Mathematics for Computer Science
MIT 6.042J/18.062J

The Ring $\mathbb{Z}_n$

Only the Remainder Interval

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

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

$\mathbb{Z}_n$ arithmetic

$$3 + 6 = 2 \quad (\mathbb{Z}_7)$$
$$9 \cdot 8 = 6 \quad (\mathbb{Z}_{11})$$

(use $=$ instead of $\equiv$)

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

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

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

Rules for Rings

$(i+j)+k = i+(j+k)$	associativity
$0+i=i$	identity
$i+(-i)=0$	inverse
$i+j=j+i$	commutativity

Rules for Rings

$(i\cdot j)\cdot k = i\cdot(j\cdot k)$	associativity
$1\cdot i=i$	identity
$i\cdot j=j\cdot i$	commutativity

Rules for Rings

distributivity

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

Rules for Rings

no cancellation rule

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

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

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

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

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

Euler's Theorem

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

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