## Systems of Linear Congruences

A general system of simultaneous linear congruences

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_r x &\equiv b_r \pmod{n_r} \end{aligned}$$

can be simplified to the form

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

by dividing each congruence through by $(a_i, n_i)$, then multiplying by the inverse mod $m_i = \frac{n_i}{(a_i, n_i)}$ of the coefficient $\frac{a_i}{(a_i, n_i)}$. The simplified system may or may not be solvable, but in any case, it must have the same set of solutions as the original system.

*Example*: The system

$$x \equiv 8 \pmod{12}$$
$$x \equiv 6 \pmod{9}$$

has no solutions, since the first congruence implies that $x \equiv 8 \equiv 2 \pmod{3}$, but the second implies that $x \equiv 6 \equiv 0 \pmod{3}$, and these are incompatible with each other.

*Example*: The system

$$x \equiv 8 \pmod{12}$$
$$x \equiv 6 \pmod{13}$$

is solvable, since the first congruence is equivalent to the condition that $x = 12k + 8$ for some integer $k$, and substituting this into the second congruence yields $12k \equiv -2 \pmod{13}$, or $-k \equiv -2 \pmod{13}$, which simplifies to $k \equiv 2 \pmod{13}$. Thus $k = 13l + 2$ for some integer $l$, so $x = 12(13l + 2) + 8 = 156l + 32$. That is, the system is solved for all $x$ that satisfy $x \equiv 32 \pmod{156}$.

These examples illustrate that the relationship between the moduli of the congruences is the most important condition that determines the solvability of a system of linear congruences. This was first discovered by ancient Chinese mathematicians and was first written down in the *Shushu Jiuzhang*

(*Nine Chapters on the Mathematical Arts*) written by the 13th century mathematician Qin Jiushao.

**Chinese Remainder Theorem** Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime moduli. Then the system of congruences

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo the product $m = m_1 m_2 \cdots m_r$.

**Proof** Let $M_i = \dfrac{m}{m_i}$. Since the $m_i$ are pairwise relatively prime, $(M_i, m_i) = 1$. Therefore, for each $i$ we can solve the congruences $M_i x \equiv 1 \pmod{m_i}$ to compute the inverses of the $M_i \bmod m_i$. Then $x \equiv c_1 M_1 M_1^{-1} + c_2 M_2 M_2^{-1} + \cdots + c_r M_r M_r^{-1} \pmod{m}$ solves the system since

$$\begin{aligned} c_1 M_1 M_1^{-1} + c_2 M_2 M_2^{-1} + \cdots + c_r M_r M_r^{-1} &\equiv c_i M_i M_i^{-1} \pmod{m_i} \\ &\equiv c_i \cdot 1 \pmod{m_i} \\ &\equiv c_i \pmod{m_i} \end{aligned}$$

The solution is unique because if $x$ and $y$ are two solutions to the system, then for all $i$, $x \equiv y \pmod{m_i}$ $\Rightarrow m_i \mid (x-y)$, and since the $m_i$ are pairwise relatively prime, it follows that $m \mid (x-y)$, or $x \equiv y \pmod{m}$. //

The proof of the theorem also suggests a speedy algorithm for computing a solution to the system. We illustrate with our previous example:

| | $c$ | $M$ | $M^{-1}$ | $cMM^{-1}$ |
|---|---|---|---|---|
| $x \equiv 8 \pmod{12}$ | 8 | 13 | 1 | 104 |
| $x \equiv 6 \pmod{13}$ | 6 | 12 | –1 | –72 |
| | | | | $x \equiv 32 \pmod{156}$ |

The case of the general system can now be handled.

**Theorem** The system of linear congruences

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

has a solution iff for all $i \neq j$, $c_i \equiv c_j \pmod{(m_i, m_j)}$. The solution, if it exists, is unique $\bmod [m_1 m_2 \cdots m_r]$.

**Proof** Consider the case $r = 2$ first. If the system of congruences has a solution $x = c$, then we can write

$$\begin{aligned} c &\equiv c_1 \pmod{m_1} \\ c &\equiv c_2 \pmod{m_2} \end{aligned} \Rightarrow \begin{aligned} c &= km_1 + c_1 \\ c &= lm_2 + c_2 \end{aligned}$$

for certain integers $k$, $l$. Then $c_1 - c_2 = lm_2 - km_1$, so $(m_1, m_2) \mid (c_1 - c_2) \Rightarrow c_1 \equiv c_2 \pmod{(m_1, m_2)}$.

Conversely, suppose $c_1 \equiv c_2 \pmod{(m_1, m_2)}$. If we write the prime factorizations of the two moduli in the form

$$m_1 = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}, \; m_2 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

with $d_i, e_i \geq 0$, then by the CRT, the system

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

is equivalent to the system

$$\begin{aligned} &x \equiv c_1 \pmod{p_1^{d_1}}, x \equiv c_1 \pmod{p_2^{d_2}}, \ldots, x \equiv c_1 \pmod{p_k^{d_k}} \\ &x \equiv c_2 \pmod{p_1^{e_1}}, x \equiv c_2 \pmod{p_2^{e_2}}, \ldots, x \equiv c_2 \pmod{p_k^{e_k}} \end{aligned}$$

Consider the first congruence in each of the two lines above; if $d_1 \geq e_1$, then by our assumption, $c_1 \equiv c_2 \pmod{p_1^{e_1}}$, so the second congruence $x \equiv c_2 \pmod{p_1^{e_1}}$ is redundant with respect to the first congruence $x \equiv c_1 \pmod{p_1^{d_1}}$ and we can discard the second congruence. Doing the same for the other prime power moduli, we can discard all the congruences whose moduli are the smaller of the two powers of the prime that appears and retain the congruences whose moduli are the larger of the two powers. Finally, again using the CRT, we can solve the remaining system and obtain a unique solution modulo $[m_1, m_2]$.

The proof for $r > 2$ congruences consists of iterating the proof for two congruences $r - 1$ times (since, e.g., $([m_1, m_2], m_3) = 1$). //

*Example*: To solve

$$x \equiv 3 \pmod{8}$$
$$x \equiv 7 \pmod{12}$$
$$x \equiv 4 \pmod{15}$$

note first that $(8,12) \mid (7 - 3)$, $(8,15) \mid (4 - 3)$, and $(12,15) \mid (7 - 4)$, so the system is solvable. Split the moduli into prime powers:

$$x \equiv 3 \pmod 8$$
$$x \equiv 7 \equiv 3 \pmod 4, x \equiv 7 \equiv 1 \pmod 3$$
$$x \equiv 4 \equiv 1 \pmod 3, x \equiv 4 \pmod 5$$

then discard the redundant congruences:

$$x \equiv 1 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 3 \pmod 8$$

The resulting system has relatively prime moduli, so the CRT method applies:

| $c$ | $M$ | $M^{-1}$ | $cMM^{-1}$ |
|---|---|---|---|
| 1 | $40 \equiv 1 \pmod 3$ | 1 | 40 |
| 4 | $24 \equiv -1 \pmod 5$ | –1 | –96 |
| 3 | $15 \equiv -1 \pmod 8$ | –1 | –45 |

whence the final solution is $x \equiv -101 \equiv 19 \pmod{120}$.