1. [15 points] Consider $\mathbb{Z}_{22}$.
   
   (i) List the elements of the unit group $U_{22}$.
   
   Since $\phi(22) = \phi(2)\phi(11) = 1 \cdot 10 = 10$, we should expect 10 integers (relatively prime to 22). They are:
   
   $1, 3, 5, 7, 9, 13, 15, 17, 19, 21$.

   (ii) What are the possible orders of the elements of $U_{22}$?
   
   Since the order of $U_{22}$ is 10, the order of its elements are divisors of 10 and so one of 1, 2, 5, 10.

2. [10 points] Prove Fermat’s Theorem for finite abelian groups: Let $G = \{e = a_1, a_2, \ldots, a_n\}$ be an abelian group with $n$ elements. Then for each $a$ in $G$, $a^n = e$, the identity of $G$.

   Proof: By the cancellation law for groups, if $a$ is any element of $G$, then $\{a a_1, a a_2, \ldots, a a_n\} = \{a_1, a_2, \ldots, a_n\}$. So
   
   $a a_1 a_2 \cdots a_n = a_1 a_2 \cdots a_n$.
   
   That is, $a^n(a_1 a_2 \cdots a_n) = (a_1 a_2 \cdots a_n)$. By cancellation, we get $a^n = e$.

3. [10 points] Let $G$ be a multiplicative group. Using only the definition of a group (the group axioms), prove that a linear equation of the form $ax = b$ has exactly one solution.

   Proof: First $a^{-1}b$ is a solution, since $a(a^{-1}b) = (aa^{-1})b = eb = b$. Suppose there are two solutions $g$ and $h$. Then $ag = b$ and $ah = b$ so that $ag = ah$. By cancellation, $h = g$. So the solution is unique.

4. [20 points] Let $G$ be a multiplicative group and let $H$ be a nonempty subset of $G$.

   (i) What two properties need to be checked for $H$ to be a subgroup of $G$?

   Closure under multipication and closure under taking inverses.

   (ii) If $H$ is a subgroup of $G$, state Lagrange’s theorem.

   The order of $H$ is a divisor of the order of $G$.

   (iii) Let $G$ be the group $U_{13}$ of units of $\mathbb{Z}_{13}$. Determine a subgroup $H$ of 3 elements and then determine its distinct cosets (as subsets of $U_{13}$).

   We need to find an element of order 3, The element 2 doesn’t work but 3 does: $3^1 = 3, 3^2 = 9, 3^3 = 1$ (all mod 13). So $H = \{1, 3, 9\}$ is a subgroup of order 3. $H$ is a coset, and the other cosets are:
\[ 2H = \{2, 6, 18 = 5\}, \quad 4H = \{4, 12, 36 = 10\}, \quad 7H = \{7, 21 = 8, 63 = 11\}. \]

5. [10 points] Let \( G \) and \( G' \) be multiplicative groups with identities \( e \) and \( e' \), respectively. Let \( f : G \to G' \) be a homomorphism. Using that \( f(e) = e' \), prove that

\[ f(a^{-1}) = f(a)^{-1} \quad (a \in G). \]

We have \( aa^{-1} = e \), and so \( f(aa^{-1}) = f(e) = e' \). Since \( f \) is a homomorphism, this gives \( f(a)f(a^{-1}) = e' \). Hence \( f(a^{-1}) \) is the inverse of \( f(a) \), that is, \( f(a)^{-1} = f(a^{-1}) \).

6. [15 points] What is the order of the subgroup of \( S_{12} \) generated by the permutation

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
7 & 10 & 9 & 8 & 1 & 12 & 3 & 4 & 11 & 6 & 5 & 2
\end{pmatrix}.
\]

\( f \) partitions into cycles of lengths 6, 4, and 2. Hence the order is \( \text{LCM}(6, 4, 2) = 12 \).

7. [20 points] Use the **Euclidean algorithm** to find the GCD of the two polynomials in \( \mathbb{Z}_2[x] \):

\[ f(x) = x^4 + x^2 + 1 \quad \text{and} \quad g(x) = x^3 + 1, \]

and express it as a linear combination of \( f(x) \) and \( g(x) \).

We have

\[
x^4 + x^2 + 1 = x(x^3 + 1) + (x^2 + x + 1) \\
x^3 + 1 = (x + 1)(x^2 + x + 1) + 0.
\]

Hence the GCD is \( x^2 + x + 1 \) and

\[ x^2 + x + 1 = 1(x^4 + x^2 + 1) + x(x^3 + 1). \]