Extended Euclidean Algorithm

An algorithm that we often use in cryptography is the extended Euclidean algorithm. Here we will explain some special issues that let us to construct an efficient algorithm. If we have two integers a and b, and we need to calculate the greatest common divisor we will do the following procedure. For convenience let us consider that $r_0 = b$ and $r_1 = a$.

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ r_2 &= r_3 q_3 + r_4 \\ \ldots &= \ldots \\ r_{i-2} &= r_{i-1} q_{i-1} + r_i \end{aligned}$$

This means that in each iteration we calculate the remainder r_i and the quotient q_{i-1}. We must remember that our goal is not only to find the gcd, but also the linear combination i.e. $\gcd(r_0, r_1) = sr_0 + tr_1$. For this purpose, we express the remainder of each ith iteration as a linear combination of r_0 and r_1 i.e. $r_i = s_i r_0 + t_i r_1$.

Notice that to construct the linear combination of the ith iteration we need the previous linear combination, thus

$$r_{i-2} = s_{i-2} r_0 + t_{i-2} r_1 \tag{1}$$

$$r_{i-1} = s_{i-1} r_0 + t_{i-1} r_1 \tag{2}$$

Also notice that in the ith iteration we calculate the quotient q_{i-1} and the remainder r_i i.e. $r_{i-2} = r_{i-1} q_{i-1} + r_i$, if we rearrange this equation we have

$$r_i = r_{i-2} - r_{i-1} q_{i-1}. \tag{3}$$

Now we can use equations 1 and 2 and we use them in 3

$$r_i = s_{i-2} r_0 + t_{i-2} r_1 - (s_{i-1} r_0 + t_{i-1} r_1) q_{i-1}$$

Rearraging we have

$$r_i = (s_{i-2} - s_{i-1} q_{i-1}) r_0 + (t_{i-2} - t_{i-1} q_{i-1}) r_1$$

This give us a way to calculate s_i and t_i:

$$\begin{aligned} s_i &= s_{i-2} - s_{i-1} q_{i-1} \\ t_i &= t_{i-2} - t_{i-1} q_{i-1} \end{aligned}$$

These equations for s_i and t_i are valid for $i \geq 2$. It is not difficult to see that which are the values for s_0, s_1 and t_0, t_1. Actually $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$. Finally you must notice that to calculate the inverse, we do not require the value of s_i. All we need is to calculate t_i. Keeping all these facts we can write down a pseudocode to find the extended Euclidean algorithm.