EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 2: 20 points Date: October 18, 2024

1. [5 points] Let a, b be positive integers. Prove the following statements.

   - There exist integers X, Y such that $Xa + Yb = \gcd(a, b)$.
   - $\gcd(a, b)$ is the smallest positive integer that can be expressed as an integer linear combination of a and b.

2. [5 points] Let G be a finite group with operation $*$. Suppose H is a nonempty subset of G that is closed under the group operation, i.e. for all $h_1, h_2 \in H$ the element $h_1 * h_2$ also belongs to H. Prove that H is a subgroup of G.

3. [5 points] Suppose $N = pq$ for some integers p, q satisfying $p > 1, q > 1$ and $\gcd(p, q) = 1$. Let X and Y be integers such that $Xp + Yq = 1$. For some $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, let $x = aYq + bXp \bmod N$. **Without using the Chinese Remainder Theorem**, prove that x belongs to $\mathbb{Z}_N^*$ for any $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

   Note: You are not allowed to use the Chinese Remainder Theorem (CRT) because this result was itself used to prove the CRT.

4. [5 points] Let $N > 1$ be an odd composite integer which is not a prime power. Let $N - 1 = 2^r u$ where $r \geq 1$ and u is odd. An integer $a \in \mathbb{Z}_N^*$ is called a **strong witness for the compositeness of** N if

   - $a^u \neq 1 \bmod N$ and
   - $a^{2^i u} \neq -1 \bmod N$ for all $i \in \{0, 1, 2, \ldots, r-1\}$

   Construct an element b in $\mathbb{Z}_N^*$ that is a strong witness for the compositeness of N. You have to prove that it satisfies the above definition.