HW1

0.3 12

Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime then there is an interger b such that $ab \equiv 0 \,(mod\;\; n)$ and deduce that there cannot be an integer c such that $ac \equiv 1 \,(mod\;\; n)$

0.3 13

Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are relatively prime then there is an interger c such that $ac \equiv 1 \,(mod\;\; n)$ (use the fact that g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers)

Proof. By Euclidean algorithm, $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + ny = (a, n) = 1$, so $1 - ax = yn$, hence $ax \equiv 1 \,(mod\;\; n)$ $\square$