Math Circles - Solution Set 1
Introduction to Linear Diophantine Equations

Zack Cramer - zcramer@uwaterloo.ca

February 28, 2018

1. Use the Euclidean algorithm to compute the following GCDs:

(a) $\gcd(204, 99)$

Solution. The Euclidean algorithm proceeds as follows:

$$204 = 99(2) + 6 \quad \Rightarrow \quad \gcd(204, 99) = \gcd(99, 6) \tag{1}$$

$$99 = 6(16) + 3 \quad \Rightarrow \quad \gcd(99, 6) = \gcd(6, 3) \tag{2}$$

$$6 = 3(2) + 0 \quad \Rightarrow \quad \gcd(6, 3) = \gcd(3, 0) = \underline{3}.$$

The process ends and we conclude that $\gcd(204, 99) = 3$.

(b) $\gcd(1\,053, 993)$

Solution. The Euclidean algorithm proceeds as follows:

$$1\,053 = 993(1) + 60 \quad \Rightarrow \quad \gcd(1\,053, 993) = \gcd(993, 60) \tag{1}$$

$$993 = 60(16) + 33 \quad \Rightarrow \quad \gcd(993, 60) = \gcd(60, 33) \tag{2}$$

$$60 = 33(1) + 27 \quad \Rightarrow \quad \gcd(60, 33) = \gcd(33, 27) \tag{3}$$

$$33 = 27(1) + 6 \quad \Rightarrow \quad \gcd(33, 27) = \gcd(27, 6) \tag{4}$$

$$27 = 6(4) + 3 \quad \Rightarrow \quad \gcd(27, 6) = \gcd(6, 3) \tag{5}$$

$$6 = 3(2) + 0 \quad \Rightarrow \quad \gcd(6, 3) = \gcd(3, 0) = \underline{3}.$$

The process ends and we conclude that $\gcd(1\,053, 993) = 3$.

(c) $\gcd(7\,404, 7\,032)$

Solution. The Euclidean algorithm proceeds as follows:

$$
\begin{aligned}
7\,404 &= 7\,032(1) + 372 &\Rightarrow\quad& \gcd(7\,404, 7\,032) = \gcd(7\,032, 372) && (1)\\
7\,032 &= 372(18) + 336 &\Rightarrow\quad& \gcd(7\,032, 372) = \gcd(372, 336) && (2)\\
372 &= 336(1) + 36 &\Rightarrow\quad& \gcd(372, 336) = \gcd(336, 36) && (3)\\
336 &= 36(9) + 12 &\Rightarrow\quad& \gcd(336, 36) = \gcd(36, 12) && (4)\\
36 &= 12(3) + 0 &\Rightarrow\quad& \gcd(36, 12) = \gcd(12, 0) = \underline{12}.
\end{aligned}
$$

The process ends and we conclude that $\gcd(7\,404, 7\,032) = 12$.

2. Find a solution for each of the following LDEs, or explain why one does not exist.

(a) $204x + 99y = 3$

Solution. Since $\gcd(204, 99) = 3$ divides 3, a solution exists. To find it, we work backwards through the Euclidean algorithm:

$$
\begin{aligned}
3 &= 99 - \underline{6}(16) && \text{by (2)}\\
&= 99 - [204 - 99(2)](16) && \text{by (1)}\\
&= 99(33) + 204(-16).
\end{aligned}
$$

A solution to our LDE is $204(-16) + 99(33) = 3$.

(b) $1\,053x + 993y = 7$

Solution. Since $\gcd(1\,053, 993) = 3$ does not divide 7, this LDE has no solution.

(c) $7\,404x + 7\,032y = 36$

Solution. Since $\gcd(7\,404, 7\,032) = 12$ divides 36, a solution exists. To find it, we work backwards through the Euclidean algorithm:

$$\begin{aligned}
12 &= 336 - \underline{36}(9) && \text{by (4)} \\[1em]
&= 336 - [372 - 336(1)](9) && \text{by (3)} \\
&= \underline{336}(10) - 372(9) \\[1em]
&= [7\,032 - 372(18)](10) - 372(9) && \text{by (2)} \\
&= 7\,032(10) - \underline{372}(-189) \\[1em]
&= 7\,032(10) - [7\,404 - 7\,032(1)](-189) && \text{by (1)} \\
&= 7\,032(199) + 7\,404(-189)
\end{aligned}$$

We arrive at the equation

$$7\,404(-189) + 7\,032(199) = 12.$$

To finish, we multiply both sides of this equation by $36/12 = 3$ and obtain the following solution to our LDE:

$$7\,404(-567) + 7\,032(597) = 36.$$

3. Can 10 000 be expressed as a sum of two integers, one of which is divisible by 126 and the other divisible by 81? If so, find examples of such integers. If not, explain why.

