

When using arithmetic modulo m , only the remainder r is kept. Two mathematical notations that are used for this are

$$r = R_m(n), \quad \text{“}r \text{ is remainder of } n \text{ when divided by } m\text{”},$$

and

$$r \equiv n \pmod{m}, \quad \text{“}r \text{ is congruent to } n \text{ modulo } m\text{”}.$$

Since the remainder of a division by m is always in the set $\{0, 1, 2, \dots, m-1\}$, this yields a **finite number system** for which the operations of addition and multiplication are defined as **addition and multiplication modulo m** .