The Extended Euclidean Algorithm

If $d = \gcd(a, b)$, then there are integers s and t such that $sa + tb = d$.

Using $\gcd(123, 54) = 3$ as an example, we can look at the expansion of the Euclidean Algorithm as a sequence monotonically decreasing from 123, 54, etc. down to zero:

$$123, 54_2, 15_3, 9_1, 6_1, 3_2, 0$$

in that $a_n = a_{n-2} - a_{n-1}q_{n-1}$ where q_{n-1} is the subscript of a_{n-1}. Observe that (i) each later term can be expressed in terms of earlier terms, and recursively so; (ii) we cannot determine an earlier term before the first term (i.e. 123), since the subscript is undetermined and can be any positive integer.

Upon musing on the above sequence, here is a simple procedure to transform it into a sequence of tuples, where each tuple is a pair of numbers representing the multiples of (a, b) or (123, 54) in this example:

	$\mathbf{a} = 123$	$\mathbf{b} = 54_2$	15_3	9_1	6_1	$\mathbf{d} = 3$	
	$(1, 0)$	$(0, 1)$	$(1, \ \ 0)$	$(0, \ \ 1)$	$(1, -2)$	$(-3, \ \ 7)$	
+)			$-2(0, \ \ 1)$	$-3(1, -2)$	$-1(-3, \ \ 7)$	$-1(\ 4, -9)$	
	$(1, 0)$	$(0, 1)$	$(1, -2)$	$(-3, \ \ 7)$	$(4, -9)$	$(-7, 16)$	$= (\mathbf{s}, \mathbf{t})$

To verify, $-7(123) + 16(54) = 3$. In fact, for every intermediate value such as 15, 9, etc. at the top row, the tuples at the bottom row contain the respective number of a's and b's that sum to the corresponding intermediate value.

Acknowledgement

Special thanks to *A Primer of Abstract Mathematics* by Robert B. Ash, 1998, The Mathematical Association of America, for the inspiration.