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 $ab \nmid c$.

b)

$a = 6$

$b = 8$

$c = 24$

$\gcd(a, b) = 2$

$ab = 48 \nmid 24 = c$

a)

Let $a = \prod p_i^{a_i}$

$b = \prod q_i^{a_i}$ $\quad p_i, q_i$ are primes

Since $\gcd(a, b) = 1$, $p_i \neq q_j \;\; \forall i, j$

Since $a \mid c$ and $b \mid c$,

$\prod p_i^{a_i}$ and $\prod q_i^{a_i}$ are in the prime factorization of c.

Hence $ab \mid c$.

if $a|c$, $b|c$ and $ab|c$

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

No. Counterexample.

$a = 3$

$c = 18$

$b = 6$

$\gcd(a,b) = 3 \neq 1$

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

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

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

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

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

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

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

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

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

---

c) Let ord(g) denote the order of g in a group.
Complete the tables:

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

a	ord(a)
0	1
1	2

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

b	ord(b)
0	1
1	3
2	3

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

(a,b)	ord(a,b)
$(0,0)$	
$(0,1)$	3
$(0,2)$	3
$(1,0)$	2
$(1,1)$	6
$(1,2)$	6

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

Prove that this is true for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$

where m and n are coprime.

$$\boxed{\mathrm{ord}((a,b)) = \frac{\mathrm{ord}(a)\,\mathrm{ord}(b)}{\gcd(a,b)}}$$

Let $d = \operatorname{ord}((a, b))$.

$d \cdot (a, b) = (0, 0)$

$d \cdot a = 0$ and $d \cdot b = 0$

Hence, $\operatorname{ord}(a) \mid d$

$\operatorname{ord}(b) \mid d$

If $\gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$,

then $\operatorname{ord}(a) . \operatorname{ord}(b) \mid d$

Let $e = \operatorname{ord}(a) \operatorname{ord}(b)$

$e . (a, b) = (ea, eb) = (0, 0)$

Hence, $d \mid e$

Since $e \mid d$ and $d \mid e$, $d = e$

$\gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$

because $\gcd(m, n) = 1$ and $\operatorname{ord}(a) \mid m$ and $\operatorname{ord}(b) \mid n$

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.

b) $a\ u + b\ v = 6$

$7 \cdot 1 + 1 \cdot (-1) = 6$

$\gcd(a, b) = \gcd(7, 1) = \underline{1}$

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) $x \equiv 7 \mod 9$

$x \equiv 3 \mod 6$

a) $x \equiv 3 \bmod 7$
$x \equiv 4 \bmod 9$ } $x = 31$

b) $x \equiv 13 \bmod 71$
$x \equiv 41 \bmod 97$ } $x = 5764$

c) $x \equiv 7 \bmod 9$
$x \equiv 3 \bmod 6$

Use Exteded Euclidean Algorithm to find n_1, n_2

$m_1 n_1 + m_2 n_2 = 1$.

Then $x = x_1 m_2 n_2 + x_2 m_1 n_1$

c) $x \equiv 7 \mod 9$

$x \equiv 3 \mod 6$

$\left.\begin{matrix} \\ \\ \end{matrix}\right\}$ If $\gcd(9,6) = 3$ then no. solution ?! NO

Proof:

If x exists, then $\exists\, q, q' \in \mathbb{Z}$

$$x = 9q + 7$$
$$x = 6q' + 3$$

$$0 = 3(3q - 2q') + 4$$

$$4 = (2q' - 3q)3$$

$3 \mid (2q' - 3q)3$ but $3 \nmid 4$

So, there can't be solution