Euclidean algorithm for calculating the gcd of two integers

We have proved that the gcd of integers m and n can be written as $mr + ns$ for some integers r and s.

How do we find r and s?

We may assume that m and n are non-negative and $m \leq n$.

<u>Key idea</u>:

$\gcd(m, n) = \gcd(m, n-m)$

(<u>Exercise</u>: Prove this.

Hint: Set $d_1 = \gcd(m,n)$, $d_2 = \gcd(m, n-m)$

Show that $d_1 \mid d_2$ and $d_2 \mid d_1$.)

As $m \leq n$, $n - m \geq 0$.

However, if $m > 0$, then $n - m < n$. So $\max(m,n) > \max(m, n-m)$.

So, we can simplify the problem by replacing the pair $\{m, n\}$ by a smaller pair $\{m, n-m\}$ as long as both m, n are positive.

If $m=0$, then $\gcd(m,n)=n$ and so we are done in this case.

Let us try to use this method.

Find gcd of 27 and 38.

$$\gcd(27, 38) = \gcd(27, 38-27)$$
$$= \gcd(27, 11) = \gcd(27-11, 11)$$
$$= \gcd(16, 11) = \gcd(16-11, 11)$$
$$= \gcd(5, 11) = \gcd(5, 11-5)$$
$$= \gcd(5, 6) = \gcd(5, 1)$$
$$= \gcd(4, 1) = \gcd(3, 1)$$
$$= \gcd(2, 1) = \gcd(1, 1) = \gcd(1, 0) = 1.$$

Given two numbers m, n with $m \leq n$, how many times can we subtract m from n till we get a number smaller than m? Write $n = mq + r$ where $0 \leq r < m$. Then, we can do this q times.

So, we can write our method more concisely as follows:

<u>Given</u>: Two non-negative integers $m \le n$.

<u>Step 1</u> If $m = 0$, $\gcd(m, n) = n$. So, we are <u>done</u>. If not, go to step 2.

Step 2 Use the division algorithm to write $n = mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$.
Replace the pair (m, n) by (r, m) and go to Step 1.

<u>Example</u> $(m,n) = (27, 38)$

$$\underline{38} = \underline{27} \cdot 1 + 11$$

$$\underline{27} = \underline{11} \cdot 2 + 5$$

$$\underline{11} = \underline{5} \cdot 2 + 1$$

$$\underline{5} = \underline{1} \cdot 5 + \underline{\underline{0}}$$

gcd.

So, given m, n, we perform the following steps:

$$n = mq_1 + r_1$$

$$m = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$\vdots$$

$$r_{n-1} = \underset{\substack{\uparrow \\ \gcd}}{r_n} \cdot q_{n+1} + 0$$

Now substitute backwards:

$$r_n = r_{n-2} - r_{n-1} q_n$$

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$$

$$r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$$

$$\vdots$$

$$r_2 = m - r_1 q_2$$

$$r_1 = n - m q_1$$

This will give an expression of the form $r_n = mx + ny$.

As we saw, $\gcd(m, n) = r_n$.

Example $(m, n) = (27, 38)$

$$38 = 27 \cdot 1 + 11$$
$$27 = 11 \cdot 2 + 5$$
$$11 = 5 \cdot 2 + 1$$
$$5 = 1 \cdot 5 + 0$$

gcd.

$$11 = 38 - 27 \cdot 1$$
$$5 = 27 - (38 - 27 \cdot 1) \cdot 2$$
$$= 27 \cdot 3 - 38 \cdot 2$$
$$1 = (38 - 27 \cdot 1) - (27 \cdot 3 - 38 \cdot 2) \cdot 2$$
$$= \boxed{38 \cdot 5 - 27 \cdot 7}$$