Systems of Linear Congruences

First we consider 2 equations in 2 variables and with the same modulus.
The method of solving is similar to that of solving equations
We learn it through examples.

ex: Solve the system

$$3x+4y \equiv 5 \pmod{13} \quad — (1)$$
$$2x+5y \equiv 7 \pmod{13}. \quad — (2)$$

(1) $\times 5$ and (2) $\times 4$ give

$$15x+20y \equiv 25 \pmod{13} \quad — (3)$$
$$8x+20y \equiv 28 \pmod{13} \quad — (4)$$

Subtract (4) from (3) to get

$$7x \equiv -3 \pmod{13}$$

Multiply by $\overline{7} = 2 \pmod{13}$ to get

$$2\times 7x \equiv 2\times(-3) \pmod{13}$$

$$\Rightarrow x \equiv -6 \pmod{13}$$
$$\Rightarrow x \equiv 7 \pmod{13}$$

Similarly, we can get

$$y \equiv 9 \pmod{13}.$$

We need to substitute these solutions in the original congruences and check whether they are actually solutions.

We see that,

$$3x + 4y \equiv 3 \times 7 + 4 \times 9 \equiv 57 \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 2 \times 7 + 5 \times 9 \equiv 59 \equiv 7 \pmod{13}$$

Hence, the solutions are given by

$$x \equiv 7 \pmod{13}$$
$$y \equiv 9 \pmod{13}.$$

This method is generalized in the following theorem.

<u>Theorem 4.16:</u> Let $a, b, c, d, e, f, m \in \mathbb{Z}$ with $m > 0$. Suppose $\gcd(\Delta, m) = 1$ where $\Delta = ad - bc$. Then, the system of congruences

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

has a unique solution modulo m, given by

$$x = \bar{\Delta}(de - bf) \pmod{m}, \quad y = \bar{\Delta}(af - ce) \pmod{m}$$

where $\bar{\Delta}$ is an inverse of Δ modulo m.

Proof: Exercise

ex: Let's solve

$$4x + y \equiv 3 \pmod 7$$
$$3x + 2y \equiv 2 \pmod 7$$

using the theorem.

We've $\Delta = 4\times 2 - 1\times 3 = 5$

and $\gcd(5,7) = 1$.

$\therefore$ a unique solution exists.

We get $\overline{\Delta} = \overline{5} \equiv 3 \pmod 7$

$$\therefore \quad x \equiv 3(2\times 3 - 1\times 2) \equiv 12 \equiv 5 \pmod 7$$
$$y \equiv 3(4\times 2 - 3\times 3) \equiv -3 \equiv 4 \pmod 7$$

are the solutions.