are coprime for all $k \in \mathbb{Z}$.

Q15 - solution. (i) $41 \times 5 - 68 \times 3 = 1$, (ii) $71 \times 5 - 118 \times 3 = 1$.

For $(3k + 2, 5k + 3)$ note that if you choose $k = 13$ you recover Part i while $k = 23$ gives Part ii. This observation might suggest considering the same linear combination seen in the answers to both parts, i.e.

$$(3k + 2) \times 5 - (5k + 3) \times 3 = 1,$$

which is true and implies that $\gcd(3k + 2, 5k + 3) = 1$.

Q16. (*Important*) Prove that if $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(ab, c) = 1$.

Q16 - solution. Solution #1: Let $d = \gcd(ab, c)$. Our goal is to prove that $d = 1$. Since d is a common divisor of ab and c, we have $d \mid c$. Then

(*) $$\gcd(d, b) = 1 :$$

indeed, a common divisor of d and b is also a common divisor of c and b (which are coprime) hence is less than or equal to 1. Now, $d \mid ab$ and d, b are coprime, hence by the Coprime Factor Lemma from the course $d \mid a$.

Since nothing changes if we swap a and b, we can show in the same way that d is coprime to a and $d \mid b$. Now, $d \mid b$ implies that

(**) $$\gcd(d, b) = d$$

From (*) and (**), $d = 1$ as claimed.

Solution #2:

$$\begin{aligned} \gcd(a, c) = 1 &\implies \exists s, t \in \mathbb{Z} : sa + tc = 1, \\ \gcd(b, c) = 1 &\implies \exists p, q \in \mathbb{Z} : pb + qc = 1. \end{aligned}$$

Multiplying together gives

$$\begin{aligned} (sa + tc)(pb + qc) = 1 \quad &\iff \quad (sa)(pb) + (sa)(qc) + (tc)(pb) + (tc)(qc) = 1 \\ &\iff \quad (sp)ab + (saq + tpb + tcq)c = 1. \end{aligned}$$

That is, with $m = sp$, $n = saq + tpb + tcq \in \mathbb{Z}$, we have $m(ab) + nc = 1$ which implies that $\gcd(ab, c) = 1$.

Q17. Alison spends £11.00 on sweets for prizes in a contest. If a large box of sweets costs 90p and a small box 70p, how many boxes of each size did she buy?

Q17 - solution. 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 cannot be a solution to our problem since the number of large boxes is negative!

Instead we look at the general solution

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

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

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

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.

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