EE 720: Introduction to Number Theory and Cryptography (Autumn 2023)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 2: 20 points Date: October 26, 2023

---

1. [5 points] Prove the following statement. Let a, b be positive integers. Then there exist integers X, Y such that $Xa + Yb = \gcd(a, b)$. Furthermore, $\gcd(a, b)$ is the smallest positive integer that can be expressed this way.

   Note: The **greatest common divisor** of two integers a, b not both zero, written $\gcd(a, b)$, is the largest integer c such that $c \mid a$ and $c \mid b$.

2. Let G be a finite **abelian** group. Let H be a subgroup of G. A coset of H is a set of the form $g + H = \{g + h \mid h \in H\}$ for a fixed $g \in G$. Prove the following statements.

   (a) [1½ points] Two cosets of H are either equal or disjoint.

   (b) [1½ points] All cosets of H have the same cardinality.

   (c) [2 points] Use the two results above, to prove Lagrange's theorem, i.e. $|H|$ divides $|G|$.

   Note: A set G with a binary operation $*$ is called a group if

   - $a * b \in G$ for all $a, b \in G$.
   - There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
   - For every $a \in G$, there is an element $b \in G$ such that $a * b = b * a = e$
   - For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$

   A subgroup H of G which is itself a group under the same binary operation.

3. [5 points] An integer $a \in \mathbb{Z}_N^*$ is called a **witness for compositeness of** N if $a^{N-1} \neq 1 \bmod N$. Prove the following statement. If there exists a witness in $\mathbb{Z}_N^*$ that N is composite, then at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

   Note: $\mathbb{Z}_N^* = \{i \in \{1, 2, \ldots, N-1\} \mid \gcd(i, N) = 1\}$ is a group with multiplication modulo N as the operation.

4. [5 points] Show that the Diffie-Hellman protocol is **insecure** against a **man-in-the-middle attack**. The setting is as follows:

   - Alice and Bob want to generate a shared key using the Diffie-Hellman protocol.
   - An attacker Eve can intercept messages sent by Alice/Bob and replace the messages with her own messages.
   - The attack is successful if Eve knows the key k_A which Alice generates **or** if Eve knows the key k_B that Bob generates. Note that k_A need not be equal to k_B.