- **Problem 1**

(a)

$$\begin{aligned}30030 &= 257\ (116) + 218\\ 257 &= 218\ (1) \quad + 39\\ 218 &= 39 \quad (5) \quad + 23\\ 39 &= 23 \quad (1) \quad + 16\\ 23 &= 16 \quad (1) \quad + 7\\ 16 &= 7 \quad (2) \quad + 2\\ 7 &= 2 \quad (3) \quad + 1\end{aligned}$$

Which leads us to the fact that $gcd(30030, 257) = 1$. by assumption we have the unique prime factorization of $30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$. By definition of gcd we know that any of $A = \{2, 3, 5, 7, 11, 13\}$ is not a prime factor for 257. and on ther other hand we have the fact that $\sqrt{257} \approx 16$ and non of primes up to 16 that are elements of set A divide 257 so there could not be any prime factor for 257 which yields that 257 is prime ■

(b)

$$\begin{aligned}4883 &= 4369\ (1) + 514\\ 4369 &= 514 \quad (8) + 257\\ 514 &= 257 \quad (2) + 0\end{aligned}$$

By part a we know that 257 is prime and thus we factor numbers as follows. $\frac{4883}{257} = 19$, and because 19 is prime, for the factorization we have: $4883 = 257 \times 19$. With the same argue for 4369 we have the factorization, $4369 = 257 \times 17$.

- **Problem 2**

(a) We know that every linear combination of a and b in the form $ax + by$ for $x, y \in \mathbb{Z}$ is a multiple of their greatest common divisor $gcd(a, b)$, by knowing this fact and that there is a linear combination of a, b such that $ax + by = 1$ it is trivial that $gcd(a, b) = 1$ ■

(b) Assume that a is invertible mod b then the equation $ax \overset{b}{\equiv} 1$ has a solution for x, which by definition of modular equation leads us to the equation $ax = by + 1$ for some value of b, which means that $ax + by = 1$ for some values of x and y which means that $gcd(a, b) = 1$.
Conversely assume that $gcd(a, b) = 1$ which means that $ax + by = 1$ for some value of x and y now consider this equation modular b which gives us $\overline{ax} + \cancel{by} \overset{b}{\equiv} \overline{1}$ which means a is invertible modular b ■

(c)

$$\begin{aligned}101 &= 17\ (5) + 16 \qquad &\text{(I)}\\ 17 &= 16\ (1) + 1 \qquad &\text{(II)}\end{aligned}$$

By the equation (II) we can write 16 as follows $16 = 17 - 1$ by putting this into the equation (I) we have the equation $101 = 17(5) + (17 - 1)$ which leads us to $101 = 17(6) - 1$, Thus $1 = 17(6) - 101(1)$. Hence $17^{-1} mod(101) = 6$ ■

- **Problem 3**

(a)

$$\begin{cases} x \overset{4}{\equiv} 1 \\ x \overset{6}{\equiv} 2 \end{cases} \longrightarrow gcd(4,6) = 2$$

Assume for the sake of contradiction that there is a solution for this system. Means that there is a x such that.

$$\begin{cases} x \overset{4}{\equiv} 1 \Rightarrow x = 4k + 1 \ (k \in \mathbb{Z}) \\ x \overset{6}{\equiv} 2 \Rightarrow x = 6l + 2 \ (l \in \mathbb{Z}) \end{cases} \Rightarrow 4k + 1 = 6l + 2 \Rightarrow 4k = 6l + 1$$

But in the last equation the Left-Hand-Side is always <u>even</u> and the Right-Hand-Side is always <u>odd</u> which contradicts. Thus there is no such a solution for the system this completes the proof of our counterexampler ■

(b)

$$\begin{cases} x \overset{17}{\equiv} 2 \\ x \overset{101}{\equiv} 9 \end{cases}$$

By the first equation we have $x = 17k + 2$, then by putting this together with the second equation we have that $17k + 2 \overset{101}{\equiv} 9$ which leads us to $17k \overset{101}{\equiv} 7$. Since we have already calculated the inverse of 17 modulo 101 we can now evaluate the value of k modular 101.

$$6 \times 17k \overset{101}{\equiv} 6 \times 7 \Rightarrow k \overset{101}{\equiv} 42 \Rightarrow k = 101u + 42$$

