

The extended Euclidean Algorithm

The purpose here is to relate the proof of the theorem on page 68 and the use of the in-built construction in implementing the extended Euclidean algorithm on page 69. It should also clarify why the starting values for the sequences $\{x_n\}$ and $\{y_n\}$ are as given.

The key step in the proof is to show that if r_j is a remainder obtained during the Euclidean algorithm process then there exists integers x^* and y^* such that $ax^* + by^* = r_j$. We expect x^* and y^* to depend on j but we will clear this up later.

The initial step of the algorithm gives $r_1 = a - q_1b$ and so we can set $x = 1$ and $y = -q_1$. The second step is $r_2 = b - q_2r_1 = (-q_2)a + (1 + q_1q_2)b$. In general, we have $r_j = r_{j-2} - q_jr_{j-1}$ and we see that if we have written r_i in terms of linear combinations of a and b for $i < j$ then we can do so also for $i = j$. In particular, we can do this for the final step with r_k .

Now back to the first step; we are going to write $x^* = x_2$ and $y^* = y_2$ here so we have the same result as on page 69. This gives $x_2 = 1$ and $y_2 = -q_1$. Now $r_2 = b - q_2r_1 = (-q_2)a + (1 + q_1q_2)b$ and the next step would set $x_3 = -q_2 = -q_2x_2$ and $y_3 = 1 + q_1q_2 = 1 - q_2y_2$. This suggests a slightly different indexing than used in the proof; we write $r_j = ax_{j+1} + by_{j+1}$. The general step gives

$$\begin{aligned} r_j &= r_{j-2} - q_jr_{j-1} \\ ax_{j+1} + by_{j+1} &= ax_{j-1} + by_{j-1} - q_j(ax_j + by_j) \end{aligned}$$

This gives that the sequences $\{x_n\}$ and $\{y_n\}$ must satisfy the recursion scheme

$$z_j = -q_{j-1}z_{j-1} + z_{j-2}$$

This is what the book obtains on page 68 with the indices of the q 's translated by 1, but exactly the scheme proposed on page 69.

How do we start these schemes? We need two starting values for each sequence, namely x_0 , x_1 and y_0 , y_1 . The key observation is that we need x_2 to satisfy $x_2 = 1$ regardless of the numbers a and b . But $x_2 = -q_1x_1 + x_0$ and the only way to do this is to select $x_0 = 1$ and $x_1 = 0$. Now $x_3 = -q_2x_2 + x_1 = -q_2$ and this is what we expected. For the y 's we need $y_2 = -q_1$ from $y_2 = -q_1y_1 + y_0$ for any value of q_1 . The only way to satisfy this is by taking $y_0 = 0$ and $y_1 = 1$.

Thus the Extended Euclidean algorithm becomes:

1. Compute the sequences r_j and q_j , for $j = 1, \dots, k$ where k is that index yielding $r_k = d = \gcd(a, b)$. This is the line in the table above where the remainder is zero.
2. Set $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$ where x_j , y_j satisfy the recursion relation $z_j = -q_{j-1}z_{j-1} + z_{j-2}$.
3. Then, $ax_{k+1} + by_{k+1} = r_k = d$; the indices are increased by 1 in x and y since we started these one in advance of the remainders r_j .

Note: This assumes the first step was $a = q_1b + r_1$, that is we assumed that $a > b$. The initial value of y , $y_0 = 0$ corresponds to the lower of the values b since y is coupled with b .