CS 435: Introduction to Cryptography **Fall 2020**

Homework 6

Professor Somesh Jha **Due:** November 28

- **Problem 1 [20 points].** Let $N = pqr$, where p, q, r are three distinct primes. Let $c \geq 1$ be a positive integer such that $c < \min\{p, q, r\}$. Suppose x is an integer that satisfies the following conditions: $x \equiv c \pmod{p}$, $x \equiv c \pmod{q}$, and $x \equiv c \pmod{r}$. Prove that $x \equiv c \pmod{N}$.

- **Problem 2 [30 points].** 1500 soldiers arrive at a training camp. A few soldiers desert the camp. The drill sergeants divide the remaining soldiers into groups of five and discover that there is one left over. When they divide them into groups of seven, there are three left over. When they divide them into groups of eleven, there are again three left over. Determine the number of deserters.

- **Problem 3 [30 points].** Suppose the $x \equiv 3 \pmod{7}$, $x \equiv 3 \pmod{10}$, and $x \equiv 3 \pmod{25}$. Explain why the Chinese Remainder Theorem does not apply to compute x. Transform the problem to an equivalent problem where the Chinese Remainder Theorem can be used and solve it.

- **Problem 4 [20 points].** Let $N = pq$, where p and q are two large odd primes (i.e. think p and q are 1000 bits). Prove that if Oscar can find a message m such that $0 < m < N$ and $m \notin \mathbb{Z}_N^\star$, he can factor N.