Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. CRT: Uniqueness of solutions. Suppose that u and v are both solutions to the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

   Prove that $u \equiv v \pmod{M}$. Hint: how many tuples $(a_1, \ldots, a_k)$ are there such that $a_i \in \mathbb{Z}_{m_i}$ for each i? If u and v were different elements in $\mathbb{Z}_M$ that both corresponded to the same tuple $(a_1, \ldots, a_k)$, what would happen?

2. Solve the following systems of congruences.

   (a)

$$\begin{aligned} x &\equiv 18 \pmod{25} \\ x &\equiv 7 \pmod{11} \\ x &\equiv 16 \pmod{32} \end{aligned}$$

   (b)

$$\begin{aligned} 17x &\equiv 8 \pmod{43} \\ 6x &\equiv 41 \pmod{55} \\ 5x &\equiv 4 \pmod{9} \end{aligned}$$

3. Alice and Bob wish to use the ElGamal cryptosystem to communicate, and they are having difficulty deciding on a prime/base pair (p, g). The pairs that they are considering are $(345601, 71482)$ (option A), $(516163, 482305)$ (option B), and $(177007, 145014)$ (option C). Which option do you recommend for Alice and Bob, and why?