Solution. We would like to know if there are integers x_0 and y_0 so that x_0 is divisible by 126, y_0 is divisible by 81, and $x_0 + y_0 = 10\,000$. Since x_0 is divisible by 126, we can write

$$x_0 = 126x$$

for some integer x. Likewise, we can write

$$y_0 = 81y$$

for some integer y. Replacing x_0 and y_0 in the equation $x_0 + y_0 = 10\,000$, we have

$$126x + 81y = 10\,000.$$

So, we are really looking for a solution to the above linear diophantine equation.

To see if a solution exists, we will see if $\gcd(126, 81)$ divides 10 000. To find this GCD, we use the Euclidean algorithm:

$$\begin{aligned}
126 &= 81(1) + 45 &&\Rightarrow \quad \gcd(126, 81) = \gcd(81, 45) \\[1em]
81 &= 45(1) + 36 &&\Rightarrow \quad \gcd(81, 45) = \gcd(45, 36) \\[1em]
45 &= 36(1) + 9 &&\Rightarrow \quad \gcd(45, 36) = \gcd(36, 9) \\[1em]
36 &= 9(4) + 0 &&\Rightarrow \quad \gcd(36, 9) = \gcd(9, 0) = \underline{9}.
\end{aligned}$$

We end the Euclidean algorithm to find that $\gcd(126, 81) = 9$.

Does 9 divide 10 000? No. Thus, there is no solution to the above LDE, and we conclude that no such integers x_0 and y_0 exist.

4. Can 10 000 be expressed as a sum of two integers, one of which is divisible by 614 and the other divisible by 72? If so, find examples of such integers. If not, explain why.

Solution. We would like to know if there are integers x_0 and y_0 so that x_0 is divisible by 614, y_0 is divisible by 72, and $x_0 + y_0 = 10\,000$. Since x_0 is divisible by 614, we can write

$$x_0 = 614x$$

for some integer x. Likewise, we can write

$$y_0 = 72y$$

for some integer y. Replacing x_0 and y_0 in the equation $x_0 + y_0 = 10\,000$, we have

$$614x + 72y = 10\,000.$$

So, we are really looking for a solution to the above linear diophantine equation.

To see if a solution exists, we will see if $\gcd(614, 72)$ divides 10 000. To find this GCD, we use the Euclidean algorithm:

$$614 = 72(8) + 38 \quad \Rightarrow \quad \gcd(614, 72) = \gcd(72, 38) \tag{1}$$

$$72 = 38(1) + 34 \quad \Rightarrow \quad \gcd(72, 38) = \gcd(38, 34) \tag{2}$$

$$38 = 34(1) + 4 \quad \Rightarrow \quad \gcd(38, 34) = \gcd(34, 4) \tag{3}$$

$$34 = 4(8) + 2 \quad \Rightarrow \quad \gcd(34, 4) = \gcd(4, 2) \tag{4}$$

$$4 = 2(2) + 0 \quad \Rightarrow \quad \gcd(4, 2) = \gcd(2, 0) = \underline{2}.$$

We end the Euclidean algorithm to find that $\gcd(614, 72) = 2$.

Does 2 divide 10 000? Yes! Such numbers x_0 and y_0 do exist. To find them, we have to work backwards through the Euclidean algorithm:

$$
\begin{aligned}
2 &= 34 - \underline{4}(8) && \text{by (4)} \\[1ex]
&= 34 - [38 - 34(1)](8) && \text{by (3)} \\
&= \underline{34}(9) - 38(8) \\[1ex]
&= [72 - 38(1)](9) - 38(8) && \text{by (2)} \\
&= 72(9) - \underline{38}(17) \\[1ex]
&= 72(9) - [614 - 72(8)](17) && \text{by (1)} \\
&= 614(-17) + 72(145)
\end{aligned}
$$

This means that $614(-17)+72(145) = 2$. To get $10\,000$ on the right-hand side, multiply both sides of this equation by $10\,000/2 = 5\,000$. We get

$$614(-85\,000) + 72(725\,000) = 10\,000.$$

Note that $614(-85\,000)$ is divisible by 614, and $72(725\,000)$ is divisible by 72.

5. Find an integer n, which, when divided by 78 leaves a remainder of 37; and when divided by 29 leaves a remainder of 17.

