Congruence

Lakshmy K V

March 30, 2022

Congruence

DEFINITION 2.1. *Let n be any non-zero integer. Define a relation*

$$\equiv \ mod\ n$$

on $\mathbb{Z}$ by

$$a \equiv b \ mod\ n \ if\ and\ only\ if\ n \mid (a-b).$$

For example,

$$12 \equiv 3 \bmod 9, \qquad 31 \equiv 6 \bmod 5.$$

Proposition 2.2. *The relation '$\equiv$ modulo n' is an equivalence relation.*

1. reflexive (i.e., every integer is related to itself),
2. symmetric (i.e., if a is related to b then b is related to a), and
3. transitive (i.e., if a is related to b, and b is related to c, then a is related to c).

Now,

- $a \equiv a$ modulo n $\forall a \in \mathbb{Z}$ as $n \mid (a - a)$.
- $a \equiv b$ modulo n implies $b \equiv a$ modulo n as
$$n \mid (a - b) \implies n \mid (b - a) \ \ \forall a, b \in \mathbb{Z}.$$
- $a \equiv b$ modulo n and $b \equiv c$ modulo n imply $a \equiv c$ modulo n, as
$$n \mid (a - b), \qquad n \mid (b - c) \implies n \mid \left[(a - b) + (b - c)\right] \qquad \forall a, b, c \in \mathbb{Z}. \qquad \square$$

Definition 2.3. *The equivalence class of an integer a, denoted by $[a]$, is referred to as the congruence class or residue class of a. Thus,*

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \ mod \ n\}.$$

It is enough to consider positive modulus, as

$$n \mid (a - b) \Leftrightarrow (-n) \mid (a - b).$$

Henceforth we will consider n to be a positive integer.

Proposition 2.4. *$a \equiv b$ mod n if and only if they leave the same remainder upon division by n.*

Corollary 2.5. *If a leaves the remainder r upon division by n then a and r are in the same congruence class modulo n, i.e., $[a] = [r]$.*

Corollary 2.6. *For any integer n, there are n distinct congruence classes modulo n.*

Proof: The only possible remainders upon division by n are $0, 1, \cdots, n-1$. So any integer a must be congruent to one of these n remainders. So the number of congruence classes is not more than n. Any two distinct remainders in the above list can not be equivalent by proposition 2.4. Hence the corollary follows. $\square$.

Definition 2.7. *A set of congruence classes is called a complete residue system if any given integer belongs to one of the congruence classes in the set.*

Thus, the set $\{[0], [1], \cdots, [n-1]\}$ is an example of a complete residue system for n. This complete residue system of n is usually denoted by $\mathbb{Z}_n$.

Properties of Congruence

Congruence modulo n has many interesting properties which simplify a lot of computations. Some of these properties are listed below.

1. $x \equiv y \bmod n \implies x + c \equiv y + c \bmod n \ \ \forall c \in \mathbb{Z}.$
2. $x \equiv y \bmod n, \ \ z \equiv w \bmod n \implies xz \equiv yw \bmod n \ \ \forall c \in \mathbb{Z}.$
3. $x \equiv y \bmod n \implies cx \equiv cy \bmod n \ \ \forall c \in \mathbb{Z}.$
4. $x \equiv y \bmod n \implies x^k \equiv y^k \bmod n \ \ \forall k \in \mathbb{N}.$
5. $x \equiv y \bmod n \implies f(x) \equiv f(y) \bmod n$ for any polynomial $f(x)$ with integer coefficients.
6. $x \equiv y \bmod n \implies x \equiv y \bmod d$ for any divisor d of n.
7. $ax \equiv ay \bmod n \implies x \equiv y \bmod \frac{n}{gcd(a,n)}.$
8. $ax \equiv ay \bmod n \implies x \equiv y \bmod n$ if $gcd(a, n) = 1$.
9. $x \equiv y \bmod m_i \implies x \equiv y \bmod lcm(m_i)$ for positive integers $m_1. \cdots, m_r$.

The first of the above properties follow easily from definition of congruence. Observe that $a \equiv b \bmod n$ implies that we can write as $a = b + nk$ for some integer k. For the second property above,

$$x = y + nk,\ z = w + nl \implies xz = yw + n(yl + kw + nkl) \equiv yw \bmod n.$$

The third property follows from the second by taking $z = w = c$. The fourth property follows from the second by taking $z = x$, $w = y$ to start with, then $z = x^2$, $w = y^2$ etc. Then the fifth is a consequence of the preceding properties. The sixth property is clear too, as

$$d \mid n, \;\; n \mid (a-b) \implies d \mid (a-b).$$

For the seventh property, we cancel the gcd d of $n = dn_1$ and $a = da_1$ to obtain

$$\begin{aligned} n &\mid a(x-y) \\ \implies n_1 &\mid a_1(x-y) \\ \implies n_1 &\mid (x-y). \end{aligned}$$

As n_1 and a_1 are coprime

The last property follows from the definition of the lcm.

PROPOSITION 2.8. *A natural number is divisible by 9 (respectively by 3) if and only if the sum of its digits in its decimal expansion is divisible by 9 (respectively by 3).*

Proof: Let m be a natural number whose decimal expansion is

$$m = b_k \cdot 10^k + b_{k-1} \cdot 10^{k-1} + \cdots + b_1 \cdot 10 + b_0, \qquad 0 \leq b_i < 10.$$

and let

$$S = b_k + b_{k-1} + \cdots + b_1 + b_0,$$

Now,

$$\begin{aligned} 10 &\equiv 1 \bmod 9 \\ \implies 10^k &\equiv 1 \bmod 9 \\ \implies b_k \cdot 10^k + b_{k-1} \cdot 10^{k-1} + \cdots + b_1 \cdot 10 + b_0 &\equiv b_k + b_{k-1} + \cdots + b_1 + b_0 \bmod 9 \\ \implies m &\equiv S \bmod 9. \end{aligned}$$

Thus $9 \mid m$ if and only if $9 \mid S$. The proof for divisibility by 3 is identical. $\square$

Proposition 2.9. *A positive integer is divisible by* 11 *if and only if the sum of its digits with alternate signs in its decimal expansion is divisible by* 11*.*

Proof: Let m be an integer whose decimal expansion is

$$m = b_k \cdot 10^k + b_{k-1} \cdot 10^{k-1} + \cdots + b_1 \cdot 10 + b_0, \qquad 0 \leq b_i < 10.$$

and let

$$A = (-1)^k b_k + (-1)^{k-1} b_{k-1} + \cdots - b_1 + b_0. \text{ Now,}$$

$$\begin{aligned} 10 &\equiv -1 \bmod 11 \\ \Longrightarrow \quad 10^k &\equiv (-1)^k \bmod 11 \\ \Longrightarrow \quad b_k \cdot 10^k + b_{k-1} \cdot 10^{k-1} + \cdots + b_1 \cdot 10 + b_0 &\equiv (-1)^k b_k + (-1)^{k-1} b_{k-1} + \cdots - b_1 + b_0 \bmod 11 \\ \Longrightarrow \quad m &\equiv A \bmod 11. \end{aligned}$$

Thus $11 \mid m$ if and only if $11 \mid A$. $\square$