1) Show that any postage of $n \geq 18$ cents can be made by using 4 and 7 cent stamps. Can you generalize the result?.

Claim: $n \geq 18 = a * 7 + b * 4$

Proof By Mathematical Induction on n: Base Case: Let $n = 18$ then $18 = 2*7+1*4$,$n = 19$ then $19 = 1*7+3*4$,$n = 20$ then $20 = 0*7+5*4$,$n = 21$ then $3 * 7 + 0 * 4$

Inductive Step: Suppose we can write $m = a*7+b*4$ for all $18 \leq m \leq k$ where $k \geq 2$. We wish to show we can write $k + 1 = a * 7 + b * 4$

$$
\begin{aligned}
P(k-3) &= a * 7 + b * 4 \\
k - 3 &= a * 7 + b * 4 \\
k + 1 &= a * 7 + b * 4 + 4 \\
k + 1 &= a * 7 + (b + 1) * 4
\end{aligned}
$$

By strong induction on n we have shown that P(k+1) is true and can conclude for $n \geq 18$ that $n = a * 7 + b * 4, a, b \in \mathbb{Z}$ ∎

2) Prove the Generalized Commutative Law.

Claim: Generalized Commutative Law holds.

Proof: Suppose the associative and commutative law hold. Next suppose: σ is a permutation where 1 maps to $\sigma(1)$, 2 maps to $\sigma(2)$, ..., n maps to $\sigma(n)$. Then $\sigma(1) \in \{1, 2, \ldots, \text{n}\}$. Let $\sigma(1)$ be any arbitrary element in that set denoted by a_k. Then,

$$
\begin{aligned}
a_1 a_2 \ldots a_n &= a_1 a_2 \ldots a_{k-1} a_k a_{k+1} \ldots a_n \\
&= a_1 a_2 \ldots a_k a_{k+1} a_{k-1} \ldots a_n (Associative) \\
&= a_1 a_2 \ldots a_k a_{k-2} a_{k-1} \ldots a_n (Associative)
\end{aligned}
$$

We continue shifting entries like this in accordance with the associative and commutative laws. We do this by swapping two entries at a time to form permutations. We end up with the following:

$$
\begin{aligned}
&= a_k a_1 a_2 \ldots a_n \\
&= a_{\sigma(1)} a_1 a_2 \ldots a_n
\end{aligned}
$$

We do the same with $\sigma(2) \in \{1, 2, \ldots, \text{n}\}$. Then $\sigma(2)$ is some arbitrary element mapped to by our set such that $\sigma(1) \neq \sigma(2)$ and is denoted a_l. We have from above that:

$$a_1a_2\dots a_n = a_{\sigma(1)}a_1a_2\dots a_{k-2}a_{k-1}a_{k+1}\dots a_n$$

By using same reasoning for $\sigma(1)$ we achieve:

$$a_1a_2\dots a_n = a_{\sigma(1)}a_{\sigma(2)}a_1a_2\dots a_n$$

We repeat this process up to the cardinality of the set in order to get:

$$a_1a_2\dots a_n = a_{\sigma(1)}a_{\sigma(2)}\cdots a_{\sigma(n)}$$

Therefore, we can conclude that the Generalized Commutative Law holds. ∎

3) Suppose that $p \geq 2$ is an integer with the following property: If m and n are integers and $p \mid mn$ then $p \mid m$ or $p \mid n$. Show that p is necessarily a prime number.

Claim: p is necessarily prime

Proof: Without loss of generalization suppose $p \geq 2, p \in \mathbb{Z}$ such that if $p \mid mn$ then $p \mid m$ or $p \mid n$, $m, n \in \mathbb{Z}$
Then by assumption we have 2 cases. Either $p \mid mn$ or p does not divide mn . In the case that p doesnt divide mn, then it is obvious $gcd(p, mn) = 1$ and by extension, $gcd(p, m) = gcd(p, n) = 1$. This is because p shares no common divisor with m or n, except 1. Therefore, p must be prime.
If $p \mid mn$ then $p \mid m$ or $p \mid n$ by assumption. If $p \mid m$ then by PFT, m is made up of a product of primes as m is an integer. Then $p \mid p_1p_2\dots p_n$. Since m is composed of primes and p divides m, then p must also be prime as its the case that $p \in \{p_1p_2\dots p_n\}$ then it is obvious p is prime. If $p \notin p_1p_2\dots p_n$ then its only factors with m are 1 and itself, so it must be the case that p is prime. ∎

4) Show that $gcd(a, b, c) = gcd(a, gcd(b, c))$.