Now by putting this together with the last equation we hae $x = 17(101u + 42) + 2$. Thus $x = 1717u + 716$ ■

- **Problem 4**

(a) Assume for the sake of contradiction that there are two identity elements e and $\acute{e}$, we get the contradiction by just applying the definition of identity element on each:

$$m(e, \acute{e}) = \begin{cases} e & \acute{e} \text{ is identity} \\ \acute{e} & e \text{ is identity} \end{cases} \Longrightarrow e = \acute{e}$$

Which contradict so the identity element must be unique ■

Assume for the sake of contradiction that arbitrary element x of our group has two inverses x_1^{-1} and x_2^{-1}.

$$\begin{cases} m(x, x_1^{-1}) = e \\ m(x, x_2^{-1}) = e \end{cases} \xrightarrow[\text{identity element}]{\text{uniqueness of}} m(x, x_1^{-1}) = m(x, x_2^{-1}) \Rightarrow x_1^{-1} = x_2^{-1} = x^{-1}$$

(b) We need to show (I)-Injectivity and (II)-Surjectivity

(I) Assume that $hg = \acute{h}g$ by multiplying g^{-1} to the both sides of equation we have $h = \acute{h}$.

(II) Take arbitrary element $h \in G$ we claim that $g^{-1}h$ is the element that maps under the function $m_g(h)$ to the element h. To prove the claim we have $m_g(g^{-1}h) = gg^{-1}h = h$ as desired.

So function is both injective and surjective together means that the function is Bijection ■

(c) (I) Closed under operator: This is easy to see that $ax+bz, \cdots, cy+dt$ are real numbers since $a, b, c, d, x, y, z, t \in \mathbb{R}$

$$A \times B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x & y \\ z & t \end{pmatrix} \Rightarrow \begin{cases} A \in GL_2(\mathbb{R}) \\ B \in GL_2(\mathbb{R}) \end{cases} \Rightarrow A \times B \in GL_2(\mathbb{R})$$

(II) Existence of Inverse: This follows immediately from the fact the determinant is non-zero and basic Linear-Algebra. Identity element is just identity matrix I_2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

(III) $(A \times B) \times C = A \times (B \times C)$: This is easy to verify by Linear-Algebra. Just write it down it is straightforward.

This is not a cummutative group. Counterexample is as follows:

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix}$$

(d) (I) Closed under operator: $\overline{a} \times \overline{b} = \overline{a \times b}$, Thus it is closed.

(II) Identity element is : $\overline{1}$ and inverse for every element exists since p is considered to be prime: $gcd(p, a)$ is either p which means p divide a, This is not the case because every element of our group is to be considered lower than p, or $gcd(p, a) = 1$ which by bezout's coefficients we know that there is an inverse for a modulo p.

(III) $\overline{a} \times \left(\overline{b} \times \overline{c}\right) = \left(\overline{a} \times \overline{b}\right) \times \overline{c}$: which is trivially true by the definition.

Under addition is similar.

(e) No it is not closed under operator: $\overline{3} \times \overline{5} = \overline{0}$
The largest prime number before 15 is 13 so $\frac{\mathbb{Z}}{13\mathbb{Z}} \equiv \mathbb{F}_{13}$ is the maximal subset of $\frac{\mathbb{Z}}{15\mathbb{Z}}$ which is a group under multiplication.

(f) We know that φ is a multiplicative function. Let's evaluate the φ for prime values:

$$\varphi(p) = \#\{1, \cdots, p-1\} = p-1$$
$$\varphi(p^\alpha) = \#\{1, \cdots, p-1, p+1, \cdots, p^2-1, p^2+1, \cdots, p^\alpha - 1\} = p^{\alpha-1}(p-1)$$

Now let's evaluate the φ for arbitrary N with the factorization $N = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$.

$$\varphi(N) = \left[\varphi(p_1^{\alpha_1})\right] \cdots \left[\varphi(p_s^{\alpha_s})\right] = \left[p_1^{\alpha_1-1}(p_1-1)\right] \cdots \left[p_s^{\alpha_s-1}(p_s-1)\right]$$

$$\xrightarrow{\text{Closed form}} \prod_{\substack{p_i \mid N \\ p_i \text{ prime}}} p_i^{\alpha_i-1}(p_i-1) = \prod_{\substack{p_i \mid N \\ p_i \text{ prime}}} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)$$

