The GCD motivational version

Wim Ruitenburg

For each pair of integers $k, m \in \mathbb{Z}$ we write (k, m) for the set of integers $\{kx + my \mid x, y \in \mathbb{Z}\}$. Similarly for sets $(k) = \{kx \mid x \in \mathbb{Z}\}$. Obviously $(k) = (k, k)$. Since x and y in the definition of (k, m) are allowed to be positive as well as negative, we also obviously have that $(k, m) = (-k, m) = (k, -m) = (-k, -m)$

We are given two positive integers $a, b \in \mathbb{N}^+$. There is a greatest common divisor $d = \gcd(a, b) \in \mathbb{N}^+$. We show below using a motivational proof that $(d) = (a, b)$, which is essentially equivalent to adding that there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.

Observe that $(k, m) \subseteq (n, p)$ is equivalent to that there are x, y such that $k = nx+py$ plus that there are z, w such that $m = nz + pw$. So $(k, m) = (n, p)$ means both ways. Since $(k) = (k, k)$ we have that $(k) = (n, p)$ exactly when $k \mid n$ plus $k \mid p$ plus there are $s, t \in \mathbb{Z}$ such that $k = ns + pt$. Replacing k by $-k$ is an inessential change, so we may suppose that $k > 0$. Let $e = \gcd(n, p)$. Then there are n' and p' such that $n = en'$ and $p = ep'$, and so $k = en's + ep't = e(n's + p't)$, so $e \mid k$. Since e is the *greatest* common divisor of n and p and k also divides both n and p, we must have $k \leq e$. Thus $k = e$. Wow, so $(k) = (n, p)$ with $k > 0$ implies that $k = \gcd(n, p)$. So if we show that there is some $k > 0$ with $(k) = (a, b)$, then we automatically have $k = d$ and $(d) = (a, b)$. So all we have to do is to show that some $k > 0$ exists for which $(k) = (a, b)$.

The following suffices. We are going to show by induction on $n+p$ that for all $n, p > 0$ there is a $k > 0$ such that $(k) = (n, p)$. The least case occurs for $n = p = 1$. In that case set $k = 1$, which gives $(1) = (1, 1)$.

Induction step: Suppose that $n, p > 0$ and for all $n', p' > 0$ with $n' + p' < n + p$ there are $k' > 0$ such that $(k') = (n', p')$. WLOG we may suppose that $0 < n \leq p$. By the 'Division Algorithm' there are q, r with $0 \leq r < n$ such that $p = nq + r$. We leave it as an easy exercise (do!) to show that $(n, p) = (n, r)$. If $r = 0$, then $(n, p) = (n)$ and we are done. Otherwise, since $r < n \leq p$ we have $n + r < n + p$. By the induction step supposition there is $k > 0$ such that $(n, r) = (k)$, so also $(n, p) = (k)$. Apply induction: For all $n, p > 0$ there is $k > 0$ such that $(n, p) = (k)$. In particular there is $k > 0$ such that $(k) = (a, b)$.