**Proof** Let

$$S = \left\{a - xb \,:\, x \in \mathbb{N},\, a - xb \in \overline{\mathbb{N}}\right\}.$$

Since $a > b$, $a - b \in S$ and hence $S$ is non-empty: $S \neq \emptyset$.

Since $S \subset \overline{\mathbb{N}}$, it follows from the Well-Ordering Principle that $S$ has a least element $r \in \overline{\mathbb{N}}$. Let $q \in \mathbb{N}$ be the corresponding value of $x$:

$$r = a - qb.$$

If $r \geq b$, then $r - b \in \overline{\mathbb{N}}$ and

$$r - b = (a - qb) - b = a - (q + 1)\,b,$$

giving that $r - b \in S$.

This contradicts the assumption that $r$ is the least element of $S$. So $r < b$.

Clearly, we have that $a = qb + r$.

Suppose that $q' \in \mathbb{N}$ and $r' \in \overline{\mathbb{N}}$ satisfy $r' < b$ and $a = q'b + r'$. Hence $qb + r = q'b + r'$.

If $q = q'$, then $r = r'$.

Suppose that $q \neq q'$. Without loss of generality, suppose that $q > q'$. We have that

$$(q - q')\,b = r' - r.$$

Furthermore,

$$q - q' \geq 1 \quad \Rightarrow \quad (q - q')\,b \geq b,$$

and

$$r' - r \leq r' < b,$$

yielding a contradiction. □

**Theorem 10.6.** *Pick $a$, $b \in \mathbb{N}$. Then*

(i) *$d = (a,\, b)$ exists;*

(ii) *$d$ is unique;*

(iii) *$d = ax + by$ for some $x$, $y \in \mathbb{Z}$.*

**Proof** (i) [Euclid, 300 BC] Suppose, without loss of generality, that $a > b$. Note that $(b,\, b) = b)$.

Successively applying Lemma 10.5 gives that there exist $q_1, q_2, q_3, \ldots, q_{i+2} \ldots \in \mathbb{N}$ and $r_1, r_2, r_3, \ldots, r_{i+1}, r_{i+2} \ldots \in \overline{\mathbb{N}}$ such that

$$\begin{aligned}
a &= q_1 b + r_1, & 0 &\leq r_1 < b;\\
b &= q_2 r_1 + r_2, & 0 &\leq r_2 < r_1;\\
r_1 &= q_3 r_2 + r_3, & 0 &\leq r_3 < r_2;\\
&\vdots & &\vdots\\
r_i &= q_{i+2} r_{i+1} + r_{i+2}, & 0 &\leq r_{i+2} < r_{i+1}.
\end{aligned}$$