1.38 Theorem. Let $a, b \in \mathbb{Z}$. If $(a, b) = 1$, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof. Let $a, b \in \mathbb{Z}$ be given such that $(a, b) = 1$. Let $P(n)$ for all $n \in \mathbb{N}$ be the number of steps of The Euclidian Algorithm (TEA) where $a = bq_n + r_n$, for $q, r \in \mathbb{Z}$, up to the n^{th} iteration until $r_n = 1$ such that $ax + by = 1$. Consider the base case $n = 1$.

$$\begin{aligned} a &= bq_1 + r_1, \\ a &= bq_1 + 1. \end{aligned}$$

Rearranging, we find $a - bq_1 = 1$, which leads to $1a + (-q_1)b = 1$. Thus, there exist coefficient integers such that $ax + by = 1$.

Since the base case is true, we will prove by induction. Suppose now, $P(k)$ is true for some $k \in \mathbb{Z}$. We want to show there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$, provided $(a, b) = 1$ and TEA requires $k + 1$ steps to find a remainder $r_{k+1} = 1$. Applying the division algorithm, $a = bq_1 + r_1$, and $1 = (a, b) = (b, r_1)$ with b and r_1 being the numbers such that TEA requires k steps. Thus, there exists $u, v \in \mathbb{Z}$ such that $bu + r_1 v = 1$ by the inductive hypothesis. Notice $r_1 = a - bq_i$. Substituting,

$$\begin{aligned} 1 &= bu + v(a - bq_i) \\ &= bu + av - bvq_i \\ &= av + b(u - vq_i). \end{aligned}$$

Letting $x = v$ and $y = u - vq_i$, we find that our induction step satisfies the existence of $x, y \in \mathbb{Z}$ such that $ax + by = 1$. $\square$