Mathematics for Computer Science
MIT 6.042J/18.062J

The Ring $\mathbb{Z}_n$

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

$\mathbb{Z}_n$ arithmetic

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

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

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

r(k) abbrevs rem(k,n)

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

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

$\equiv \pmod n$ versus $\mathbb{Z}_n$

$i \equiv j \pmod n$ 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 $\mathbb{Z}_n$

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

Rules for $\mathbb{Z}_n$

distributivity

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

Rules for $\mathbb{Z}_n$

no cancellation rule

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

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

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

Lemma 1

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

$$|kS| = |S|$$

Lemma 1

$$|kS| = |S|$$

proof :

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

since k is cancellable

Lemma 2

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

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

Corollary

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

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

permuting $\mathbb{Z}_9$

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

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

permuting $\mathbb{Z}_9$

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

permuting $\mathbb{Z}_9$

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

Proof of Euler

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

product

Proof of Euler

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

Proof of Euler

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

Proof of Euler

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

Proof of Euler

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

QED