The Euclidean Algorithm

Given: $m, n \in \mathbb{Z}, n \neq 0$.

Procedure: use the division algorithm to obtain:

$$
\begin{array}{lll}
(1) & m = q_1 \cdot n + r_1, & 0 < r_1 < |n|, \\
(2) & n = q_2 \cdot r_1 + r_2, & 0 < r_2 < r_1, \\
(3) & r_1 = q_3 \cdot r_2 + r_3, & 0 < r_3 < r_2, \\
\vdots & \vdots & \vdots \\
(k-1) & r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-1}, & 0 < r_{k-1} < r_{k-2}, \\
(k) & r_{k-2} = q_k \cdot r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\
(k+1) & r_{k-1} = q_{k+1} \cdot r_k. &
\end{array}
$$

We then have:

(1) $|n| > r_1 > r_2 > \ldots > r_{k-1} > r_k > 0$.

(2) $\gcd(r_{i-2}, r_{i-1}) = \gcd(r_{i-1}, r_i)$, for $i = 1, \ldots, k$

$\Rightarrow \gcd(m, n) = r_k$. [Here: $r_{-1} = m, r_0 = n$.]

(3) For all $\ell, 0 \leq \ell \leq k-1$,there exist $x_\ell, y_\ell \in \mathbb{Z}$ s. th.

$$r_{\ell-1} x_\ell + r_\ell y_\ell = r_k.$$

(4) There exist $x, y \in \mathbb{Z}$ such that $mx + ny = r_k$.