

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

The Ring \mathbb{Z}_n



Albert R Meyer October 13, 2015

Zn.1

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Only the Remainder Interval

$$i + j (\mathbb{Z}_n) ::= \text{rem}(i + j, n)$$

$$i \cdot j (\mathbb{Z}_n) ::= \text{rem}(i \cdot j, n)$$

The integer interval $[0, n)$
under $+, \cdot (\mathbb{Z}_n)$ is called \mathbb{Z}_n
the **ring of integers mod n**



Albert R Meyer October 13, 2015

Zn.2

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

\mathbb{Z}_n arithmetic

$$3 + 6 = 2 \quad (\mathbb{Z}_7)$$

$$9 \cdot 8 = 6 \quad (\mathbb{Z}_{11})$$

(use $=$ instead of \equiv)



Albert R Meyer October 13, 2015

Zn.3

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

$\equiv (\text{mod } n)$ versus \mathbb{Z}_n

$$i \equiv j (\text{mod } n) \quad \text{IFF}$$

$$r(i) = r(j) (\mathbb{Z}_n)$$



Albert R Meyer October 13, 2015

Zn.5

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Rules for \mathbb{Z}_n

$$(i + j) + k = i + (j + k) \quad \text{associativity}$$

$$0 + i = i \quad \text{identity}$$

$$i + (-i) = 0 \quad \text{inverse}$$

$$i + j = j + i \quad \text{commutativity}$$



Albert R Meyer October 13, 2015

Zn.6

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Rules for Rings

$$(i + j) + k = i + (j + k) \quad \text{associativity}$$

$$0 + i = i \quad \text{identity}$$

$$i + (-i) = 0 \quad \text{inverse}$$

$$i + j = j + i \quad \text{commutativity}$$



Albert R Meyer October 13, 2015

Zn.7

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Rules for Rings

$$(i \cdot j) \cdot k = i \cdot (j \cdot k) \quad \text{associativity}$$

$$1 \cdot i = i \quad \text{identity}$$

$$i \cdot j = j \cdot i \quad \text{commutativity}$$



Albert R Meyer October 13, 2015

Zn.8

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Rules for Rings

$$\text{distributivity}$$

$$i \cdot (j + k)$$

$$= i \cdot j + i \cdot k$$



Albert R Meyer October 13, 2015

Zn.9

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Rules for Rings

no cancellation rule

$$3 \cdot 2 = 8 \cdot 2 \quad (\mathbb{Z}_{10})$$

$$3 \neq 8 \quad (\mathbb{Z}_{10})$$



Albert R Meyer October 13, 2015

Zn.10

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

\mathbb{Z}_n^* ::= elements of \mathbb{Z}_n
relatively prime to n

$$i \in \mathbb{Z}_n^* \text{ IFF } \gcd(i, n) = 1$$

IFF i is cancellable in \mathbb{Z}_n

IFF i has an inverse in \mathbb{Z}_n



Albert R Meyer October 13, 2015

Zn.11

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

\mathbb{Z}_n^* ::= elements of \mathbb{Z}_n
relatively prime to n

$$\phi(n) ::= |\mathbb{Z}_n^*|$$



Albert R Meyer October 13, 2015

Zn.12

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Euler's Theorem

$$k^{\phi(n)} = 1 \quad (\mathbb{Z}_n)$$

for $k \in \mathbb{Z}_n^*$



Albert R Meyer October 13, 2015

Zn.13