Math 342 Tutorial
June 11, 2025

Question 1. Find all solutions to following systems of congruences in two ways: first, using the Chinese Remainder Theorem; and second, by iteratively solving and substituting linear congruences.

(a) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$.

(b) $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$.

Question 2. Give the following generalization of the Chinese Remainder Theorem. Let $m_1, \ldots, m_r$ be pairwise coprime integers, and let $a_1, \ldots, a_r$ be given integers such that each $(a_i, m_i) = 1$. Then the system $a_1x \equiv b_1 \pmod{m_1}, \ldots, a_rx \equiv b_r \pmod{m_r}$ has exactly one solution modulo $m_1 \cdots m_r$.

Question 3. (a) Show that the system of congruences $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$ has a solution if and only if $(m_i, m_j) \mid (a_i - a_j)$ for all $i < j$. Show that if a solution exists, then it is unique modulo $[m_1, \ldots, m_r]$. [Hint: succesively substitute linear equations.] (b) Solve the system $x \equiv 4 \pmod 6$, $x \equiv 13 \pmod{15}$. (c) Solve the system $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$. (d) Does the system $x \equiv 1 \pmod 8$, $x \equiv 3 \pmod 9$, $x \equiv 2 \pmod{12}$ have any solutions?

Question 4. Show there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1. [Hint: Use CRT to show there is a simultaneous solution to the system $x \equiv 0 \pmod 4$, $x \equiv -1 \pmod 9$, $x \equiv -2 \pmod{25}$, $\ldots$, $x \equiv -k + 1 \pmod{p_k^2}$ where p_k is the kth prime.]

Question 5. Let $m = 2^{e_0}p_1^{e_1} \cdots p_k^{e_k}$. Show the congruence $x^2 \equiv 1 \pmod m$ has exactly r^{r+s} solutions where $s = 0$ is $e_0 = 0$ or 1, $s = 1$ if $e_0 = 2$, and $s = 2$ if $e_0 > 2$. [Hint: Use question 12 from the May 28th tutorial set.]

Question 6. Find all solutions to the following congruences. (a) $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{121}$. (b) $x^2 + 4x + 2 \equiv 0 \pmod{343}$. (c) $13x^7 - 42x - 649 \equiv 0 \pmod{1323}$.

Question 7. Suppose $(a, p) = 1$. Use Hensel's Lemma to find a recursive formula for the solutions of $ax \equiv 1 \pmod{p^k}$ for all positive integers k.