Solution. If n has a remainder of 37 when divided by 78, then by the division algorithm we can write

$$n = 78x + 37 \tag{1}$$

for some integer x. Likewise, the same n may be written as

$$n = 29y + 17 \tag{2}$$

for some integer y. Since n is the same in both equations, it must be the case that $78x + 37 = 29y + 17$. By rearranging the terms, we arrive at the LDE

$$78x + 29(-y) = -20.$$

If we can find a solution to this LDE, we can use equation (1) or (2) to obtain n. Our first step is to find $\gcd(78, 29)$:

$$
\begin{aligned}
78 &= 29(2) + 20 &&\Rightarrow&& \gcd(78,29) = \gcd(29,20) && (3) \\[1ex]
29 &= 20(1) + 9 &&\Rightarrow&& \gcd(29,20) = \gcd(20,9) && (4) \\[1ex]
20 &= 9(2) + 2 &&\Rightarrow&& \gcd(20,9) = \gcd(9,2) && (5) \\[1ex]
9 &= 2(4) + 1 &&\Rightarrow&& \gcd(9,2) = \gcd(2,1) && (6) \\[1ex]
2 &= 1(2) + 0 &&\Rightarrow&& \gcd(2,1) = \gcd(1,0) = \underline{1}.
\end{aligned}
$$

We end the Euclidean algorithm to find that $\gcd(78, 29) = 1$. Since 1 divides -20, a solution to this LDE exists. To find it, we have to work backwards through the Euclidean algorithm:

$$
\begin{aligned}
1 &= 9 - \underline{2}(4) && \text{by (6)} \\[1em]
&= 9 - [20 - 9(2)](4) && \text{by (5)} \\
&= \underline{9}(9) - 20(4) \\[1em]
&= [29 - 20(1)](9) - 20(4) && \text{by (4)} \\
&= 29(9) - \underline{20}(13) \\[1em]
&= 29(9) - [78 - 29(2)](13) && \text{by (3)} \\
&= 78(-13) + 29(35).
\end{aligned}
$$

This means that $78(-13) + 29(35) = 1$. We get a solution to our LDE by multiplying both sides of this equation by -20. The equation becomes

$$78(260) + 29(-700) = -20,$$

and hence our solution is $(x, -y) = (260, -700)$ (i.e., $x = 260, y = 700$).

We may now use either equation (1) or equation (2) to get n. By plugging $x = 260$ into equation (1), we get $n = 20\,317$.

6. (a) Use the Euclidean algorithm to find a solution to $25x + 10y = 215$, the LDE from example (III).

Solution. When solving an LDE, our first step is always to find the GCD of the coefficients using the Euclidean algorithm:

$$
\begin{aligned}
25 &= 10(2) + 5 &&\Rightarrow\quad \gcd(25, 10) = \gcd(10, 5) \\[1em]
10 &= 5(2) + 0 &&\Rightarrow\quad \gcd(10, 5) = \gcd(5, 0) = \underline{5}
\end{aligned}
$$

We end the Euclidean algorithm to find that $\gcd(25, 10) = 5$.

Does 5 divide 215? Yes! This means that a solution to our LDE exists. To find it, we have to work backwards through the Euclidean algorithm.

Since our algorithm ended so quickly, it is easy to see that $5 = 25 - 10(2)$. By multiplying both sides of this equation by $215/5 = 43$, we get

$$25(43) + 10(-86) = 215.$$

(b) Does your answer in part (a) make sense in the context of the problem? If not, how can we find a solution that does make sense?

Solution. The answer does not make sense in the context of the problem. The solution we obtained in (a) suggests that we should use 43 quarters and -86 dimes to total \$2.15. What we are really looking for is a solution to the LDE

$$25x + 10y = 215$$

where both x and y are non-negative integers.

One way to rectify this problem is the following: for every 5 dimes we are told to subtract, we just add 2 fewer quarters (since 5 dimes and 2 quarters both total 50 cents). So by taking away $36 = 2(18)$ quarters, we can add $90 = 5(18)$ dimes. This means that $x = 43 - 36 = 7$ and $y = -86 + 90 = 4$ is another solution to the LDE

$$25x + 10y = 215.$$

That is, Becky can buy the coffee with 7 quarters and 4 dimes. We'll talk more about constraints like this in the second lesson.

Challenge Problems

7. (a) Use the division algorithm to show that $\gcd(k + 1, k) = 1$ for any integer k.

Solution. Recall from the division algorithm that if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$. How can we use this to solve our problem?

Well, we can write

$$(k + 1) = k(1) + 1.$$

Here $k + 1$ is playing the role of a, k is playing the role of b, and 1 is playing the roles of q and r. Thus,

$$\gcd(k + 1, k) = \gcd(k, 1) = 1.$$

(b) Use part (a) and two application of the division algorithm (i.e., the Euclidean algorithm) to show that

$$\gcd(7k + 6, 6k + 1) = 1$$

for any integer $k \geq 1$.

