Cryptographic Protocols
Session 1 - Number Theory & Algebra

1. Prove that a prime order group is cyclic and find the set of all its generators.

2. Analyze $\mathbb{Z}_{22}^*$:
   (a) Find all elements of $\mathbb{Z}_{22}^*$ and a multiplicative inverse of each element.
   (b) Check that $\phi(22) = \text{Ord}(\mathbb{Z}_{22}^*)$.
   (c) Find all subgroups of $\mathbb{Z}_{22}^*$.
   (d) Is $\mathbb{Z}_{22}^*$ cyclic? What is $\text{ord}(7)$?

3. Let $G$ be a group and $C$ be a cyclic group.
   (a) Prove that $G \times G$ is a group respect to point-wise operations.
   (b) Is $G \times C$ or $C \times C$ cyclic?

4. Let $H$ be the set of all matrices of the form
   $\begin{pmatrix}
   1 & a & c \\
   0 & 1 & b \\
   0 & 0 & 1
   \end{pmatrix}$ for $a, b, c \in \mathbb{R}$.
   (a) Prove that $H$ is a group respect to matrix multiplication or bring a counterexample.
   (b) Prove that $H$ is an Abelian group or bring a counterexample.

5. Prove that $\mathbb{Z} \times \mathbb{Z}$ with pointwise addition and multiplication defined as $(a, b) 
   \cdot (c, d) = (ac-bd, ad+bc)$ is a ring (or even a field?) or bring a counterexample.

6. Represent the polynomial $X^2Y + 3XZ + ZY + 5X + 7$ as an arithmetic circuit.
Theorem 1. For any \( n \geq 1 \), \( \mathbb{Z}_n^* = \{ x \in \mathbb{Z}_n \mid \gcd(x, n) = 1 \} \).

Theorem 2 (Bézout’s Identity). Let \( a, b \in \mathbb{Z} \) and \( \gcd(a, b) = d \), then there exists \( x, y \in \mathbb{Z} \) such that \( ax + by = d \).

Theorem 3 (Totient properties). Following properties hold:
1. If \( p \) is prime and \( k \geq 1 \), then \( \phi(p^k) = p^k - 1 \).
2. If \( p \) and \( q \) are prime, then \( \phi(pq) = (p - 1)(q - 1) \).
3. For any \( n \geq 1 \),
\[
\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}),
\]
where \( p|n \) denotes any prime dividing \( n \).

Theorem 4 (Fermat’s Little Theorem). If \( p \) is a prime, then for any \( a \in \mathbb{Z} \), \( a^p \equiv a \pmod{p} \).

Theorem 5 (Euler’s Theorem). If \( n \) and \( a \) are positive coprime integers, then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

Theorem 6 (Chinese Remainder Theorem). Let \( n_1, \ldots, n_k > 1 \) be pairwise coprime, \( N := \prod_{i=1}^{k} n_i \), and \( a_1, \ldots, a_k \) are integers such that \( 0 \leq a_i < n_i \). Then, the equation system
\[
x \equiv a_1 \pmod{n_1} \\
\vdots \\
x \equiv a_k \pmod{n_k}
\]
has a unique solution up to modulo \( N \). Equivalently \( \mathbb{Z}_N \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k} \) as rings.

Theorem 7. If \( p \) is prime, then \( \mathbb{Z}_p \) is a field (ring where elements in \( \mathbb{Z}_p \setminus \{0\} \) are invertible).