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

Assignment 4: 20 points Date: October 10, 2024

1. [5 points] Suppose $N = pq$ where $\gcd(p, q) = 1$. Prove that the map $f(x) = (x \bmod p, x \bmod q)$ is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

2. [5 points] Compute $101^{4,800,000,002} \bmod 35$ using the Chinese remainder theorem.

3. [10 points] Solve the following system of congruences using the Chinese remainder theorem.

$$
\begin{aligned}
x &= 2 \bmod 11, \\
x &= 3 \bmod 12, \\
x &= 4 \bmod 13, \\
x &= 5 \bmod 17, \\
x &= 6 \bmod 19.
\end{aligned}
$$