## Modular arithmetic

For every positive integer m, the *integers modulo* m are:

$$\mathbb{Z}_m$$
: 0, 1, ...,  $m-1$ .

with arithmetic operations of addition  $+_{\mathfrak{m}}$  and multiplication  $\cdot_{\mathfrak{m}}$  defined as follows

$$k +_{m} l = [k + l]_{m} = \operatorname{rem}(k + l, m) ,$$
  
$$k \cdot_{m} l = [k \cdot l]_{m} = \operatorname{rem}(k \cdot l, m)$$

for all  $0 \leq k, l < m$ .

For & and y in Um, x tmy and x.my are The unique modular integers in Zm such That  $\chi + \chi \neq \chi \chi \neq \chi (m d m)$  $\chi \cdot m \gamma \equiv \chi \cdot \gamma \pmod{mod}$ 

Associativity of <u>m</u>

(2 · m 2) · m 2  $\equiv (\chi_{in} \chi) \cdot z$  $\equiv (x, y), z$  $= \chi \cdot (\gamma \cdot z)$  $\equiv \chi \cdot (\gamma \cdot m^2)$ 

 $\Xi \chi \cdot m(\gamma \cdot m^2)$ 

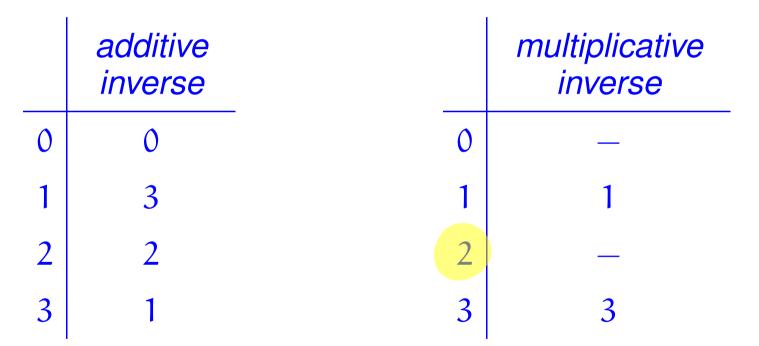
 $\implies (\chi \cdot m \cdot \chi) \cdot m \cdot t = \chi \cdot m (\gamma \cdot m \cdot t)$ 

**Example 49** The addition and multiplication tables for  $\mathbb{Z}_4$  are:

$+_{4}$	0	1	2	3		•4	0	1	2	
0	0	1	2	3	(	0	0	0	0	
1	1	2	3	0		1	0	1	2	4
2	2	3	0	1		2	0	2	0	
3	3	0	1	2		3	0	3	2	

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:



Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

**Example 50** The addition and multiplication tables for  $\mathbb{Z}_5$  are:

$+_{5}$	0	1	2	3	4	•5	0	1	2	3	4
0	0	1	2	3	4	0					
1	1	2	3	4	0	1	0	1	2	3	4
2						2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

•	additive inverse		<i>multiplicative</i> <i>inverse</i>
0	0	0	_
1	4	1	1
2	3	2	3
3	2	3	2
4	1	4	4

Surprisingly, every non-zero element has a multiplicative inverse.

**Proposition 51** For all natural numbers m > 1, the modular-arithmetic structure

 $(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$ 

is a commutative ring.

**NB** Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses

Proposition. Let m be à positive integer. A modular integer 2 in Zm has a reciprocal iff There exist integers i and j such That  $z \cdot i + m \cdot j = 1$ PROOF: Let mbe a positive integer and let x be a modular marger in Um. (=) Assume There exists i m 2m such that  $z \cdot m i \equiv 1 \pmod{m}$ . As  $x \cdot i \equiv x \cdot m i \pmod{m}$  we have That for some integer j.

(E) Assume integers i and j such That  $x_i + m_j = 1$ Then, & has reciprocal [i]m. Indeed,  $\chi \cdot m[i]m = [\chi \cdot i]m \equiv \chi \cdot i$   $\lim_{n \to \infty} 1$ 1 - m j1 (mrdm)

Integer Linear Combinations Definition. An integer l 15 said to be an integer linear combination of Two integers a and b whenever there are integers i and j such That  $l = i \cdot a + j \cdot b$ . Proposition. Let m be a positive integer. A modular integer x in  $\mathbb{Z}m$  has a recipro cal iff 1 is an integer linear combination of m and x.