

Introductory Number Theory

Problem 1: Solve the congruence

$$9x \equiv 21 \pmod{12}$$

listing all the incongruent solutions. (25 points)
(This is Problem 1 (c) for Chapter 5 in the course notes.)

Problem 2: By the Chinese remainder theorem, the system of congruences

$$x \equiv 1 \pmod{4} \quad x \equiv 4 \pmod{5} \quad x \equiv 3 \pmod{7}$$

has a unique solution modulo 140. Find this solution by using the method for the proof of the Chinese remainder theorem, as in the example in the course notes directly following this theorem. This method consists of the following steps:

1. For the numbers $M_1 := 5 \cdot 7 = 35$, $M_2 := 4 \cdot 7 = 28$, and $M_3 := 4 \cdot 5 = 20$, find numbers b_1 , b_2 , and b_3 such that

$$M_1 b_1 \equiv 1 \pmod{4} \quad M_2 b_2 \equiv 1 \pmod{5} \quad M_3 b_3 \equiv 1 \pmod{7}$$

2. Let $x := 1 \cdot M_1 b_1 + 4 \cdot M_2 b_2 + 3 \cdot M_3 b_3$. (25 points)

(This is a variant of Problem 5 for Chapter 5 in the course notes.)

Problem 3: Prove that the system of congruences

$$x \equiv a_1 \pmod{m_1} \quad \text{and} \quad x \equiv a_2 \pmod{m_2}$$

can be solved if and only if (m_1, m_2) divides $a_1 - a_2$. Prove furthermore that the solution, when it exists, is unique modulo $m := [m_1, m_2]$. (25 points)
(This is Problem 6 (a) for Chapter 5 in the course notes.)

Problem 4: Suppose that we are given positive integers d and m with $d \mid m$ and that a is any number with $(a, d) = 1$. Prove that one can find a number a' with $(a', m) = 1$ and $a' \equiv a \pmod{d}$. (25 points)
(This is Problem 8 for Chapter 5 in the course notes.)

Due date: Monday, November 4, 2024. Write your solution on letter-sized paper, and write your name on your solution. Write down all necessary computations in full detail, and explain your computations in English, using complete sentences. Prove every assertion that you make in full detail. It is not necessary to copy down the problems again or to submit this sheet with your solution.