Chapter 4: CONGRUENCES AND THE INTEGERS MODULO n

Mphako-Banda

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF MATHEMATICS

LEARNING OUTCOMES FOR THE LECTURE

By the end of this lecture, students will be able to:

- define a multiplicative inverse in $\mathbb{Z}_n$
- state whether or not $\overline{a}$ in $\mathbb{Z}_n$ has an inverse using gcd(a,n)
- find the inverse of $\overline{a}$ in $\mathbb{Z}_n$ if it has one
-
-

DEFINITION For a modulus $n \geq 2$ and an integer a, a residue class $\overline{b}$ in $\mathbb{Z}_n$ is called a multiplicative inverse of $\overline{a}$ if $\overline{b}.\overline{a} = \overline{1} = \overline{a}.\overline{b}$ in $\mathbb{Z}_n$.

REMARK: If $\overline{a}$ has an inverse, it is unique.

Note: Not all elements in $\mathbb{Z}_n$ have a multiplicative inverse.

Summary of inverses in $\mathbb{Z}_n$:

The additive inverse of $\overline{a}$ is $\overline{-a} = \overline{n\text{-}a}$ (See Thm 4.2.4 part iv in slide 10)

The multiplicative inverse of $\overline{a}$ is defined above...

Theorem (4.2.6) (the condition to check if an element has an inverse)

Let $a, n \in \mathbb{Z}$, and $n \geq 2$. Then $\bar{a}$ has inverse in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$.

PROOF:

$\Rightarrow$

say $\bar{b} \in \mathbb{Z}_n$ such that $\bar{a}\bar{b} = \bar{1}$. (say the inverse exists, then there is a $\bar{b}$ that satisfies the condition)

$$\boxed{\Rightarrow} \quad \bar{a}\bar{b} = \bar{1} \overset{1}{\Rightarrow} \overline{ab} = \bar{1} \overset{2}{\Rightarrow} ab \equiv 1 \pmod{n}$$
$$\overset{3}{\Rightarrow} ab - 1 = kn, \qquad k \in \mathbb{Z}$$
$$\overset{4}{\Rightarrow} ab - kn = 1, \qquad k, a, b, n \in \mathbb{Z}$$
$$\overset{5}{\Rightarrow} \gcd(a, n) = 1. \text{ by Theorem 2.4.2}$$

(what are the reasons to justify each implication ?)

reasons - 1 (residue class of a product) 2 (equality of residue classes) 3 (defn of congruence mod n) 4 (properties of integers) 5 (theorem 2.4.2)

$\boxed{\Leftarrow}$

say $\gcd(a, n) = 1$. Then $\exists p, q \in \mathbb{Z}$ such that $ap + nq = 1$ by Theorem 2.4.2.

Thus $ap - 1 = (-q)n, \quad -q \in \mathbb{Z}$

$\therefore \quad ap \equiv 1 \pmod{n}$

$\overline{ap} = \overline{1}$ and $\overline{a}.\overline{p} = \overline{1}$.

$\therefore \quad \overline{p}$ is the inverse of $\overline{a}$.

Example (4.2.7 (1))

Find the inverse of $\overline{16}$ *in* $\mathbb{Z}_{35}$ *and use to solve* $\overline{16}x = \overline{9}$ *in* $\mathbb{Z}_{35}$.

$$\begin{aligned} 35 &= 2.16 + 3 \\ 16 &= 5.3 + 1 \\ 3 &= 3.1 \end{aligned}$$

Last nonzero remainder is 1.
$\therefore \quad \gcd(16, 35) = 1$ i.e. coprime
$\therefore \overline{16}$ is invertible in $\mathbb{Z}_{35}$ by Theorem 4.2.6.

Now to find the inverse:

(Finding the inverse using techniques from chapter 2)

(Using the inverse to solve the equation with coefficients in $\mathbb{Z}_n$)

Use to solve $\overline{16}x = \bar{9}$ in $\mathbb{Z}_{35}$.
Substituting back in

$$\begin{aligned} 1 &= 16 - 5.3 = 16 - 5(35 - 2.16) = 16 + 10.16 - 5.35 \\ &= 11.16 - 5.35. \end{aligned}$$

Therefore $11.16 \equiv 1 \pmod{35}$ so $\overline{11}$ is inverse of $\overline{16}$ in $\mathbb{Z}_{35}$.
$\therefore \quad \overline{16}x = \bar{9} \quad \Rightarrow \quad x = \overline{11}.\bar{9} = \overline{99} = \overline{29}.$

Example (4.2.7 (2))

Find the elements of $\mathbb{Z}_9$ that have inverses.

9 is not prime. 1,2,4,5,7,8 are coprime with 9 but 3 and 6 have common factors with 9.
So $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \bar{8}$ are invertible in $\mathbb{Z}_9$. And
$\overline{2}.\overline{5} = \overline{10} = \overline{1}$ so $\overline{2}$ and $\overline{5}$ are inverses.
$\overline{4}.\overline{7} = \overline{28} = \overline{1}$ so $\overline{4}$ and $\overline{7}$ are inverses.
$\overline{8}.\overline{8} = \overline{64} = \overline{1}$ so $\overline{8}$ is self inverting.