Problem 1. (The group $\mathbb{Z}_{101}^*$)
Let $G = \mathbb{Z}_{101}^*$.

(a) Find $|G|$. This is the number of positive integers less than 101 which are relatively prime to 101.

(b) Find the inverse of $\overline{33}$ in G.

(c) For $k = 2, 4, 7, 8$, find an element in G of order k, or state why it cannot exist.

(d) Does $\overline{10}$ have a square root modulo 101? Give reasons for you answer.

Solution. Recall that $\mathbb{Z}_n^*$ is the set of members of $\mathbb{Z}_n$ which are invertible. Each such member is represented by a unique integer between 1 and $n-1$ which is relatively prime to n.

(a) Since 101 is prime, every positive integer less than 101 is relatively prime to 101. Thus $|\mathbb{Z}_{101}^*| = 100$.

(b) Perform the Euclidean algorithm to find that

$$33(49) + 101(-16) = 1.$$

Thus

$$1 \equiv 33(49) + 101(-16) \equiv 33(49) + 0 \equiv 33(49) \pmod{101},$$

so the inverse of $\overline{33}$ in $\mathbb{Z}_{101}^*$ is $\overline{49}$.

(c) For convenience, we modulo 101 without bars.

Since $100 = -1$, we see that $100^2 = 1$, so $\operatorname{ord}(100) = 2$.

Since $10^2 = 100$, we see that $\operatorname{ord}(10) = 4$.

Since neither 7 nor 8 divides $|G| = 100$, we cannot have elements of those orders in $G = \mathbb{Z}_{101}^*$.

(d) A square root of $\overline{10}$ would have order 8, so no such element exists.

$\square$

Problem 2. (The group A_5)
Let $G = A_5$.

(a) Find $|G|$.

(b) Find the inverse of `(1 3 5 2)(2 4 5)(3 7 4)(5 7)`.

(c) Find all possible shapes of members of G. Find how many elements of each shape exist.

(d) Does A_5 have a subgroup of order ten? Give reasons for you answer.

Solution. The group A_5 consists of all even permutations in S_5.

(a) Since exactly half of the $5! = 120$ permutations are even, $|A_5| = 60$.

(b) Let α = `(1 3 5 2)(2 4 5)(3 7 4)(5 7)`. Multiply the cycles to get α = `(1 3 7)(2 4 5)`. So α^{-1}`(1 7 3)(2 5 4)`.

(c) The possible shapes in S_5 are `[1]`, `[2]`, `[3]`, `[4]`, `[5]`, `[2, 2]`, and `[2, 3]`. Of these, only `[1]`, `[3]`, `[2, 2]`, `[5]`, and `[2, 3]` give even permutations.

`[1]`: There is only one identity, so there is 1 element of this shape.

`[3]`: There are $\binom{5}{3}$ ways to choose three elements, and each set of three elements gives two permutations. Thus there are $2\binom{5}{3} = 2 \cdot 10 = 20$ permutations of this shape.

`[5]`: Each five cycle moves all points. Writing the cycle with `1` first, the last four elements of the cycle can be arranged in any order, so there are $4! = 24$ permutations of this shape.

`[2, 2]`: Each set of four elements from $\{1, 2, 3, 4, 5\}$ give three different involutions of shape $[2, 2]$; these three, together with the identity, four a Klein four subgroup of A_5. There are $\binom{5}{4}$ ways to select such a set, so there are $3\binom{5}{4} = 3 \cdot 5 = 15$ permutations of this shape.

Note that $1 + 20 + 24 + 15 = 60$, so we have accounted for every element of A_5.

(d) We have seen that all of the permutations in D_5 are even, so $D_5 \leq A_5$. Since $|D_5| = 10$, we know that A_5 contains a subgroup of order ten.

