Classical Algebra

Posted Problem Solution

Monday, September 24, 2007

There was a request in today's class to present a solution to the problem taken from the course text, p. 52, that follows. (I did not want to devote in-class time to it.)

Problem. *If* $(a,\ b)\ =\ 1$ *and* c *is an integer, then there is some integer* m *so that*

$$(a+bm,\ c)\ =\ 1 \quad .$$

Solution. Since $(a,\ b)\ =\ 1$, by "Bezout's Identity" every integer is an integer linear combination of a and b. In particular, there are integers r, s such that

$$c\ =\ ar+bs \quad .$$

The mechanism that is used to show that the greatest common divisor of two successive remainders in the Euclidean algorithm stays unchanged through the steps of the algorithm may be described as the principle that for any integers x, y, and q one has the identity

$$\text{(*)} \qquad (x,\ y)\ =\ (y,\ x-qy) \quad .$$

Then, using this principle, for any m, one has:

$$\begin{aligned}(c,\ a+bm)\ &=\ (ar+bs,\ a+bm)\\ &=\ (a+bm,\ (ar+bs)-r(a+bm)) \quad \text{by (*)}\\ &=\ (a+bm,\ b(s-m))\end{aligned}$$

Now choose m so that $s-m\ =\ 1$, i.e., take $m\ =\ s-1$. Then

$$\begin{aligned}(c,\ a+bm)\ &=\ (a+bm,\ b)\\ &=\ (b,\ (a+bm)-mb) \quad \text{by (*)}\\ &=\ (b,\ a)\\ &=\ 1\end{aligned}$$