Let x_1, x_2 be two solutions of the congruence $ax \equiv b \pmod m$

Then $ax_1 \equiv b \pmod m$ and $ax_2 \equiv b \pmod m$

This implies $ax_1 \equiv ax_2 \pmod m \Rightarrow x_1 \equiv x_2 \pmod m$, since $\gcd(a, m) = 1$

This proves that the linear congruence $ax \equiv b \pmod m$ has a unique solution.

Note: The solutions are $x = bu + \lambda m$ where $\lambda = 0, \pm 1, \pm 2, \ldots$ and they all belong to one and only one residue class modulo m or one congruence class modulo m.

Theorem 2.5.6 If $\gcd(a, m) = d$, then the linear congruence $ax \equiv b \pmod m$ has no solution if d is not a divisor of b.

If d be a divisor of b, then the linear congruence $ax \equiv b \pmod m$ has d incongruent solutions $\pmod m$

Proof: Let $ax \equiv b \pmod m$ has a solution $x = u$.

Then $au \equiv b \pmod m$ and this implies $m \mid (b - au)$.

$d \mid m \Rightarrow d \mid b - au$. $d \mid a$ and $d \mid (b - au) \Rightarrow d$ is a divisor of b.

Contrapositively, d is not a divisor of b implies $ax \equiv b \pmod m$ has no solution.

Second part: $d \mid b$. For an integer u, $au \equiv b \pmod m$ holds if and only if $\frac{a}{d}u \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, by Theorem 2.5.4.

$\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ and therefore the congruence

$\frac{a}{d}u \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ has just one solution $u \equiv x_1 \pmod{\frac{m}{d}}$,

In other words, the solution of the congruence $\frac{a}{d}u \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ are the integers $u \equiv x_1 \pmod{\frac{m}{d}}$, i.e., $u = x_1 + \frac{m}{d}t$, $t = 0, \pm 1, \pm 2, \ldots$

If t assumes the values $0, 1, 2, \ldots, d-1$, then u assumes d values

$$x_1,\ x_1 + \frac{m}{d},\ x_1 + \frac{2m}{d},\ \ldots,\ x_1 + \frac{(d-1)m}{d} \quad \ldots \text{(i)}$$

We now show that the integers in the list (i) are incongruent modulo m, while each of all other solutions (corresponding to the values of t other than $0, 1, \ldots, d-1$) is congruent to some one of the integers in (i).

$x_1 + t_1\frac{m}{d} \equiv x_1 + t_2\frac{m}{d} \pmod{m}$, where $0 \le t_1 < t_2 \le d-1$ gives

$$t_1\frac{m}{d} \equiv t_2\frac{m}{d} \pmod{m}$$

$$\gcd\left(\frac{m}{d}, m\right) = \frac{m}{d} \Rightarrow t_1 \equiv t_2 \pmod{d} \Rightarrow d \mid t_2 - t_1.$$

This is an impossibility because, $0 < t_2 - t_1 < d$

Thus all solutions in the list (i) are incongruent modulo m.

Let any other solution be $x_1 + t_j\frac{m}{d}$, where t_j is an integer other than $0, 1, \ldots, d-1$. By division algorithm, we can write $t_j = qd + r$ where q and r are integers and $0 \le r \le d-1$

Then $x_1 + t_j\frac{m}{d} = x_1 + (qd+r)\frac{m}{d} \equiv x_1 + r\frac{m}{d} \pmod{m}$

Since $0 \le r \le d-1$, $x_1 + t_j\frac{m}{d}$ is one of the solutions listed in (i)

Thus the congruence $ax \equiv b \pmod{m}$ has d incongruent solutions listed in (i)

This completes the proof.

Note: The solutions belong to a single residue class or congruent class modulo $\frac{m}{d}$ and this is the union of d distinct residue classes modulo m. The residue class $\overline{i}$ modulo $\frac{m}{d}$ is the union of d distinct residue classes

$\overline{i}, \overline{i+\frac{m}{d}}, \overline{i+2\frac{m}{d}}, \ldots, \overline{i+\frac{(d-1)m}{d}}$ modulo m.

Worked examples

1. Solve the linear congruence $5x \equiv 3 \pmod{11}$

Solution: $\gcd(5, 11) = 1$. Hence the congruence has a unique solution. Since $\gcd(5,11) = 1$, there exists integer u, v such that $5u + 11v = 1$. Here we take $u = -2$ and $v = 1$. So, $5(-2) + 11 \cdot 1 = 1$ and this implies

$5 \cdot (-2) \equiv 1 \pmod{11}$. So, $5 \cdot (-6) \equiv 3 \pmod{11}$

Hence $x = -6$ is a solution.

All solutions are $x \equiv -6 \pmod{11}$, i.e., $x \equiv 5 \pmod{11}$

All the solutions are congruent to 5 (mod 11) and therefore the given congruence has a unique solution.

2. Solve the linear congruence $2x \equiv 5 \pmod{6}$

Solution: $\gcd(2, 6) = 2$ and 2 does not divide 5. So, by Theorem 2.5.6,

$2x \equiv 5 \pmod{6}$ has no solutions.

3. Solve the linear congruence $15x \equiv 9 \pmod{18}$

Solution: $\gcd(15, 18) = 3$ and $3 \mid 9$. Therefore the given congruence has a solution. The given congruence is equivalent to $5x \equiv 3 \pmod 6$.

$\gcd(5, 6) = 1$. Hence the congruence $5x \equiv 3 \pmod 6$ has a unique solution.

Since $\gcd(5, 6) = 1$, there exists integers u, v such that $5u + 6v = 1$. Here we take $u = -1$, $v = 1$

So, $5(-1) + 6.1 = 1$ and this implies

$5(-1) \equiv 1 \pmod 6$. So, $5.(-3) \equiv 3 \pmod 6$. Hence $x = -3$ is a solution of the congruence $5x \equiv 3 \pmod 6$.

There are three incongruent solutions of the given congruence. They are $x = -3, -3+6, -3+12$ modulo 18, i.e.,

$x \equiv -3, 3, 9 \pmod{18}$.

4. Solve the congruence $12x \equiv 9 \pmod{15}$

Solution: Since $\gcd(12, 15) = 3$ and $3 \mid 9$, the congruence $12x \equiv 9 \pmod{15}$ ... (1)

has exactly three solutions.

Now $3 = 12(-1) + 15(1)$. Then $9 = 12(-3) + 15(3)$

Accordingly, we have $12(-3) \equiv 9 \pmod{15}$ and hence $x_0 = -3$ is a solution of $12x \equiv 9 \pmod{15}$. Therefore the three solutions corresponding to the congruence (1) is given by $x \equiv (-3 + (\frac{15}{3})i) \pmod{15}$, $i = 0, 1, 2$