The Chinese Remainder Theorem

We now know how to solve a single linear congruence. In this lecture we consider how to solve systems of *simultaneous* linear congruences.

Example. We solve the system $2x \equiv 5 \pmod 7$; $3x \equiv 4 \pmod 8$ of two linear congruences (in one variable x). Multiply the first congruence by $2^{-1} \mod 7 = 4$ to get $4 \cdot 2x \equiv 4 \cdot 5 \pmod 7$. This simplifies to $x \equiv 6 \pmod 7$, so $x = [6]_7$ or $x = 6 + 7t$, where $t \in \mathbb{Z}$.

Now substitute for x in the second congruence: $3(6+7t) \equiv 4 \pmod 8$. This simplifies to $5t \equiv 2 \pmod 8$, which we solve by multiplying both sides by $5^{-1} \mod 8 = 5$ to obtain $t \equiv 2 \pmod 8$. So $t = [2]_8$ or $t = 2 + 8s$, where $s \in \mathbb{Z}$.

Substituting t back into x gives $x = 6 + 7(2 + 8s) = 20 + 56s$, which gives the solution $x = [20]_{56}$ or $x \equiv 20 \pmod{56}$. (Notice that $56 = 7 \cdot 8$.)

Example. Solve $4x \equiv 2 \pmod 6$; $3x \equiv 5 \pmod 8$.

Start by reducing the first congruence to $2x \equiv 1 \pmod 3$. Multiply both sides by 2 (an inverse of 2 mod 3) to solve it, which gives $x \equiv 2 \pmod 3$, so $x = 2 + 3t$.

Now substitute x into the second given congruence: $3(2 + 3t) \equiv 5 \pmod 8$. This simplifies to $t \equiv -1 \pmod 8$ or $t \equiv 7 \pmod 8$. So $t = 7 + 8s$.

Substituting t into the formula for x we obtain $x = 2+3(7+8s) = 23+24s$. So $x \equiv 23 \pmod{24}$. This is the complete solution. (Notice that 24 is the least common multiple of $6, 8$.)

The technique of the examples can always be used to solve simultaneous congruences when there is a solution.

There may be no solution, but the technique detects that as well.

Example. The system $x \equiv 3 \pmod 4$; $x \equiv 0 \pmod 6$ has *no solution.*

Solving the first congruence gives $x = 3 + 4t$, and substituting that into the second gives $3 + 4t \equiv 0 \pmod 6$ or $4t \equiv -3 \pmod 6$. This congruence has no solution, since $d = \gcd(4, 6)$ does not divide -3.

Actually, in this case there is a simpler way to see there is no solution. Just notice that the first congruence implies x is odd, but the second implies that x is even. That's a contradiction.

Systems that have no solution are said to be *inconsistent*.

Theorem (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_r$ be a collection of pairwise relatively prime integers. Then the system of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2, \cdots m_r$, for any given integers $a_1, a_2, \ldots, a_r$.

Proof of CRT. Put $M = m_1 \cdots m_r$ and for each $k = 1, 2, \ldots, r$ let $M_k = \frac{M}{m_k}$. Then $\gcd(M_k, m_k) = 1$ for all k. Let y_k be an inverse of M_k modulo m_k, for each k. Then by definition of inverse we have $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$

Then x is a simultaneous solution to all of the congruences. Since the moduli $m_1, \ldots, m_r$ are pairwise relatively prime, any two simultaneous solutions to the system must be congruent modulo M. Thus the solution is a unique congruence class modulo M, and the value of x computed above is in that class. □

Notice that the proof is constructive! Not only does it tell us why the theorem is true, it also gives an explicit *formula* for the solution.

Example. Find all integers x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.

We are asked to solve the system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{9} \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

Notice that the moduli are pairwise relatively prime, as required by the theorem. We have $M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$ and $M_1 = M/5 = 693$,

$M_2 = M/7 = 495$, $M_3 = M/9 = 385$, and $M_4 = M/11 = 315$. A small calculation gives $y_1 = 2$, $y_2 = 3$, $y_3 = 4$, and $y_4 = 8$. Hence $x = 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8 = 19056$. So $x = [19056]_M = [1731]_M$. In fact, 1731 is the smallest positive integer solution. The full solution is $x \equiv 1731 \pmod{M}$.

In the preceding example, in order to find y_k for $k = 1, 2, 3, 4$ we needed to invert $[693]_5 = [3]_5$, $[495]_7 = [5]_7$, $[385]_9 = [7]_9$, and $[315]_{11} = [7]_{11}$. The inverses can all (in this case) be guessed mentally. Notice carefully how we do not actually need to work with the large numbers M_k for $k = 1, 2, 3, 4$ in order to find the desired inverses!

This is another example of the useful fact that when doing modular problems, we can always replace any integer by any other integer in its congruence class.

We can also solve other systems by the Chinese remainder theorem. For example, verify that the system $2x \equiv 5 \pmod{7}$; $3x \equiv 4 \pmod{8}$ is equivalent to the simpler system

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

By solving this by the Chinese remainder theorem, we also solve the original system. (The solution is $x \equiv 20 \pmod{56}$.)

Of course, the formula in the proof of the Chinese remainder theorem is not the only way to solve such problems; the technique presented at the beginning of this lecture is actually more general, and it requires no memorization. Nevertheless, the formula in the proof of the Chinese remainder theorem is sometimes convenient.