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

Proof. Let $a, b \in \mathbb{Z}$ be given. Let $x, y \in \mathbb{Z}$ such that $ax + by = 1$. We want to show $(a, b) = 1$. Let $d = (a, b)$. It follows that $d \mid a$ and $d \mid b$. Observing $ax + by = 1$, since $d \mid a$, d divides any multiple of a. Similarly, since $d \mid b$, d divides any multiple of b. Both terms are divisible by d, therefore, the sum is divisible my d. Thus, $d \mid 1$.

Clearly, the only two numbers that divide 1, are -1 and 1. Since $d \geq 1$, we could assume $d = 1$. But suppose not. That is, given $d|1$, suppose $d > 1$. By definition, $1 = dt$ for $t \in \mathbb{Z}$. Since $d > 1$, it follows that $1 \leq t < dt$. Thus, $1 < dt$. This contradicts the definition of $d|1$. Thus, $d = 1 = (a, b)$. $\square$