Modular arithmetic

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

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

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

$$\begin{aligned} k +_m l &= [k+l]_m = \mathrm{rem}(k+l, m) \, , \\ k \cdot_m l &= [k \cdot l]_m = \mathrm{rem}(k \cdot l, m) \end{aligned}$$

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

For x and y in $\mathbb{Z}_m$,

$$x +_m y \quad \text{and} \quad x \cdot_m y$$

are the unique modular integers in $\mathbb{Z}_m$ such that

$$x +_m y \equiv x + y \pmod{m}$$

$$x \cdot_m y \equiv x \cdot y \pmod{m}$$

Associativity of $\cdot_m$

$$(x \cdot_m y) \cdot_m z$$

$$\equiv (x \cdot_m y) \cdot z$$

$$\equiv (x \cdot y) \cdot z$$

$$= x \cdot (y \cdot z)$$

$$\equiv x \cdot (y \cdot_m z)$$

$$\equiv x \cdot_m (y \cdot_m z)$$

$$\Rightarrow (x \cdot_m y) \cdot_m z = x \cdot_m (y \cdot_m z)$$

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

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

$x \neq 0$ has additive inverse $m-x$

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

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	—
1	1
2	—
3	3

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
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
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:

$\cdot$	*additive inverse*
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	—
1	1
2	3
3	2
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 a positive integer. A modular integer x in $\mathbb{Z}_m$ has a reciprocal iff there exist integers i and j such that $x \cdot i + m \cdot j = 1$.

PROOF: Let m be a positive integer and let x be a modular integer in $\mathbb{Z}_m$.

$(\Rightarrow)$ Assume there exists i in $\mathbb{Z}_m$ such that $x \cdot_m i \equiv 1 \pmod{m}$.

As $x \cdot i \equiv x \cdot_m i \pmod{m}$ we have that

$$x \cdot i - 1 = m j$$

for some integer j.

($\Leftarrow$) Assume integers i and j such that

$$xi + mj = 1$$

Then, x has reciprocal $[i]_m$.

Indeed,

$$x \cdot_m [i]_m = [x \cdot i]_m \equiv x \cdot i = 1 - mj \equiv 1 \pmod{m}$$

$\boxtimes$

Integer Linear Combinations

Definition. An integer ℓ is said to be an integer linear combination of two integers a and b whenever there are integers i and j such that $\ell = i \cdot a + j \cdot b$.

Proposition. Let m be a positive integer. A modular integer x in $\mathbb{Z}_m$ has a reciprocal iff 1 is an integer linear combination of m and x.