Euclid’s algorithm

NA3_RT4

Here’s an interesting thought. If I tell you that $122381 = 3 \times 35889 + 14714$ and that 7 divides both 35889 and 14714, then we know immediately that 7 also divides 122381.

Why is that? Try to find your own explanation.

Here’s a picture that might be helpful.

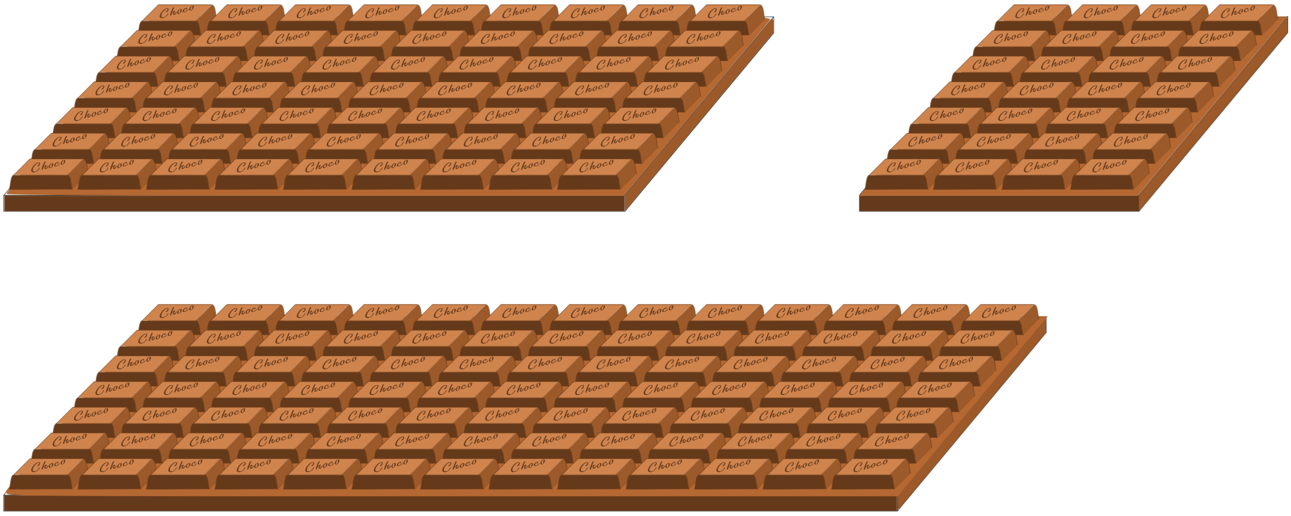

Figure NA3_RT4.1: Diagram

We can use this idea to understand *Euclid’s algorithm*.

To obtain the statement $122381 = 3 \times 35889 + 14714$, I divided 122381 by 35889 and looked for the *quotient* (in this case 3) and the *remainder* (in this case 14714). We can now repeat this for the numbers 35889 and 14714, and so on. Here’s the list of equations that we get.

$$\begin{aligned}
122381 &= 3 \times 35889 + 14714 \\
35889 &= 2 \times 14714 + 6461 \\
14714 &= 2 \times 6461 + 1792 \\
6461 &= 3 \times 1792 + 1085 \\
1792 &= 1 \times 1085 + 707 \\
1085 &= 1 \times 707 + 378 \\
707 &= 1 \times 378 + 329 \\
378 &= 1 \times 329 + 49 \\
329 &= 6 \times 49 + 35 \\
49 &= 1 \times 35 + 14 \\
35 &= 2 \times 14 + 7 \\
14 &= 2 \times 7
\end{aligned}$$

We stop there because the remainder in the final equation is 0.

Here's a handy tip. I've written numbers that do the same job in the same column. For example, the quotients are all just before the × sign, and the remainders are all at the end. There's a lot of flexibility about the order in which we write the components of these equations, but it's a lot easier to keep track of which numbers are doing which jobs if you keep them in the same place each time.

What can we deduce from these equations?

The last non-zero remainder is 7, so we'd like to show that the highest common factor of 122381 and 35889 is 7. (You might have been able to predict this if you'd made a suitable conjecture following your work on the introductory investigation at this station.)

To show that 7 is the highest common factor of these two numbers, we need to show two things:

- that 7 really is a common factor of them (it divides both numbers);
- and that it's the highest such number (any common factor of 122381 and 35889 is at most 7).

We'll show these things in order.

7 is a common factor of 122381 and 35889 Let's first start at the bottom and then work up.

The last equation, $14 = 2 \times 7$, tells us that 7 divides 14.

The next equation up, $35 = 2 \times 14 + 7$, then tells us that 7 divides 35 (because it divides both 14 and 7 on the right-hand side).

The next equation up, $49 = 1 \times 35 + 14$, then tells us that 7 divides 49 (because it divides both 35 and 14 on the right-hand side).

And so on, all the way up to the first equation, $122381 = 3 \times 35889 + 14714$, which tells us that 7 divides 122381 (because it divides both 35889 and 14714). In particular, 7 is a common factor of 122381 and 35889.

That's a good start.

You might reasonably think that it would be a lot easier just to check directly that 7 divides both numbers, but the advantage of what we've just done is that we can generalise it to *any* pair of starting numbers and still know that the last non-zero remainder divides both starting numbers.

Any common factor of 122381 and 35889 is at most 7 Now let's suppose that we have any old common factor of 122381 and 35889. Let's call it d. (It's much easier to talk about something if we've given it a name, and d is a good name for a divisor.)

Then the top equation, which we can rewrite as $14714 = 122381 - 3 \times 35889$, tells us that d divides 14714 (because it divides both 122381 and 35889).

The next equation down, which we can rewrite as $6461 = 35889 - 2 \times 14714$, tells us that d divides 6461 (because it divides both 35889 and 14714).

The next equation down, which we can rewrite as $1792 = 14714 - 2 \times 6461$, tells us that d divides 1792 (because it divides both 14714 and 6461).

And so on, all the way down to the penultimate (last but one) equation, which we can rewrite as $7 = 35 - 2 \times 14$. This tells us that d divides 7 (because, from the previous equations, it divides both 35 and 14).

So if d is any common factor of 122381 and 35889, then it divides 7, and also 7 is a common factor of 122381 and 35889. But that means precisely that 7 is the *highest common factor* of 122381 and 35889.

We do not have to write out all of that explanation every time we use Euclid's algorithm. But it's important that you're able to explain why the algorithm finds the highest common factor.

Pick your own pair of positive integers, and run Euclid's algorithm on them. Now explain to a friend why your equations have found the highest common factor for you.

Here are some follow-up questions to help you develop your understanding of Euclid's algorithm.

1. Find a pair of integers that have highest common factor 12 and where it takes exactly four steps of Euclid's algorithm to find that highest common factor.
   Can you still do this if you change the highest common factor and/or the number of steps?
2. Find a pair of four-digit numbers for which it takes very few steps for Euclid's algorithm to find their highest common factor.
3. Find a pair of four-digit numbers for which it takes many steps for Euclid's algorithm to find their highest common factor.

Relevance

NA3 What are highest common factors and why do they matter?