then there exist integers $x_{i+1}, y_{i+1} \in \mathbb{Z}$ such that

$$r_{i+1} = ax_{i+1} + by_{i+1}.$$

Indeed,

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1}r_i = (ax_{i-1} + by_{i-1}) - q_{i+1}(ax_i + by_i) \\ &= a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i). \end{aligned}$$

Noting that $d = r_{n+1}$ gives the required result.

□

Example 10.7. Take $a = 1225$, $b = 1155$. We have that

$$\begin{array}{rl|rl} & 1225 = 1 \cdot 1155 + 70, & 70 &= 1225 - 1155 \\ & 1155 = 16 \cdot 70 + 35, & 35 &= 1155 - 16 \cdot 70 \\ & 70 = 3 \cdot 35 & &= 1155 - 16(1225 - 1155) \\ \Rightarrow & d = 35 & &= 17 \cdot 1155 - 16 \cdot 1225. \end{array}$$

Remark 10.8. There are infinitely many pairs $(x, y) \in \mathbb{Z}^2$ satisfying (iii). Indeed, suppose that $x, y \in \mathbb{Z}$ satisfy $d = ax + by$. Pick $m \in \mathbb{Z}$ and take

$$x' = x - mb, \quad y' = y + ma.$$

Then

$$ax' + by' = a(x - mb) + b(y + ma) = ax + by = d.$$

Remarks 10.9. The definition of greatest common divisor can be extended to $a, b \in \mathbb{Z} \setminus \{0\}$:

(1) The Euclidean Algorithm can be applied to find $(|a|, |b|)$

(2) Then the greatest common dividers of a and b are $\pm(|a|, |b|)$.

Corollary 10.10. *Let $a, b, k \in \mathbb{N}$. Then*

$$(ka, kb) = k(a, b).$$

Proof Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, $kd \mid ka$ and $kd \mid kb$.

Let $d' = (ka, kb)$. Then, since $kd \mid ka$ and $kd \mid kb$, so $kd \mid d'$.

On the other hand, $d' \mid ka$ and $d' \mid kb$. So $d' \mid kd$. Hence $kd \mid d'$ and $d' \mid kd$, giving that $d' = kd$. □