

Hence $a > b > r_1 > r_2 > r_3 > \dots > r_{i+1} > r_{i+2} > \dots \geq 0$.

It follows that $\exists n \in \mathbb{N}$ such that

$$\begin{aligned} r_{n-1} &= q_{n+1}r_n + r_{n+1}, & 0 \leq r_{n+1} < r_n, \\ r_n &= q_{n+2}r_{n+1}, \end{aligned}$$

with $r_{n+1} \neq 0$. Take $d = r_{n+1}$. Clearly, $d \in \mathbb{N}$.

Also, $r_n = q_{n+2}d$ and hence $d \mid r_n$.

Furthermore

$$r_{n-1} = q_{n+1}r_n + r_{n+1} = q_{n+1}q_{n+2}d + d = (q_{n+1}q_{n+2} + 1)d,$$

giving that $d \mid r_{n-1}$.

Similarly, $d \mid r_{n-2}, d \mid r_{n-3}, \dots, d \mid r_1, d \mid b, d \mid a$.

So d satisfies (D1) in Definition 10.4.

Suppose now that $e \mid a$ and $e \mid b$. Then, by Lemma 10.3,

$$\begin{aligned} r_1 &= a - q_1b && \Rightarrow e \mid r_1; \\ r_2 &= b - q_2r_1 && \Rightarrow e \mid r_2; \\ r_3 &= r_1 - q_3r_2 && \Rightarrow e \mid r_3; \\ &\vdots && \vdots \\ r_n &= r_{n-2} - q_n r_{n-1} && \Rightarrow e \mid r_n; \\ r_{n+1} &= r_{n-1} - q_{n+1}r_n && \Rightarrow e \mid r_{n+1}. \end{aligned}$$

But $r_{n+1} = d$, giving that $e \mid d$. So d satisfies (D2) in Definition 10.4.

(ii) Suppose that $d, d' \in \mathbb{N}$ satisfy (D1) and (D2) in Definition 10.4.

Then $d \mid d'$ and $d' \mid d$. It follows from Remark 10.2 that $d \leq d'$ and $d' \leq d$. Hence $d = d'$.

(iii) From (i),

$$\begin{aligned} r_1 &= a - bq_1, \\ r_2 &= b - q_2r_1 = b - q_2(a - bq_1) = -aq_2 + b(1 + q_1q_2). \end{aligned}$$

We now argue by induction. We prove that for any $i \geq 2$, if there exist integers $x_{i-1}, y_{i-1}, x_i, y_i \in \mathbb{Z}$ such that

$$\begin{aligned} r_{i-1} &= ax_{i-1} + by_{i-1}, \\ r_i &= ax_i + by_i; \end{aligned}$$