Homework 3

MATH 301

Solution to graded problem

Exercise 4. Let $n \in \mathbb{N}$ with $n > 1$, and let $a \in \mathbb{Z}$.

(a) Prove that if $\gcd(a, n) = 1$ and $b, c \in \mathbb{Z}$ such that $ab = ac \pmod{n}$, then $b = c \pmod{n}$.

(b) Give an example of integers n, a, b, c such that $ab = ac \pmod{n}$ but $b \neq c \pmod{n}$.

Solution. (a) We proved in class that if a and n are relatively, then there exists $x \in \mathbb{Z}$ such that $ax = 1 \pmod{n}$. Therefore, if $ab = ac \pmod{n}$, then $axb = axc \pmod{n}$, and hence, as $axb = b \pmod{n}$ and $axc = c \pmod{n}$, we have that $b = c \pmod{n}$.

(b) Let $n = 6$, $a = 2$, $b = 1$, and $c = 4$, then $1 \neq 4 \pmod{6}$ but $2 = 2(1) = 2(4) \pmod{n}$. □