Math Diversion Problem 504

P. Reany

April 8, 2025

> Ask, and it shall be given you; seek, and ye shall find;
> knock, and it shall be opened unto you:
> — Matthew 7:7

1 The Problem

```
Title: Applying Euclid's Algorithm
 Presenter:  Patrick
```

Given the relation

$$18x - 25y = 1\,, \tag{1}$$

solve for integers x, y.

2 The Preparation

The Euclidean Algorithm will aid in this procedure.[1]

If we can find a solution, say (x_0, y_0), to (1), then it's easy to show that the solution is not unique. Our initial solution (called the 'particular solution') takes the form

$$18x_0 - 25y_0 = 1\,, \tag{2}$$

and we will use the Euclidean algorithm to get this. Into this we can add in and subtract out $18 \cdot 25k$ (for k an integer):

$$(18x_0 + 18 \cdot 25k) - (25y_0 + 18 \cdot 25k) = 1\,. \tag{3}$$

This becomes

$$18(x_0 + \cdot 25k) - 25(y_0 + 18k) = 1\,. \tag{4}$$

We can also think of these additional solutions as coming from the so-called **homogeneous equation** (where the unity on the RHS is replaced by zero.) with solutions: $(x_\mathrm{h}, y_\mathrm{h})$, so that

$$18x_\mathrm{h} - 25y_\mathrm{h} = 0\,, \tag{5}$$

[1] I got some help from both Wikipedia and Copilot.

bringing us to the general equation[2]

$$18(x_0 + x_\mathrm{h}) - 25(y_0 + y_\mathrm{h}) = 1\,, \tag{6}$$

with general solutions

$$x = x_0 + x_\mathrm{h}\,, \qquad y = y_0 + y_\mathrm{h}\,. \tag{7}$$

The Euclidean Algorithm will tell us what the greatest common divisor is of 18 and 25. Of course we already know it's 1, but we can run the algorithm in reverse to tell us how to find the particular solution (x_0, y_0). We will do this by stepwise eliminating the remainders of each step. Let's see how this works. But one more lemma to go.

Bézoit's lemma states that if two integers a, b have GCD $= d$, then there exists integers x, y that solves

$$ax + by = d\,. \tag{8}$$

But if GCD$(a, b) = 1$, then d in the above equation is unity, and thus there is a solution x, y that solves

$$ax + by = 1\,, \tag{9}$$

and this matches our given equation form in (1).

The point of this lemma is that we are guaranteed that a particular solution does exists.

3 The Solution

First, Euclid's algorithm produces the following equation 'stack':[3]

$$25 = 1 \cdot 18 + 7\,, \tag{10a}$$
$$18 = 2 \cdot 7 + 4\,, \tag{10b}$$
$$7 = 1 \cdot 4 + 3\,, \tag{10c}$$
$$4 = 1 \cdot 3 + 1\,, \tag{10d}$$
$$3 = 1 \cdot 3 + 0\,. \tag{10e}$$

So, what happened here? In the first line we divided the larger number 25 by the smaller number 18 and got the remainder 7. From then on, line after line until the remainder is zero, we divided the current divisor by the current remainder and got a new remainder.

Thus, we have shown by this algorithm that the GCD(25,18) is unity. Now, to find (x_0, y_0). So, look at Eq. (2) again. Where among the lines (10a)–(10e)

[2] By adding together Eqs. (2) and (5).

[3] Since I have to refer to it, I have to give it a name. (Recently, I've heard it called a 'tower'.) By the way, we're first going to go down the stack and then back up it.

do we find a '1' hanging out by itself (as a term, not as a factor)? That's right. Line (10d), where we will solve for the '1' and place it on the LHS and keep it there untouched for the rest of the procedure. Hence,

$$1 = 4 - 1 \cdot 3 \,. \tag{11}$$

Here's the procedure from this point on: Until we run out of previous lines, we will go to the next line up, find the remainder term, solve for it, and use it to substitute out that value in the current equation, which in this case is (11).

The line in the stack that corresponds to the current line, which is (10c). It's remainder is '3'. Solve for it:

$$3 = 7 - 1 \cdot 4 \,. \tag{12}$$

Use this value to substitute out the '3' in (11).

$$1 = 4 - (7 - 4) = 2 \cdot 4 - 7 \,. \tag{13}$$

Go up one more line in the stack, find its remainder term, which is '4. Solve for it.

$$4 = 18 - 2 \cdot 7 \,. \tag{14}$$

Use this value to substitute out the '4' in (13).

$$1 = 2 \cdot (18 - 2 \cdot 7) - 7 = 2 \cdot 18 - 5 \cdot 7 \,. \tag{15}$$

Go up to the next line in the stack, find the remainder term, which is '7', solve for it:

$$7 = 25 - 18 \,. \tag{16}$$

Use this value to substitute out the '7' in (15).

$$1 = 2 \cdot 18 - 5 \cdot (25 - 18) = 7 \cdot 18 - 5 \cdot 25 \,. \tag{17}$$

We can rewrite this as

$$7 \cdot 18 - 5 \cdot 25 = 1 \,. \tag{18}$$

On comparison with (2) we have that

$$x_0 = 7 \,, \qquad y_0 = 5 \,. \tag{19}$$

Lastly, the general solutions are

$$x = 7 + 25k \,, \qquad y = 5 + 18k \,. \tag{20}$$