CSD2259 Tutorial 6

Some notes

- Solving $ax \equiv b \pmod{m}$ means giving solutions (in x) in one of the forms
  1. $x \equiv c \pmod{n}$, or
  2. $x = c + kn$ for $k \in \mathbb{Z}$
- To solve $ax \equiv b \pmod{m}$, we do following steps
  1. Check if b is divisible by $\gcd(a, m)$. If no, the equation has no solution. If yes, divide all terms of the equation by $\gcd(a, m)$ to get a new equation
  $$a_1 x \equiv b_1 \pmod{m_1}$$
  2. The solution is
  $$x \equiv a_1^{-1} b_1 \pmod{m_1} \Leftrightarrow x = a_1^{-1} b_1 + k m_1,$$
  where a_1^{-1} is the modular inverse of a_1 mod m_1.

Problem 1. The Bezout coefficients of two integers a, m are integers s, t such that $as + mt = \gcd(a, m)$. Using extended Euclidean algorithm, find the Bezout's coefficients of a and m in the following cases.

(a) $a = 34, m = 55$ (b) $a = 117, m = 213$ (c) $a = 3454, m = 4666$

Problem 2. Solve the linear congruence $ax \equiv b \pmod{m}$ in the following cases.
(a) $a = 34, m = 55, b = 3$
(b) $a = 117, m = 213, b = 5$
(c) $a = 3454, m = 4666, b = 2$
Remark: Use the results of Question 1.

Problem 3. Let m be a positive integer. The set of all possible remainders when dividing a number by m is $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

(a) How many integers $x \in \mathbb{Z}_{93}$ satisfies $36x \equiv 9 \pmod{93}$?
(b) Let a, b, m be positive integers. Put $d = \gcd(a, m)$ and assume $d \mid b$. Find the number of integers $x \in \mathbb{Z}_m$ which satisfies the equation

$$ax \equiv b \pmod{m}.$$

(c) Without actually solving, find out how many solutions x there are in the set $\mathbb{Z}_n$, where n is the modulo.

(i) $25x \equiv 2 \pmod{15}$ (ii) $25x \equiv 10 \pmod{15}$ (iii) $55x \equiv 121 \pmod{187}$

Problem 4. In this problem, we learn to solve system of linear congruences

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \end{cases}$$

To solve this system, we do the following

1. Solve the 1st equation $a_1x \equiv b_1 \pmod{m_1}$: Assume the solution is $x \equiv x_0 \mod k_1$, that is, $x = x_0 + yk_1$.
2. Replace $x = x_0 + yk_1$ into the 2nd equation $a_2x \equiv b_2 \pmod{m_2}$ to get an equation in y and solve for y.

As an application, solve the following system

$$\begin{cases} 2x \equiv 5 \pmod{9} \\ 16x \equiv 6 \pmod{70} \end{cases}$$

Hints and Instructions

1-2. Try it.
3b. Answer: $\gcd(a, m)$.
4. Answer: $x = 241 + 315k$ with $k \in \mathbb{Z}$.