Lecture 31

Handout or Document Camera or Class Exercise

Theorem: [Chinese Remainder Theorem (CRT) If $\gcd(m_1, m_2) = 1$, then for any choice of integers a_1 and a_2, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem: (Generalized CRT (GCRT)) If $m_1, m_2, \ldots, m_k$ are integers and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, \ldots, a_k$, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}$$

Instructor's Comments: This is the 5 minute mark. Remark that the statement of CRT is not nearly as useful as understanding the proof.

Example: Solve

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod{11} \end{aligned}$$

From the first equation, $x = 5 + 6k$ for some $k \in \mathbb{Z}$. Plug this into the second equation gives

$$\begin{aligned} 5 + 6k &\equiv 2 \pmod 7 \\ 6k &\equiv -3 \pmod 7 \\ -k &\equiv -3 \pmod 7 \\ k &\equiv 3 \pmod 7 \end{aligned}$$

and hence $k = 3 + 7\ell$ for some $\ell \in \mathbb{Z}$. Therefore, $x = 5 + 6(3 + 7\ell) = 23 + 42\ell$. Therefore $x \equiv 23 \pmod{42}$. Now, we need to satisfy

$$\begin{aligned} x &\equiv 23 \pmod{42} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

Instructor's Comments: This is done so that students can see the reduction pattern that emerges.

Since $x = 23 + 42\ell$, plugging this into the final equation gives

$$\begin{aligned} 23 + 42\ell &\equiv 3 \pmod{11} \\ -2\ell &\equiv -20 \pmod{11} \\ \ell &\equiv 10 \pmod{11} \end{aligned}$$

By Congruences and Divisibility [CD] valid since $\gcd(-2, 11) = 1$

Hence, $\ell = 10 + 11m$ for some $m \in \mathbb{Z}$. Combining gives

$$x = 23 + 42\ell = 23 + 42(10 + 11m) = 443 + 462m$$

Therefore, $x \equiv 442 \pmod{462}$.

Instructor's Comments: This is the 20 minute mark.

Some twists to Chinese Remainder Problems: Example: Solve

$$\begin{aligned} 3x &\equiv 2 \pmod 5 \\ 2x &\equiv 6 \pmod 7 \end{aligned}$$

Instructor's Comments: The twist here is that the left hand sides are not just x but they have a coefficient.

Solution: Treat each congruence separately and solve using Linear Congruence Theorem 1 (LCT1). By inspection $x = 4$ solves the first congruence (could also use Linear Diophantine Equation techniques). Hence by LCT1, $x \equiv 4 \pmod{5/\gcd(3,5)}$ or $x \equiv 4 \pmod 5$. Similarly, notice that $x = 3$ is a solution to the second congruence. Hence by LCT1 again,

$x \equiv 3 \pmod{7/\gcd(2,7)}$. This is equivalent to $x \equiv 3 \pmod 7$. Thus, the above system is equivalent to solving

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

which can be solved like a typical Chinese Remainder Theorem problem.

Instructor's Comments: Don't do this in class - included only because I used to solve this this way.

Alternate Solution: Multiplying the first equation by 2 and the second equation by 4 gives

$$\begin{aligned} 6x &\equiv 4 \pmod 5 \\ 8x &\equiv 24 \pmod 7. \end{aligned}$$

Simplifying gives

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

Then proceed like a typical Chinese Remainder Theorem problem.

Example: Solve

$$\begin{aligned} x &\equiv 4 \pmod 6 \\ x &\equiv 2 \pmod 8 \end{aligned}$$

Instructor's Comments: The twist here is that the moduli are not coprime. Turns out that the engine that proves the Chinese Remainder Theorem is exactly what one needs to do here. Sometimes however there are no solutions and usually there are solutions but at a moduli smaller than the product.

Solution: Using the first equation gives $x = 4 + 6k$ for some $k \in \mathbb{Z}$. Plug this into the second equation gives

$$\begin{aligned} 4 + 6k &\equiv 2 \pmod 8 \\ 6k &\equiv -2 \pmod 8 \\ 6k &\equiv 6 \pmod 8 \end{aligned}$$

Now, note that $k = 1$ is definitely a solution. By LCT1, we have that

$$k \equiv 1 \pmod{8/(\gcd(6,8))}$$

gives all solution. Hence $k \equiv 1 \pmod 4$ and thus $k = 1 + 4\ell$ for some $\ell \in \mathbb{Z}$. Therefore,

$$x = 4 + 6(1 + 4\ell) = 10 + 24\ell$$

Therefore, $x \equiv 10 \pmod{24}$ gives the complete set of solutions.

Instructor's Comments: This is the 40 minute mark. Could even take your time and make this a full lecture if you wanted. We're reaching a catch up lecture if you have fallen behind.

Example: Solve $x^2 \equiv 34 \pmod{99}$.

This implies that $99 \mid (x^2-34)$. Note that $9 \mid 99$. Therefore $9 \mid (x^2-34)$ by transitivity, $x^2 \equiv 34 \pmod{9}$. Note further that $11 \mid 99$. Therefore, $11 \mid (x^2-34)$ by transitivity. this implies that

$$\begin{aligned} x^2 &\equiv 34 \pmod{11} \\ x^2 &\equiv 1 \pmod{11} \\ x^2 &\equiv \pm 1 \pmod{11} \end{aligned} \qquad \text{By trying all 11 possibilities}$$

Similarly, $x^2 \equiv 34 \equiv 7 \pmod{9}$ and so $x \equiv \pm 4 \pmod{9}$ (try all 9 possibilities).

This gives four systems of equations:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 4 \pmod{9} \end{aligned} \qquad \begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv -4 \pmod{9} \end{aligned}$$

$$\begin{aligned} x &\equiv -1 \pmod{11} \\ x &\equiv 4 \pmod{9} \end{aligned} \qquad \begin{aligned} x &\equiv -1 \pmod{11} \\ x &\equiv -4 \pmod{9} \end{aligned}$$

To finish solving this, we can use the Chinese Remainder Theorem 4 times to give the solutions

$$x \equiv 23, 32, 67, 76 \pmod{99}$$

This leads to the following theorem.

Theorem: Splitting the Modulus (SM) Let m and n be coprime positive integers. Then, for any integers x and a, we have

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv a \pmod{n} \end{aligned}$$

simultaneously if and only if $x \equiv a \pmod{mn}$.

Instructor's Comments: This is the 50 minute mark. If not, start the proof.