2.3 Lecture 3

Preamble:In this lecture, we will discuss more than one linear congruences. Under certain conditions, we will show that such simultaneous congruences have a solution. We will also discuss the uniqueness of such a solution. For solving such congruences, there is a well-known method known as the Chinese Remainder Theorem.

Keywords: simultaneous congruences, Chinese Remainder Theorem

2.3.1 Simultaneous Linear Congruences

Consider the congruences

$$x \equiv 3 \text{ mod } 10, \qquad x \equiv 2 \text{ mod } 8.$$

Clearly, there is no common solution to both. The first one indicates that a solution x_0 must be an odd integer, as $x_0 - 3$ is divisible by 2, whereas the second one can have only even integers as solutions. On the other hand, the congruences

$$x \equiv 3 \text{ mod } 10, \qquad x \equiv 2 \text{ mod } 7$$

have a common solutions 23. We will now determine a sufficient condition for such congruences to have common solutions. We will also see when such a solution is unique. Note that in the second set of congruences, the moduli 10 and 7 are coprime. We will first show that when we have coprime moduli the simultaneous congruences will always have a solution.

2.3.2 Chinese Remainder Theorem

The following theorem is known as the Chinese Remainder Theorem. It gives us a sufficient condition for existence of a solution to simultaneous linear congruences.

THEOREM 2.13. *Consider the linear congruences*

$$\begin{array}{rcl} x & \equiv & a_1 \; mod \; m_1, \\ x & \equiv & a_2 \; mod \; m_2, \\ \vdots & & \vdots \\ x & \equiv & a_n \; mod \; m_n. \end{array}$$

If the m_i are pairwise coprime, then these congruences have a common solution. Further, such a common solution is unique modulo $M = m_1 \cdot \, \cdots \, \cdot m_n$.

Proof: Let us define n integers

$$M_i = \frac{M}{m_i} = m_1 \cdot \cdots \cdot m_{i-1} \cdot m_{i+1} \cdot \cdots \cdot m_n, \qquad 1 \leq i \leq n.$$

As m_i's are pairwise coprime, each M_i is coprime to the corresponding m_i. For each i $(1 \leq i \leq n)$, consider the linear congruence

$$M_i x \equiv 1 \bmod m_i.$$

As M_i and m_i are coprime, the above congruence has a solution. So there is an integer $\tilde{m}_i$ such that

$$M_i \tilde{m}_i \equiv 1 \bmod m_i.$$

We claim that

$$x_0 = a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n$$

satisfies all the given congruences in the theorem. Observe that

$$\begin{aligned} x_0 &= a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n \\ &\equiv a_i M_i \tilde{m}_i \bmod m_i \\ &\equiv a_i \bmod m_i. \end{aligned}$$

As for the uniqueness of common solutions, let x_1 be another common solution to the above system of linear congruences. Then, for each i, we have

$$x_1 \equiv a_i \equiv x_0 \bmod m_i \quad \Longrightarrow \quad m_i | (x_1 - x_0).$$

As the m_i's are coprime, we have

$$(m_1 \cdot \cdots \cdot m_n) | (x_1 - x_0) \quad \Longrightarrow \quad x_1 \equiv x_0 \bmod M. \qquad \square$$

Let us illustrate the method with the following example.

Exercise: Solve the following system of linear congruences

$$x \equiv 2 \bmod 6, \quad x \equiv 1 \bmod 5, \quad x \equiv 3 \bmod 7.$$

Solution: Observe that the moduli are pairwise coprime. Here,

$$M = 6.5.7 = 210, \qquad M_1 = 5 \cdot 7 = 35, \qquad M_2 = 6 \cdot 7 = 42, \qquad M_3 = 6 \cdot 5 = 30.$$

Now,

$$\begin{aligned} 35\tilde{m}_1 \equiv 1 \bmod 6 &\implies -\tilde{m}_1 \equiv 1 \bmod 6 &\implies \tilde{m}_1 \equiv 5 \bmod 6 \\ 42\tilde{m}_2 \equiv 1 \bmod 5 &\implies 2\tilde{m}_2 \equiv 1 \bmod 5 &\implies \tilde{m}_2 \equiv 3 \bmod 5 \\ 30\tilde{m}_3 \equiv 1 \bmod 7 &\implies 2\tilde{m}_3 \equiv 1 \bmod 7 &\implies \tilde{m}_3 \equiv -3 \bmod 7 \end{aligned}$$

Hence, by , we have a solution

$$x_0 = 2 \cdot 35 \cdot 5 + 1 \cdot 42 \cdot 3 + 3 \cdot 30 \cdot (-3) = 350 + 126 - 270 = 206.$$

The solution is unique modulo $M = 6 \cdot 5 \cdot 7 = 210$. $\square$

It may appear that the Chinese Remainder Theorem does not cover a general system of linear congruences with coprime moduli, as we have not really taken congruences of the type

$$b_i x \equiv a_i \bmod m_i, \quad 1 \leq i \leq n, \quad gcd(m_i, m_j) = 1 \text{ when } i \neq j.$$

But we can reduce a congruence of this form to a form considered in the above theorem, provided $gcd(b_i, m_i) = 1$. We know that $b_i c_i \equiv 1 \bmod m_i$ has a solution if and only if $gcd(b_i, m_i) = 1$. Then,

$$b_i x \equiv a_i \bmod m_i \Leftrightarrow x \equiv c_i a_i \bmod m_i,$$

and we obtain a linear congruence which is in the desired form so that the Chinese Remainder Theorem can be applied. Let us demonstrate this with an example:

Exercise: Solve the system of linear congruences

$$5x \equiv 1 \bmod 6, \quad 3x \equiv 2 \bmod 5, \quad 4x \equiv 5 \bmod 7.$$

Solution: Observe that each of the above congruences is solvable, for example, in the first one, 5 is coprime to 6. We have $5.5 \equiv 1 \bmod 6$, so we can multiply the first congruence by 5 to obtain $x \equiv 5 \bmod 6$. Similarly, we multiply the second congruence by 2 (as $3 \cdot 2 \equiv 1 \bmod 5$) to obtain $x \equiv 4 \bmod 5$. We multiply the the congruence above by 2 to obtain $x \equiv 10 \equiv 3 \bmod 7$. Thus, the given system is reduced to

$$x \equiv 5 \bmod 6, \quad x \equiv 4 \bmod 5, \quad x \equiv 3 \bmod 7.$$

Proceeding as in the previous example, we have

$$M = 6 \cdot 5 \cdot 7 = 210, \qquad M_1 = 5 \cdot 7 = 35, \qquad M_2 = 6 \cdot 7 = 42, \qquad M_3 = 6 \cdot 5 = 30.$$

and

$$\begin{aligned} 35\tilde{m}_1 \equiv 1 \bmod 6 \quad &\Longrightarrow \quad \tilde{m}_1 \equiv 5 \bmod 6 \\ 42\tilde{m}_2 \equiv 1 \bmod 5 \quad &\Longrightarrow \quad \tilde{m}_2 \equiv 3 \bmod 5 \\ 30\tilde{m}_3 \equiv 1 \bmod 7 \quad &\Longrightarrow \quad \tilde{m}_3 \equiv -3 \bmod 7 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 5 \cdot 35 \cdot 5 + 4 \cdot 42 \cdot 3 + 3 \cdot 30 \cdot (-3) = 875 + 504 - 270 = 1109 \equiv 59 \bmod 210.$$

The solution is unique modulo 210. $\square$