2.4 Lecture 4

Preamble: In this lecture, we will discuss a generalization of the Chinese Remainder Theorem. We will show how to solve a system of linear congruences even when the moduli are not pairwise coprime.

Keywords: non-coprime moduli

2.4.1 System of Congruences with Non-coprime Moduli

We have seen that the system of linear congruences congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 8$$

has no common solution. The first congruence can have only odd integers as solutions, whereas the second one has only even integers as solutions. On the other hand, consider the system of linear congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 1 \bmod 8.$$

We can verify that 33 is a common solution, and so is 73. We will now see under which conditions such congruences are guaranteed to have a common solution. We will also discuss whether such a solution is unique. Note that in the second set of congruences, the gcd of the two moduli divides $3 - 1$. We will first show that such a system of congruences will always have a solution if we have such a condition for each pair of moduli.

THEOREM 2.14. *Consider the linear congruences*

$$\begin{aligned} x &\equiv a_1 \ mod\ m_1, \\ x &\equiv a_2 \ mod\ m_2, \\ &\vdots \qquad \vdots \\ x &\equiv a_n \ mod\ m_n, \end{aligned}$$

where the moduli m_i's are not necessarily pairwise coprime. Let $d_{i,j} = gcd(m_i, m_j)$ for $i \neq j$. Then the above system has a simultaneous solution if and only if $d_{i,j}$ divides $(a_i - a_j)$ for all $i \neq j$. Further, such a solution is unique modulo $lcm(m_1, \cdots, m_n) = l$.

Proof: If a simultaneous solution exists, it is easy to show that $d_{i,j}$ divides $(a_i - a_j)$. Let x_0 be a common solution. Then for each pair $i \neq j$,

$$\begin{aligned} x_0 \equiv a_i \bmod m_i \quad &\Longrightarrow \quad m_i|(x_0 - a_i) \quad \Longrightarrow \quad d_{i,j}|(x_0 - a_i) \\ x_0 \equiv a_j \bmod m_j \quad &\Longrightarrow \quad m_j|(x_0 - a_j) \quad \Longrightarrow \quad d_{i,j}|(x_0 - a_j) \\ \Longrightarrow \quad d_{i,j}|[(x_0 - a_j) - (x_0 - a_i)] \quad &\Longrightarrow \quad d_{i,j}|(a_i - a_j). \end{aligned}$$

For the converse, we will show that the above system can be reduced to a system of linear congruences with coprime moduli, which definitely has a solution. First observe that if

$$m = p_1^{e_1}.p_2^{e_2}.\cdots.p_r^{e_r},$$

where p_k's are distinct primes, then $x \equiv a \bmod m$ if and only if $x \equiv a \bmod p_k^{e_k}$ for each p_k in the factorization of m. Now, suppose $d_{i,j}|(a_i - a_j)$ for all $i,\ j$. Let p be a prime factor of the lcm l of the moduli m_i's, and e be the highest p dividing l. Then p^e must divide one of the moduli, say it divides m_i. Let p^{e_j} be the highest power of p dividing m_j. Thus, in our notation $e = e_i$, and $e_j \leq e = e_i$. Now

$$x \equiv a_i \bmod p^{e_i} \implies x \equiv a_i \bmod p^{e_j}.$$

But $p^{e_j}|d_{i,j}$, and $d_{i,j}|(a_i - a_j)$, hence $a_i \equiv a_j \bmod p^{e_j}$, and

$$x \equiv a_i \bmod p^{e_i} \implies x \equiv a_i \bmod p^{e_j} \implies x \equiv a_j \bmod p^{e_j} \quad \forall j.$$

Thus, the given system will have a solution provided the system of linear congruences

$$x \equiv a_i \bmod p^{e_i},$$

for each prime p dividing l (where e_i is the highest power of p dividing l, occurring in the modulus m_i) has a solution. By the Chinese Remainder Theorem, the latter system has a solution.

Now we examine whether a common solution is unique. If x_0 and x_1 are two solutions of the given system, we will have

$$\begin{aligned} & x_1 \equiv a_i \equiv x_0 \bmod m_i \ \ \forall i \\ \Longrightarrow \quad & m_i|(x_1 - x_0) \ \ \forall i \\ \Longrightarrow \quad & lcm(m_1.\cdots.m_n)|(x_1 - x_0) \\ \Longrightarrow \quad & x_1 \equiv x_0 \bmod l. \end{aligned}$$

Therefore the solutions is unique modulo the lcm of the moduli. □

Let us illustrate the theorem with the following example.

Exercise: Solve the system of linear congruences

$$x \equiv 2 \bmod 12, \quad x \equiv 6 \bmod 10, \quad x \equiv 11 \bmod 45.$$

Solution: Observe that

$$gcd(12, 10)|(6 - 2), \quad gcd(10, 45)|(11 - 6), \quad gcd(12, 45)|(11 - 2).$$

By the above theorem, the given system will have a solution. Here, the lcm of 12, 10, 45 is $2^2 \cdot 3^2 \cdot 5 = 180$. Hence, the given system reduces to

$$x \equiv 2 \bmod 2^2, \quad x \equiv 6 \bmod 5, \quad x \equiv 11 \bmod 3^2.$$

For the above system with prime-power moduli which are pairwise coprime, we can apply Chinese Remainder Theorem with

$$M = 2^2 \cdot 3^2 \cdot 5 = 180 = l, \qquad M_1 = 5 \cdot 9, \qquad M_2 = 4 \cdot 9, \qquad M_3 = 4 \cdot 5.$$

Now,

$$\begin{aligned} 5 \cdot 9 \cdot \tilde{m}_1 \equiv 1 \bmod 4 \quad &\Longrightarrow \quad \tilde{m}_1 \equiv 1 \bmod 4 \\ 4 \cdot 9 \cdot \tilde{m}_2 \equiv 1 \bmod 5 \quad &\Longrightarrow \quad \tilde{m}_2 \equiv 1 \bmod 5 \\ 4 \cdot 5 \cdot \tilde{m}_3 \equiv 1 \bmod 9 \quad &\Longrightarrow \quad 2\tilde{m}_3 \equiv 1 \bmod 9 \Longrightarrow \quad \tilde{m}_3 \equiv -4 \bmod 9 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 2 \cdot (5 \cdot 9) \cdot 1 + 6 \cdot (4 \cdot 9) \cdot 1 + 11 \cdot (4 \cdot 5) \cdot (-4) = -574 \equiv 146 \bmod 180.$$

The solution is unique modulo 180. □