EE 720: Introduction to Number Theory and Cryptography (Autumn 2025)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 3: 20 points — Date: October 9, 2025

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 $\phi(g^{-1}) = \left[\phi(g)\right]^{-1}$.

3. [5 points] Compute $101^{4,800,000,002} \bmod 35$ using the properties of $\mathbb{Z}_{35}^*$.

4. [5 points] Solve the following system of congruences using the Chinese remainder theorem.
$$\begin{aligned} x &= 2 \bmod 11, \\ x &= 3 \bmod 12, \\ x &= 4 \bmod 13. \end{aligned}$$