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:

- state 3 equivalent conditions under which an element has an inverse in $\mathbb{Z}_n$
- prove that these 3 conditions are equivalent
- write out addition and multiplication tables for $\mathbb{Z}_n$
- apply modular arithmetic to problem of finding remainders when dividing numbers raised to large powers by a natural number
-

Theorem (4.2.8)

The following are equivalent for $n \geq 2$.

(i) *Every element $\overline{a} \neq \overline{0}$ in $\mathbb{Z}_n$ has an inverse.*

(ii) *If $\overline{ab} = \overline{0}$ in $\mathbb{Z}_n$, then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.*

(iii) *n is prime.*

(This theorem links the conditions under which an element in $\mathbb{Z}_n$ has an inverse depending on whether or not n is prime.)

PROOF:

Assume (i) prove (ii) (direct proof used here)

$\overline{a} \neq \overline{0}$ has inverse $\overline{c}$ in $\mathbb{Z}_n$ so $\overline{ac} = \overline{ca} = \overline{1}$.

(Can you state the reasons here?)

$$\begin{aligned}
\overline{a}\overline{b} = \overline{0} \quad &\Rightarrow \quad \overline{c}(\overline{a}\overline{b}) = \overline{c}\overline{0} \\
&\Rightarrow \quad (\overline{ca})\overline{b} = \overline{0} \\
&\Rightarrow \quad \overline{1}.\overline{b} = \overline{0} \Rightarrow \overline{b} = \overline{0} \text{ by property of unity: Theorem } \cancel{4.}\ 4.2
\end{aligned}$$

Therefore (ii) holds.

Assume (ii) prove (iii) (this part is proved by contradiction)

If $\overline{a}\overline{b} = \overline{0}$ then $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

Assume n not prime, say $n = kp$ where $2 \leq k < n$, and $2 \leq p < n$.

Then $\overline{n} = \overline{kp} = \overline{k}\overline{p} = \overline{0}$. ($\overline{n} = \overline{0}$ Why?)

Thus $\overline{k} = \overline{0}$ or $\overline{p} = \overline{0}$.

But $2 \leq k < n$, and $2 \leq p < n$.

So that is not possible. $\therefore$ $k = 1$ or $p = 1$ as required. i.e n is prime.

Assume (iii) prove (i)

n is prime so for $\overline{a} \in \mathbb{Z}_n$, the $\gcd(a, n) = 1$.

$\Rightarrow \quad \exists p, q$ such that $pa + qn = 1$

$\Rightarrow \quad pa \equiv 1 \pmod{n}$.

Thus $\overline{pa} = \overline{1}$. $\therefore$ $\overline{a}$ has inverse (By Thm4.2.6) . $\therefore$ (i) holds.

Since (i) implies (ii)

and (ii) implies (iii)

and (iii) implies (i),

the 3 statements are equivalent.

Example (4.2.9)

Write down the addition and multiplication tables for $\mathbb{Z}_5$.

$(\mathbb{Z}_5,+)$	$b=\overline{0}$	$b=\overline{1}$	$b=\overline{2}$	$b=\overline{3}$	$b=\overline{4}$
$a=\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$a=\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$a=\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$a=\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$a=\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Every entry in the table is $a+b$ in $\mathbb{Z}_5$.

$\overline{2}+\overline{3}=\overline{5}=\overline{0}$

$\overline{4}+\overline{3}=\overline{7}=\overline{2}$

$\overline{3}+\overline{2}$

We read $(\mathbb{Z}_5,+)$ as "the set $\mathbb{Z}_5$ under addition"

$\mathbb{Z}_5$ under multiplication...

$(\mathbb{Z}_5, .)$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\overline{3} \,.\, \overline{2} = \overline{6} = \overline{1}$

$\mathbb{Z}_9$ under addition...

$(\mathbb{Z}_9, +)$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Note: The residue class $\bar{a}$ will, from here on, be denoted simply without the bar as a

$\mathbb{Z}_9$ under multiplication

$(\mathbb{Z}_9, .)$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Only 0's, 3's and 6's in these columns and rows

NOTE: The product of two non-zero numbers gives us a zero here...

3.3=0 3.6=0 6.3=0 6.6=0 (just note it...)

Exercises

$\overline{7}$ in different $\mathbb{Z}_n$

In $\mathbb{Z}_9$: $\overline{7} = \{\cdots, -11, -2, 7, 16, 25, \cdots\} = \overline{-2}$

In $\mathbb{Z}_5$: $\overline{7} = \{\cdots, -3, 2, 7, 12, 17, \cdots\} = \overline{2}$

In $\mathbb{Z}_7$: $\overline{7} = \{\cdots, -14, -7, 0, 7, 14, \cdots\} = \overline{0}$

Addition in $\mathbb{Z}_9$

$\overline{5} = \{\cdots, -13, -4, 5, 14, 23, \cdots\} = \overline{14}$

$\overline{8} = \{\cdots, -19, -10, -1, 8, 17, \cdots\} = \overline{-10}$

$\overline{5} + \overline{8} = \overline{13} = \{\cdots, -23, -14, -5, 4, 13, 22, \cdots\} = \overline{4}$

Multiplication in $\mathbb{Z}_9$

$\overline{5}.\overline{8} = \overline{40} = \{\cdots, 4, 13, 22, 31, 40, 49, \cdots\} = \overline{4}$

Calculator says 3^1027 = 1.0081579916007541175389913362991e+490

Exercise

{No information on last digit here}

Unit decimal digit of 3^{1027}

3 9 27 81 243 729 2187 6561 19683 etc

Look at the pattern of the last digits... 3 9 7 1 3 9 7 1 3 ... etc

$$
\begin{aligned}
3^{4n+1} &\equiv 3 \pmod{10}\\
3^{4n+2} &\equiv 9 \pmod{10}\\
3^{4n+3} &\equiv 7 \pmod{10}\\
3^{4n} &\equiv 1 \pmod{10}\\
1027 &= 4(256)+3.
\end{aligned}
$$

1027 = 4*n* + ?

Therefore last digit is 7.

Exercise

8^{391} divided by 5 gives remainder?

$8 = 8$ $\quad 8^2 = 64$ $\quad 8^3 = 512$ $\quad 8^4 = 4096$ $\quad 8^5 = 32768$ $\quad 8^6 = 262144$ etc

$$\begin{aligned} 8^{4n+1} &\equiv 3 \pmod 5 \\ 8^{4n+2} &\equiv 4 \pmod 5 \\ 8^{4n+3} &\equiv 2 \pmod 5 \\ 8^{4n} &\equiv 1 \pmod 5 \\ 391 &= 4(97) + 3. \end{aligned}$$

Therefore remainder is 2.