Euclidean Algorithm

The Euclidean Algorithm provides an efficient way of finding the gcd of two natural numbers. Suppose that a and b are both natural numbers. We seek to find the largest number that divides them both. We'll denote this as (a, b).

To start, suppose that $a > b$. Nothing can divide a number that is smaller, so the gcd cannot be larger than b. If it should happen that $b \mid a$, then $(a, b) = b$, and we are done. If this doesn't happen, which is the usual case, the we divide a by b, and get both a quotient and a remainder: $a = qb + r$.

Now the key observation: anything that divides both a and b must also divide r. Consequently $(a, b) = (b, r)$. This means that we can now work with smaller numbers, and eventually work down to very simple cases. Let's try a numerical example.

We want to find (437,26). To start we divide 437 by 26, giving a quotient of 16 with a remainder of 21. Therefore $437 = 16 \times 26 + 21$. Because the remainder wasn't 0 we continue with 26 and 21. Continuing as long as possible, we get this sequence of equations:

$$\begin{aligned} 437 &= 16 \times 26 + 21 \\ 26 &= 21 + 5 \\ 21 &= 4 \times 5 + 1 \\ 5 &= 5 \times 1 + 0 \end{aligned}$$

In short, (437,26)=1, so they share no divisors, a property known as being relatively prime.

We now have our algorithm, but we can get more out of it. In each equation we can rewrite the remainder in terms of the numbers being examined. Our example looks like this:

$$\begin{aligned} 1 &= 21 - 4 \times 5 \\ &= 21 - 4 \times [26 - 21] = 5 \times 21 - 4 \times 26 \\ &= 5 \times [437 - 16 \times 26] - 4 \times 26 = 4 \times 437 - 84 \times 26 \end{aligned}$$

In general, we have this important result:
For any a and b, there exist x and y for which $(a, b) = xa + yb$