

MTH 309

Additional Problems for Section 4.3

1. Recall the following theorem discussed in class:

Theorem 1 *Let $a \in \mathbb{Z}_m$. Then a has a multiplicative inverse mod m if and only if $\gcd(a, m) = 1$.*

- (a) Use the theorem to find the elements of \mathbb{Z}_{12} that have a multiplicative inverse mod 12. Determine the multiplicative inverse for each of these elements.
 - (b) Use the theorem to find the elements of \mathbb{Z}_{15} that have a multiplicative inverse mod 15. Determine the multiplicative inverse for each of these elements.
2. Prove the following theorem

Theorem 2 *Let $a, b \in \mathbb{Z}^+$. If $d|a$ and $d|b$ then $d|\gcd(a, b)$*

3. Let m and n be relatively prime and let $a, b \in \mathbb{Z}$. Prove
 - (a) If $m | a$ and $n | a$ then $mn | a$
 - (b) If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ then $a \equiv b \pmod{mn}$
 - (c) Show that (a) and (b) are false without the assumption that m and n are relatively prime.