Solution. We're going to try an approach similar to that in part (a). First, let's use the division algorithm once to write

$$(7k+6) = (6k+5)(1) + (k+1).$$

Here, $7k+6$ is playing the role of a, $6k+5$ is playing the role of b, 1 is playing the role of q, and k is playing the role of r. We deduce from the statement of the division algorithm that

$$\gcd(7k+6, 6k+5) = \gcd(6k+5, k+1).$$

Again, we'll apply the division algorithm to our new pair to get

$$(6k+5) = (k+1)(5) + k.$$

Now the roles of a, b, q and r are played by $6k+5$, $k+1$, 5, and k, respectively. The statement of the division algorithm tells us that

$$\gcd(6k+5, k+1) = \gcd(k+1, k),$$

which we know to be 1 from part (a).

Putting it all together, we get

$$\gcd(7k+6, 6k+5) = \gcd(6k+5, k+1) = \gcd(k+1, k) = 1.$$

8. (a) Let a and b be integers. For which integers c does $ax + by = c$ have a solution?

Solution. Our theorem tells us that $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides c. Thus, c can be any multiple of $\gcd(a, b)$.

(b) Let a, b, and c be integers. For which integers d does $ax + by + cz = d$ have a solution?

Solution. This one may look daunting at first, but it's really nothing new.

Let's first consider at all possible integer combinations of the first two terms. Which numbers can be written as $ax + by$ for some integers x and y? These are precisely the combinations from part (a)! Thus, the numbers that we can write as $ax + by$ are exactly the multiply of $\gcd(a, b)$.

This means that I can replace the term $ax+by$ in my 3-variable LDE with multiples of $\gcd(a, b)$. The equation now looks like

$$ax + by + cz = d \quad \longrightarrow \quad \gcd(a, b)w + cz = d$$

where w is a new variable replacing x and y.

For what values of d does the new equation $\gcd(a,b)w + cz = d$ have a solution? Since this is now a 2-variable LDE, we can use part (a). Neat!

The LDE has a solution whenever d is a multiple of $\gcd(\gcd(a,b),c)$.

(c) Find a solution to the 3-variable LDE $18x + 14y + 63z = 5$.

Solution. How would one go about solving an LDE with 3-variables? As we saw in part (b), the equation can be rewritten as

$$\gcd(18,14)w + 63z = 5.$$

This gives us a plan of attack: we'll first solve this 2-variable LDE for w and z. To get a solution for our original equation, we should then find x and y so that $18x+14y = \gcd(18,14)w$. Thus, we have to solve 2 LDEs, each with 2 unknowns.

First, we must find $\gcd(18,14)$ in order to rewrite our equation.

$$\begin{aligned} 18 &= 14(1) + 4 &\Rightarrow\quad& \gcd(18,14) = \gcd(14,4) \\ 14 &= 4(3) + 2 &\Rightarrow\quad& \gcd(14,4) = \gcd(4,2) \\ 4 &= 2(2) + 0 &\Rightarrow\quad& \gcd(4,2) = \gcd(2,0) = \underline{2} \end{aligned}$$

The Euclidean algorithm ends with $\gcd(18,14) = 2$.

Thus, we may rewrite the equation as

$$2x + 63z = 5.$$

To solve this equation, we again use the Euclidean algorithm to find $\gcd(63,2)$:

$$\begin{aligned} 63 &= 2(31) + 1 &\Rightarrow\quad& \gcd(63,2) = \gcd(2,1) \\ 2 &= 1(2) + 0 &\Rightarrow\quad& \gcd(2,1) = \gcd(1,0) = \underline{1}. \end{aligned}$$

Therefore $\gcd(63,2) = 1$, and by working backwards we have $2(-31)+63(1) = 1$. Multiplying by 5, we obtain a solution to our transformed LDE:

$$2(-155) + 63(5) = 5.$$

Now we must express $2(-155)$ as $18x+14y$ for some integers x and y. We carried out the Euclidean algorithm for this pair and found that $\gcd(18,14) = 2$. Working backwards, we have

$$2 = 14 - 4(3) = 14 - [18 - 14(1)](3) = 18(-3) + 14(4)$$

Multiply both sides of this equation by -155 to get

$$18(465) + 14(-620) = 2(-155).$$

Whew! Putting this back into the equation $2(-155)+63(5) = 5$, we find a solution to our original LDE:

$$18(465) + 14(-620) + 63(5) = 5.$$