

**Homework 20: Additional Notes, ch.10: q.1, 2***How to do Modulos*

The result of an operation  $x \circ y$  modulo  $n$  is the remainder left after dividing  $x \circ y$  by  $n$ .

e.g.  $4 \times 2 \bmod 5$  is

(i)  $4 \times 2 = 8$

(ii)  $8/5 = 1$  remainder 3

(iii) Therefore the answer is 3.

e.g.  $9 + 6 \bmod 11$  is

(i)  $9 + 6 = 15$

(ii)  $15/11 = 1$  remainder 4

(iii) Therefore, the answer is 4

(2a)

$\langle \{1,3,5,7,8\}, \times \bmod 11 \rangle$

$\times \bmod 11$	1	3	5	7	8
1	1	3	5	7	9
3	3	9	4	10	2
5	5	4	3	2	7
7	7	10	2	5	1
8	9	2	7	1	9

!! Not closed: 2, 4, 10 are not in the set  $\{1,3,5,7,8\}$ !

- does have an identity element (1), and everything has an inverse.

(b)

$\times \bmod 11$	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

Closed? Yes.

Associative? Yes.

Identity element? 1

Inverses? Yes

(c) Problem: not associative:

$$(c \circ d) \circ b = c \circ (d \circ b)$$

$$a \circ b = c \circ c$$

$$b = a \quad !!$$

Also, see corollary 10.2: there can only be one inverse for each element, but  $c$  has two.  $d$  has no right inverse.

(e) Let  $x_1 = a$  and  $x_2 = b$ .

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

It's closed, associative, and the identity element is  $\emptyset$ .

However, almost no elements have inverses, EXCEPT for  $\emptyset$ .

(f) Let  $x_1 = a$  and  $x_2 = b$ .

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{a\}$	$\{a,b\}$

Closed and associative.

Identity element =  $\{a,b\}$

But no inverses EXCEPT for  $\{a,b\}$ .