By multiplying $p_i^{\alpha_i}$ we get the formula as desired.

$$\varphi(N) = N \prod_{\substack{p_i \mid N \\ p_i \text{ prime}}} \left(1-\frac{1}{p_i}\right)$$

- **Problem 5**

(a) By definition of φ we know that $\varphi(N)$ is the number of number less than N and relatively prime to N. Assume that order of element a is d by Lagrange's Theorem this d should divivde $\varphi(N)$ so $d \times k = \varphi(N)$, Hence $a^{\varphi(N)} \overset{N}{\equiv} a^{d.k} \overset{N}{\equiv} 1$

(b)

$$30 = 7(4) + 2 \Rightarrow \qquad 2 = 30 + 7(-4)$$
$$7 = 2(3) + 1 \Rightarrow \qquad 1 = 7 + 2(-3)$$

$$1 = 7 + [30 + 7(-4)](-3) = 30(-3) + 7(13)$$

Hence inverse of 7 modulo 30 is 13, i.e $7 \times 13 \overset{30}{\equiv} 1$

$$m^7 \overset{31}{\equiv} x \Rightarrow \left(m^7\right)^e \overset{31}{\equiv} x^e \Rightarrow 7 \times e \overset{\varphi(31)}{\equiv} 1 \Rightarrow 7 \times e \overset{30}{\equiv} 1 \Rightarrow e = 13$$

$$\left(m^7\right)^{13} \overset{31}{\equiv} m \overset{31}{\equiv} x^{13}$$

- **Problem 6**

(a) Assume that $g \in G$ with $\phi(g) = h \in H$ then by definition of identity element we know that $g = 1_G *_G g$ Hence $\phi(g) = \phi(1_G *_G g) = \phi(1_G) *_H h = h$ the last equation establish that $\phi(1_G) = 1_H$ ■

(b)

$$1_G = g *_G g^{-1} \xrightarrow{\phi} \phi(1_G) = 1_H = \phi(g) *_H \phi(g^{-1}) \Rightarrow \phi(g^{-1}) = \phi(g)^{-1}$$

(c) Obviously $\phi(G) \subseteq H$ only thing we need to show is that $\phi(G)$ is group under the operation of group H. Just for easier writing assume that operator for G and H are $*$, $\#$, respectively

(I) Closed under Operator
Assume for the sake of contradiction that this is not the case, i.e. $h_1, h_2 \in \phi(G)$and $g_1, g_2 \in G$ are related elements, but $h_1 \# h_2 \notin \phi(G)$: Because G is group $g_1 * g_2 \in G$ and Hence $\phi(g_1 * g_2) = h_1 \# h_2$ should be in $\phi(G)$ by definition of ϕ which contradicts.

(II) Associativity :
Is true in H so it is true in $\phi(G) \subseteq H$.

(III) Identity Element : By part (a)

(IV) Inverse Element : By part (b)

(d) **(I) Closed under Operator :**
Assume $a, b \in \ker(\phi)$ then $\phi(a * b) = \phi(a) \# \phi(b) = 1_H \# 1_H = 1_H$. Thus $a * b \in \ker(\phi)$.

(II) Associativity : Quite Obvious.

(III) Inverse Element :
If $a \in \ker(\phi)$ then it's inverse is $\phi(a^{-1}) = \phi(a)^{-1} = {1_H}^{-1} = 1_H$ which means $a^{-1} \in \ker(\phi)$

(IV) Identity Element : By definition $1_G \in \ker(\phi)$

Prove that $\ker(\phi)$ **is normal subgroup of** G: Assume $a \in \ker(\phi)$ and $g \in G$

$$\phi(g * a * g^{-1}) = \phi(g) \# \phi(a) \# \phi(g)^{-1} = \phi(g) \# 1_H \# \phi(g)^{-1} = 1_H$$

Which means $g * a * g^{-1} \in \ker\phi$ for every choice of $g \in G$ which by definition means that $\ker(\phi) \triangleleft G$

- **Problem 7**
- **Problem 8**