On Bézout's Lemma

R. C. Daileda

August 29, 2017

The goal of this note is to provide a constructive proof of the following well-known result.

Lemma 1 (Bézout). *Let $a, b \in \mathbb{Z}$. There exist $r, s \in \mathbb{Z}$ so that*

$$\gcd(a,b) = ra + sb.$$

Proof. We use the Euclidean algorithm to obtain

$$\begin{array}{ll}
b = q_1 a + r_1, & 0 < r_1 < |a|, \\
a = q_2 r_1 + r_2, & 0 < r_2 < r_1, \\
r_1 = q_3 r_2 + r_3, & 0 < r_3 < r_2, \\
\quad\vdots & \quad\vdots \\
r_{j-1} = q_{j+1} r_j + r_{j+1}, & 0 < r_{j+1} < r_j, \\
\quad\vdots & \quad\vdots \\
r_{N-2} = q_N r_{N-1} + r_N, & 0 < r_N < r_{N-1}, \\
r_{N-1} = q_{N+1} r_N & (\text{ i.e. } r_{N+1} = 0),
\end{array}$$

in which $r_N = \gcd(a,b)$.[1] For $0 \le j \le N$ define

$$\mathbf{x}_j = \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix},$$

where we set $r_{-1} = b$, $r_0 = a$. If we write the general relation $r_{j-1} = q_{j+1} r_j + r_{j+1}$ as

$$r_{j+1} = r_{j-1} - q_{j+1} r_j$$

we find that we have the recursive relationship

$$\mathbf{x}_{j+1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{pmatrix} \mathbf{x}_j, \ 0 \le j \le N-1.$$

Setting

$$A_j = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix}$$

for $1 \le j \le N$ we find that

$$\mathbf{x}_N = A_N \mathbf{x}_{N-1} = A_N A_{N-1} \mathbf{x}_{N-2} = \cdots = A_N A_{N-1} \cdots A_1 \mathbf{x}_0. \tag{1}$$

Write

$$A_N A_{N-1} \cdots A_1 = \begin{pmatrix} * & * \\ s & r \end{pmatrix}. \tag{2}$$

Since $r_{-1} = b$, $r_0 = a$ and $r_N = \gcd(a,b)$, (1) yields

$$\begin{pmatrix} * \\ \gcd(a,b) \end{pmatrix} = \begin{pmatrix} * & * \\ s & r \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} * \\ ra + sb \end{pmatrix},$$

which establishes what we wanted to prove.

$\square$

[1] We have assumed $a \nmid b$. In the case that $a | b$ we have $\gcd(a,b) = |a|$ and we can take $r = \pm 1$, $s = 0$ to prove the Lemma.

Remarks

- The constructive nature of the preceding proof of Bézout's Lemma lies in equation (2), expressing the coefficients r and s in terms of the quotients q_j occurring in the Euclidean algorithm. As these are provided by the division algorithm, which in turn has a constructive proof, we see that we have provided a means of computing r and s explicitly.

- The r and s whose existence is assured by Bézout's Lemma are not unique. Indeed, notice that

$$ra + sb = (r - kb)a + (s + ka)b$$

  for any $k \in \mathbb{Z}$.

- The proof we have given here is computationally efficient in that it requires a minimal amount of variable storage to be implemented by a machine. Indeed, by evaluating the product $A_N A_{N-1} \cdots A_1$ of equation (2) from right to left, one finds that it is only necessary to keep track of one stage of the Euclidian algorithm and the corresponding partial product of the A_j at a time.

- In the context of modular arithmetic the coefficients appearing in Bézout's Lemma (specifically r) are particularly important. For when $\gcd(a, b) = 1$ we see that $ra \equiv 1 \pmod{b}$, i.e. $r \equiv a^{-1} \pmod{b}$.