

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 March 11, 2015

Zn.1

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

Just Remainders

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

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

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



Albert R Meyer March 11, 2015

Zn.2

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

\mathbb{Z}_n arithmetic

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

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



Albert R Meyer March 11, 2015

Zn.4

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

\mathbb{Z} versus \mathbb{Z}_n

$r(k)$ abbrevs $\text{rem}(k, n)$

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

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



Albert R Meyer March 11, 2015

Zn.5

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

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

$i \equiv j \pmod{n}$ IFF

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



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

Rules for \mathbb{Z}_n

$(i + j) + k = i + (j + k)$ associativity

$0 + i = i$ identity

$i + (-i) = 0$ inverse

$i + j = j + i$ commutativity



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

Rules for \mathbb{Z}_n

$(i \cdot j) \cdot k = i \cdot (j \cdot k)$ associativity

$1 \cdot i = i$ identity

$i \cdot j = j \cdot i$ commutativity



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

Rules for \mathbb{Z}_n

distributivity

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



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

Rules for \mathbb{Z}_n

no cancellation rule

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

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



Albert R Meyer March 11, 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 March 11, 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 March 11, 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 March 11, 2015

Zn.13

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

Lemma 1

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

$$|kS| = |S|$$



Albert R Meyer March 11, 2015

Zn.14

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

Lemma 1

$$|kS| = |S|$$

proof:

$s_1 \neq s_2$ IMPLIES $ks_1 \neq ks_2$

since k is cancellable



Albert R Meyer March 11, 2015

Zn.15

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

Lemma 2

For $i, j \in \mathbb{Z}_n$

$i, j \in \mathbb{Z}_n^*$ IFF $i \cdot j \in \mathbb{Z}_n^*$



Albert R Meyer March 11, 2015

Zn.16

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

Corollary

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

$$\mathbb{Z}_n^* = k\mathbb{Z}_n^*$$



Albert R Meyer March 11, 2015

Zn.17

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

permuting \mathbb{Z}_9

$$\phi(9) = 3^2 - 3 = 6$$

$$\mathbb{Z}_9^* = 1 \ 2 \ 4 \ 5 \ 7 \ 8$$



Albert R Meyer March 11, 2015

Zn.18

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

permuting \mathbb{Z}_9

$$\mathbb{Z}_9^* = \begin{array}{cccccc} 1 & 2 & 4 & 5 & 7 & 8 \\ 2 \cdot & 2 & 4 & 8 & 1 & 5 & 7 \end{array}$$



Albert R Meyer March 11, 2015

Zn.19

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

permuting \mathbb{Z}_9

$$\mathbb{Z}_9^* = \begin{array}{cccccc} 1 & 2 & 4 & 5 & 7 & 8 \\ 2 \cdot & 2 & 4 & 8 & 1 & 5 & 7 \\ 7 \cdot & 7 & 5 & 1 & 8 & 4 & 2 \end{array}$$



Albert R Meyer March 11, 2015

Zn.20

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

Proof of Euler

$$\prod \mathbb{Z}_n^* = \prod k \mathbb{Z}_n^*$$

product



Albert R Meyer March 11, 2015

Zn.22

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

Proof of Euler

$$\begin{aligned} \prod \mathbb{Z}_n^* &= \prod k \mathbb{Z}_n^* \\ &= k^{\phi(n)} \prod \mathbb{Z}_n^* \end{aligned}$$



Albert R Meyer March 11, 2015

Zn.23

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

Proof of Euler

$$\begin{aligned} \cancel{\prod \mathbb{Z}_n^*} &= \\ &= k^{\phi(n)} \cancel{\prod \mathbb{Z}_n^*} \end{aligned}$$



Albert R Meyer March 11, 2015

Zn.24

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

Proof of Euler

$$1 = k^{\phi(n)}$$



Albert R Meyer March 11, 2015

Zn.25

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

Proof of Euler

$$1 = k^{\phi(n)}$$

QED



Albert R Meyer March 11, 2015

Zn.26