Euclidean algorithm

There is a very important theorem (Proposition 7.1 on p. 126) that states that for any integers a, b, their greatest common divisor has a *linear representation*: there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

We will assume that $b > 0$. The proof in the book (which we also discussed in class) is *non-constructive*: we prove that x and y must exist without providing any recipe on how to find them.

A different, constructive, proof is given by the so-called **Euclidean algorithm**. Here's how this algorithm works.

First, remember the division algorithm: for any integers a, b (we are assuming $b > 0$), there exist integers q and r such that

$$a = bq + r \quad \text{and } 0 \leq r < b.$$

In this situation r is called the *remainder*.

The Euclidean algorithm works as follows: we divide a by b with remainder, and replace the pair (a, b) with the pair (b, r). Then repeat. This means, divide b by r with remainder (call it r_1), and replace the pair (b, r) with the pair (r, r_1). Repeat this until the remainder becomes zero. The last non-zero remainder equals the $\gcd(a, b)$! Moreover, working back from the set of equalities one gets from each division with remainder, one can get the integers x and y that we were after.

Here is an illustration.

Example. Let $a = 89$ and $b = 69$. Find the linear representation of $\gcd(a, b)$. We write the Euclidean algorithm on the left, and in the right column rewrite each equality in a way that is helpful for finding x and y. Write the Euclidean algorithm:

$89 = 69 + 20$ $\qquad$ $20 = 89 - 69.$

$69 = 20 \cdot 3 + 9$ $\qquad$ $9 = 69 - 20 \cdot 3 = 69 - (89 - 69) \cdot 3 = 69 \cdot 4 - 89 \cdot 3.$

$20 = 9 \cdot 2 + 2$ $\qquad$ $2 = 20 - 9 \cdot 2 = (89 - 69) - (69 \cdot 4 - 89 \cdot 3) \cdot 2 = 89 \cdot 7 - 69 \cdot 9.$

$9 = 2 \cdot 4 + 1.$ $\qquad$ $1 = 9 - 2 \cdot 4 = (69 \cdot 4 - 89 \cdot 3) - (89 \cdot 7 - 69 \cdot 9) \cdot 4 = 69 \cdot 40 - 89 \cdot 31.$

We find that $\gcd(89, 69) = 1$, and the last line is the representation of 1 as a combination of 89 and 69. We get that $x = 40$ and $y = 31$. I bet they would be hard to guess in this example!

Exercise. Prove that Euclidean algorithm indeed produces the $\gcd(a, b)$.

Hint: First, prove that the algorithm has to terminate (why can't this process go on forever?). Then prove that at every step of the algorithm, though the pair of numbers changes, their gcd does not.