



Mathematics for Computer Science
MIT 6.042J/18.062J

The Ring \mathbb{Z}_n



Albert R Meyer March 11, 2013 Zn.1




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, 2013 Zn.2




\mathbb{Z}_n arithmetic

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

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



Albert R Meyer March 11, 2013 Zn.4




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

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

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


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


Albert R Meyer March 11, 2013 Zn.5




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

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




Albert R Meyer March 11, 2013 Zn.6




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




Albert R Meyer March 11, 2013 Zn.7




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




Albert R Meyer March 11, 2013 Zn.8




Rules for \mathbb{Z}_n

distributivity

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




Albert R Meyer March 11, 2013 Zn.9




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, 2013 Zn.10




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


$i \in \mathbb{Z}_n^*$ 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, 2013 Zn.11



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

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



Albert R Meyer March 11, 2013 Zn.12




Euler's Theorem

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

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




Albert R Meyer March 11, 2013 Zn.13




Lemma 1

$$|kS| = |S|$$

for $S \subseteq \mathbb{Z}_n$

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


Albert R Meyer March 11, 2013 Zn.14




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, 2013 Zn.15




Lemma 2

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

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



Albert R Meyer March 11, 2013 Zn.16




Corollary

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

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




Albert R Meyer March 11, 2013 Zn.17




permuting \mathbb{Z}_9

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

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




Albert R Meyer March 11, 2013 Zn.18




permuting \mathbb{Z}_9

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




Albert R Meyer March 11, 2013 Zn.19




permuting \mathbb{Z}_9

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




Albert R Meyer March 11, 2013 Zn.20




Corollary

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

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




Albert R Meyer March 11, 2013 Zn.21




Proof of Euler

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


product




Albert R Meyer March 11, 2013 Zn.22




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, 2013 Zn.23




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, 2013 Zn.24



Proof of Euler

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


Albert R Meyer March 11, 2013 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



MIT OpenCourseWare
<http://ocw.mit.edu>

6.042J / 18.062J Mathematics for Computer Science
Spring 2015

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.