Claim: $gcd(a, b, c) = gcd(a, gcd(b, c))$

Proof: Suppose $x \in gcd(a, b, c)$, mainly that x = $gcd(a, b, c)$. By definition, x is the largest non zero integer that divides a,b, and c. So $x \mid a, x \mid b, x \mid c$. Then $x \mid a, x \mid gcd(b, c)$, and by extension $x \mid gcd(a, gcd(b, c))$.
Similarly, suppose $x \in gcd(a, gcd(b, c))$, then $x \mid gcd(a), x \mid gcd(gcd(b, c))$, furthermore, $x \mid a, x \mid gcd(b, c) \Rightarrow x \mid b, x \mid c$. So $x \mid gcd(a, b, c)$. Then we can say that $gcd(a, gcd(b, c)) \mid gcd(a, b, c)$ and $gcd(a, b, c) \mid gcd(a, gcd(b, c))$. We can conclude by stating that $gcd(a, b, c) = gcd(a, gcd(b, c))$, ∎

5) Show that the following conditions on an integer n 2 are equivalent:

- $\bar{a}^2 = \bar{0}^2$ **in** $\mathbb{Z}_n$ **implies that** $\bar{a} = \bar{0}$
- **n is square free.**

Proof: Suppose n is not square free. We wish to show that for some a that $a^2 = 0 mod n$ for which $a! = 0 mod n$. Consider when $r = 2$, then $n = mp^2$ and $0 = mn = (mp)^2 mod n$. Thus, we have found an $a = mp$, such that $a^2 = 0 mod n$ but $a! = 0 mod n$. This forms a contradiction on the contrapositive. This proves that a implies b. Now for the vice versa.
Suppose $a^2 = 0 mod n$ and n is square free. Then $a^2 = kn, k \in \mathbb{Z}$. By PFT we write:

$$p_1^{2r_1} p_2^{2r_2} \dots p_j^{2r_j} = k q_1 q_2 \dots q_j n$$

where $p_j \neq p_i, q_j \neq q_i, i, j \in \mathbb{Z}$. Since from the assumption of n is square free we have that all q's are distinct and that each p must equal at most one 1. Then $a \mid k$, so $k = la$ and $a^2 = lan$. If a is not zero then $a = ln$ and $a = 0 mod n$. If a is zero then obviously $a = 0 mod n$. ∎

6) Find $x \in \mathbb{Z}$ **such that** $x \equiv 5(mod 10), x \equiv 3(mod 11), x \equiv 2(mod 7)$**.**

Proof: Let us first examine the first two congruence relations.

$$\begin{aligned} x &= 5(1 * 11) + 3(-1 * 10) \\ x &= 55 - 30 \\ x &= 25 \end{aligned}$$

Now we are left with two relations: $x \equiv 25 mod 110, x \equiv 2 mod 7$

$$\begin{aligned} x &= 25(-47 * 7) + 2(3 * 110) \\ x &= -8225 + 660 \\ x &= -7565 \\ x &= -7565 * (770 * 10) \\ x &= 135 \end{aligned}$$

∎

7) Let $n \in \mathbb{N}, n \geq 2$. Define $\phi(n)$ to be the cardinality of the set $\{i : 1 \leq i \leq n-1, gcd(i,n) = 1$ Note that only part a is completed, neither part b nor c are here..

Claim: If p is a prime number and $k \in \mathbb{N}$ with $k \geq 1$, then $\phi(p^k) = p^{k1}(p1)$

Proof By Mathematical Induction on n: Base Case: Suppose p is prime and n = 1, then $\phi(p) = p^{1-1}(p-1) = (p-1)$.
Inductive Step: Suppose $\phi(p^k) = p^{k-1}(p-1)$ we wish to show $\phi(p^{k+1}) = p^k(p-1)$.
Suppose $\phi(p^{k+1})$ then there are $p^{k+1}-1$ terms potentially coprime to p^{n+1}. By the inductive hypothesis we say there are $p^{k-1}(p-1)$ terms coprime to p^k. This must be true for p^{k+1} because they share no common primes. From the terms left over we have $p^k(p-1)-1$ of the form $p^k + pm, 1$. We take the difference: $(p^{k+1}-1) - (p^{k-1}(p-1))$ and we get the following:

$$\begin{aligned} p^{k+1} - 1 - p^{k-1}(p-1) - p^{k-1} + 1 \\ = p^{k-1} * p(p-1) \\ = p^k(p-1) \end{aligned}$$

This concludes our proof. ∎

8) Suppose that $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$ and $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ in $\mathbb{S}_5$. If $\sigma(1) = 2$ find σ and τ..

Proof: This was done by tracing each element back, but was also reduced to a system of linear equations which was solved via linear algebra.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

∎

9) Factor σ into disjoint cycles, find the parity, and factor the inverse in disjoint cycles, where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 9 & 5 & 2 & 1 & 6 & 4 & 7 \end{pmatrix}$.

Proof: σ can be factored into these disjoint cycles: $\begin{pmatrix} 1 & 3 & 9 & 7 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 8 & 4 & 5 \end{pmatrix}$. By section 1.4, Theorem 6 we have that $\begin{pmatrix} 1 & 3 & 9 & 7 & 6 \end{pmatrix}$ has an even parity, and $\begin{pmatrix} 2 & 8 & 4 & 5 \end{pmatrix}$ has odd parity. So σ is odd because an even plus an odd is also odd. $\sigma^{-1} = \begin{pmatrix} 3 & 8 & 9 & 5 & 2 & 1 & 6 & 4 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$. This can be factored into these disjoint cycles: $\begin{pmatrix} 1 & 6 & 7 & 9 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 5 & 4 & 8 \end{pmatrix}$ ∎