CS 70 Discrete Mathematics and Probability Theory
Summer 2021 DIS 2C

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x+5 \equiv 7 \pmod{11}$.

(b) Show that $3x+15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x+2y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{21} \equiv x \pmod{11}$.

2 When/Why can we use CRT?

Let $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$ where $m_i > 1$ and pairwise relatively prime. In lecture, you've constructed a solution to

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

Let $m = m_1 \cdot m_2 \cdots m_n$.

1. Show the solution is unique modulo m. (Recall that a solution is unique modulo m means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$.)

2. Suppose m_i's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.

3. Suppose m_i's are not pairwise relatively prime and a solution exists. Is it guaranteed that the solution is unique modulo m? Prove or give a counterexample.

3 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

(a) Find a number $0 \leq b_2 < 30$ such that $b_2 \equiv 1 \pmod 2$, $b_2 \equiv 0 \pmod 3$, and $b_2 \equiv 0 \pmod 5$.

(b) Find a number $0 \leq b_3 < 30$ such that $b_3 \equiv 0 \pmod 2$, $b_3 \equiv 1 \pmod 3$, and $b_3 \equiv 0 \pmod 5$.

(c) Find a number $0 \leq b_5 < 30$ such that $b_5 \equiv 0 \pmod 2$, $b_5 \equiv 0 \pmod 3$, and $b_5 \equiv 1 \pmod 5$.

(d) What is x in terms of b_2, b_3, and b_5? Evaluate this to get a numerical value for x.