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

Assignment 3: 20 points | Date: October 6, 2023

---

1. [5 points] Let a, b be integers not both zero. Let c also be an integer. Prove that the equation $ax + by = c$ has a solution (x, y) in $\mathbb{Z}^2$ if and only if $\gcd(a, b)$ divides c.

2. Let G and H be groups. A function $\phi : G \mapsto H$ is called a **group homomorphism** if it satisfies
$$\phi\left(g_1 \star g_2\right) = \phi(g_1) \circ \phi(g_2), \text{ for all } g_1, g_2 \in G.$$
Here $\star$ is the group operation in G and $\circ$ is the group operation in H.
   (a) [2½ points] Let e_G be the identity of G and let e_H be the identity of H. Prove that $\phi(e_G) = e_H$.
   (b) [2½ points] For all $g \in G$, prove that $\phi(g^{-1}) = [\phi(g)]^{-1}$.

3. Let G be a group whose identity element is e.
   (a) [2½ points] Prove that if H and K are finite subgroups of G whose orders are relatively prime, then $H \cap K = \{e\}$.
   (b) [2½ points] Prove that if $g^2 = e$ for all $g \in G$ then G is abelian.

4. [5 points] Find all solutions of the following equation in $\mathbb{Z}_{77}$ by hand, i.e. not using a computer.
$$x^2 + 3x + 4 = 0 \bmod 77.$$