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 (practice)

Solve for $x \in \mathbb{Z}$ where:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

(a) Find the multiplicative inverse of 5×7 modulo 3.

(b) What is the smallest $a \in \mathbb{Z}^+$ such that $5 \mid a$, $7 \mid a$, and $a \equiv 2 \pmod 3$?

(c) Find the multiplicative inverse of 3×7 modulo 5.

(d) What is the smallest $b \in \mathbb{Z}^+$ such that $3 \mid b$, $7 \mid b$, and $b \equiv 3 \pmod 5$?

(e) Find the multiplicative inverse of 3×5 modulo 7.

(f) What is the smallest $c \in \mathbb{Z}^+$ such that $3 \mid c$, $5 \mid c$, and $c \equiv 4 \pmod 7$?

(g) Write down the set of solutions for the system of equations.