$\square$

Problem 3. (The group $\mathcal{P}(X)$)
The *symmetric difference* of two sets A and B is

$$A \triangle B = (A \cup B) \smallsetminus (A \cap B).$$

Let X be any set. Then $\mathcal{P}(X)$ is a group under the operation of symmetric difference. Let $G = \mathcal{P}(\{1, 2, 3, 4\})$.

(a) Find $|G|$.

(b) State the identity element of G. Let $A \in G$; state the inverse and the order of A.

(c) Does G have any subgroups isomorphic to C_4? to K_4? Explain.

(d) Is $\mathcal{P}(X)$ a group under intersection? Justify your answer.

Solution. Recall that $\mathcal{P}(X)$ consists of all subsets of the set X. Let $X = \{1, 2, 3, 4\}$ so that $G = \mathcal{P}(X)$.

(a) The power set of a set of cardinality n contains 2^n elements, so $|\mathcal{P}(X)| = 2^4 = 16$.

(b) The identity element is $\varnothing$, since $A \triangle \varnothing = \varnothing$.

(c) Every element in G has order two, so there is no cyclic subgroup of order four. However, since G is abelian, any two distinct element of order two generate a Klein four subgroup.

(d) No, $\mathcal{P}(X)$ is not a group under intersection. There is an identity element, namely X, since $A \cap X = A$ for all $A \subset X$. However, let A be a proper subset of X, and let B be any subset of X. Since $A \cap B$ is a subset of A, it is a proper subset of X, and there B is not an inverse for A, so A is not invertible.

$\square$

Problem 4. (Number Theory)
Complete the following proofs.

(a) Let $a, b, c \in \mathbb{Z}$.
Show that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. Since $a \mid bc$, there exists $k \in \mathbb{Z}$ such that $\underline{ka} = bc$.

Since $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $\underline{ax + by} = 1$.

Multiply the second equation by $\underline{c}$ to obtain $\underline{acx + bcy} = c$.

Substitute the first equation into the second to obtain $\underline{axc + kay} = c$.

Factor out a from the left hand side to obtain $\underline{a(xc + ky)} = c$.

Thus $a \mid c$. $\square$

(b) Let $m, n \in \mathbb{Z}$. Let G be a group, and let $g \in G$ be an element of order m.
Show that if $g^n = 1$, then $m \mid n$.

Proof. By the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $n = \underline{mq + r}$,

where $0 \leq \underline{r} < \underline{m}$.

Since $g^n = 1$, we have $1 = g^{mq+r} = (g^m)^q g^r = 1^q g^r = g^r$.

Since $g^r = 1$, and $0 \leq r < m$, and m is the smallest positive integer such that $g^m = 1$, we must have $r = 0$; that is, $n = mq$.

Thus $m \mid n$. $\square$

Problem 5. (Group Theory)
Supply a short proof in each case.

(a) Let G be a finite group of even order. Show that G has an element of order two.

Solution. Consider the function $\alpha : G \to G$ given by $\alpha(g) = g^{-1}$. Then α is a permutation of G, and G is the disjoint union of the orbits of α. Since $\alpha(1) = 1$, the orbit of 1 is odd, and since $|G|$ is even, α must have another orbit of odd length. However, since $(a^{-1})^{-1} = a$, each orbit of α has cardinality at most two. Thus, α has another orbit of length one, so α has another fixed element, say $\alpha(g) = g$ where $g \neq 1$. Thus $g = g^{-1}$, which implies $g^2 = 1$, so g is an element of order two. $\square$

(b) Let G be a finite group in which every nontrivial element has order two. Show that G is abelian.

Solution. Let $a, b \in G$. Then $a^2 = 1$ and $b^2 = 1$. Multiplying these equations gives $a^2b^2 = 1$.

But ab is also in G, so $(ab)^2 = 1$; that is, $abab = 1$. Combining these equations produces $a^2b^2 = abab$. Multiplying on the left by a^{-1} and on the right by b^{-1} produces $ab = ba$, as we desired. $\square$