Let a be an arbitrary integer. Upon division by m, a leaves one and only one of the integers $0, 1, 2, \ldots, m-1$ as the remainder

The whole set of integers is divided into m distinct and disjoint subsets, called the residue classes modulo m, denoted by $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}$ and defined by

$$\bar{0} = \{0, \pm m, \pm 2m, \cdots\}$$
$$\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \cdots\}$$
$$\bar{2} = \{2, 2 \pm m, 2 \pm 2m, \cdots\}$$
$$\cdots \quad \cdots \quad \cdots$$
$$\overline{(m-1)} = \{m-1, (m-1) \pm m, (m-1) \pm 2m, \cdots\}$$

Any two integers in a ~~set~~ residue classes are congruent modulo m and any two integers belonging to two different residue classes are ~~not~~ incongruent modulo m.

Theorem 2.5.2 If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$ for all positive integers n.

Proof: We use the principle of mathematical induction to prove the theorem.

The theorem is true for $n = 1$ as $a \equiv b \pmod m$

Let us assume that the theorem is true for some positive integer k.

Then $a^k \equiv b^k \pmod m$

Now $a^k \equiv b^k \pmod m$ and $a \equiv b \pmod m$ together imply that

$a^k \cdot a = b^k \cdot b \pmod m$, i.e., $a^{k+1} \equiv b^{k+1} \pmod m$

This shows that the theorem is true for the positive integer $k+1$ if we assume it to be true for k.

By the principle of mathematical induction, the theorem is true for all positive integers n

Note. The converse of the theorem fails to hold.

As for example $9^2 \equiv 7^2 \pmod 8$ but $9 \not\equiv 7 \pmod 8$

Theorem 2.5.3 If $ax \equiv ay \pmod m$ and a is prime to m then $x \equiv y \pmod m$

Proof: $ax - ay = km$ where k is an integer

or, $x - y = \frac{km}{a}$

Since $x-y$ is integer $a \mid km$. Since a is prime to m and $a \mid km$, it shows that $a \mid k$. So, $k = aq$, q is an integer. Hence $x - y = qm$ and

so, $x \equiv y \pmod m$

Note $ax \equiv ay \pmod m$ does not necessarily imply

$x \equiv y \pmod m$

For example, $3 \cdot 2 \equiv 3 \cdot 4 \pmod 6$

does not imply $2 \equiv 4 \pmod 6$

We can cancel the common factor a freely from both sides of the congruence $\pmod m$ provided a is prime to m.

Cancellation is allowed however, in some restricted sense which is provided in the following theorem.

Theorem 2.5.4 If $d = \gcd(a, m)$, then

$$ax \equiv ay \pmod{m} \iff x \equiv y \pmod{\frac{m}{d}}$$

Proof: Let $ax \equiv ay \pmod{m}$. So, $ax - ay = qm$, q is an integer. Since $\gcd(a,m) = d$, $a = dr$ and $m = ds$ where r and s are integers prime to each other.

So, $dr x - dr y = qds$

or, $x - y = \frac{qs}{r}$

Since $x-y$ is an integer, $r \mid qs$. r is prime to s and $r \mid qs$ implies $r \mid q$, i.e., $\frac{q}{r}$ is an integer k.

So, $x - y = ks$ and so, $x \equiv y \pmod{\frac{m}{d}}$ as $s = \frac{m}{d}$

Conversely, $x \equiv y \pmod{\frac{m}{d}} \Rightarrow \frac{m}{d} \mid (x-y)$

$\Rightarrow m \mid d(x-y) \Rightarrow m \mid a(x-y) \Rightarrow ax \equiv ay \pmod{m}$

Corollary: If $ax \equiv ay \pmod{m}$ and $a \mid m$ then $x \equiv y \pmod{\frac{m}{a}}$

Definition: A congruence of the form

$$ax \equiv b \pmod{m} \quad \ldots (1)$$

where a, b are integers, m is a positive integer and x is an unknown integer, is called a linear congruence in one variable x. An integer x_0 is called a solution of (1) if $ax_0 \equiv b \pmod{m}$

Example $2x \equiv 1 \pmod 5$ is a linear congruence in one variable. Since $2 \cdot 3 \equiv 1 \pmod 5$ we find that 3 is a solution of this congruence. Now $8 \equiv 3 \pmod 5$. we find that 8 is also a solution of $2x \equiv 1 \pmod 5$. In fact, we can show that if x_0 is an integer such that $x_0 \equiv 3 \pmod 5$ i.e., x_0 is a member of the congruence class $\bar{3}$ modulo 5 (or residue class $\bar{3}$ modulo 5), then x_0 is a solution of the congruence.

Let $ax \equiv b \pmod m$ be a linear congruence. Suppose x_0 is a solution of $ax \equiv b \pmod m$. Then $ax_0 \equiv b \pmod m$. Suppose $x_1 \equiv x_0 \pmod m$. Then $ax_1 \equiv ax_0 \pmod m$. Hence $ax_1 \equiv b \pmod m$. So, we find that x_1 is also a solution of this congruence. Hence any member of the congruence class $\overline{x_0}$ is a solution. Therefore, for a given linear congruence $ax \equiv b \pmod m$, we like to know how many of the m congruence classes modulo m will be the solution of the given congruence.

Theorem 2.5.5 Let a, b and m be integers with $m > 0$ and $\gcd(a, m) = 1$. Then the congruence $ax \equiv b \pmod m$ has a unique solution.

Proof: Since $\gcd(a,m) = 1$, $\exists$ integers u and v such that $au + mv = 1 = 1$. So, $a(bu) + m(bv) = b$. This gives $a(bu) \equiv b \pmod m$. This shows that $x = bu$ is a solution of the congruence $ax \equiv b \pmod m$.