Homework 3

1a) Let a, b, c be integers such that

$$a \mid c, \quad b \mid c \quad \text{and} \quad \gcd(a,b) = 1,$$

show that $ab \mid c$.

b) Show that $\gcd(a,b) = 1$ is necessary.

Find a, b, c such that $a \mid c$ and $b \mid c$

but $ab \nmid c$.

c) Let $\text{ord}(g)$ denote the order of g in a group. Complete the tables:

In $(\mathbb{Z}_2, +)$

a	$\text{ord}(a)$
0	
1	

In $(\mathbb{Z}_3, +)$

b	$\text{ord}(b)$
0	
1	
2	

In $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$

(a,b)	$\text{ord}(a,b)$
$(0,0)$	
$(0,1)$	
$(0,2)$	
$(1,0)$	
$(1,1)$	
$(1,2)$	

Observe that $\text{ord}((a,b)) = \text{ord}(a)\,\text{ord}(b)$

Prove that this is true for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$ where m and n are coprime.

2. Prove the Extended Euclidean algorithm:

For all integers a, b, there exists integers u, v such that

$$au + bv = \gcd(a, b)$$

3. a) Given integers a, b. Show that if there exists integers u, v such that

$au + bv = 1$

then $\gcd(a, b) = 1$

b) If there exists integers u, v such that

$au + bv = 6$, is it always true that $\gcd(a, b) = 6$?

If no, provide a counterexample.

4. Find a value x that simultaneously solves the congruences or show that no such value x can exist.

a) $x \equiv 3 \mod 7$

$x \equiv 4 \mod 9$

b) $x \equiv 13 \mod 71$

$x \equiv 41 \mod 97$

c) $x \equiv 7 \mod 9$

$x \equiv 3 \mod 6$