Appendix A

Associativity and Distributivity of Operations in $\mathbf{Z}_n$

Let $n \in \mathbf{Z}$ satisfy $n \geq 2$. Let $\mathbf{Z}_n = \{x \in \mathbf{N}: x < n\}$. Let $\oplus_n$ and $\odot_n$ be the binary operations on $\mathbf{Z}_n$ defined by

$$\begin{aligned} a \oplus_n b &= \text{remainder when } a+b \text{ is divided by } n, \\ a \odot_n b &= \text{remainder when } ab \text{ is divided by } n. \end{aligned}$$

Thus for all $a, b \in \mathbf{Z}_n$,

$$a + b = r \cdot n + (a \oplus_n b) \text{ for some } r \in \mathbf{N}. \tag{A.1}$$

$$a \cdot b = s \cdot n + (a \odot_n b) \text{ for some } s \in \mathbf{N}. \tag{A.2}$$

We will show that $\oplus_n$ and $\odot_n$ are associative by using the usual properties of addition and multiplication on $\mathbf{Z}$.

A.3 Lemma. *Let $x, y \in \mathbf{Z}_n$, $q, r \in \mathbf{Z}$. If $nq + x = nr + y$, then $x = y$ and $q = r$.*

Proof:

Case 1. Suppose $y \leq x$. Then by our assumptions,

$$x - y = n(r - q)$$

and

$$0 \leq x - y \leq x < n \cdot 1.$$

So

$$0 \leq n(r-q) < n \cdot 1.$$

Since $n > 0$, it follows that $0 \leq r - q < 1$ and since $r - q$ is an integer $r - q = 0$, so $r = q$. Then $x - y = 0$, so $x = y$.

Case 2. If $y > x$, use Case 1 with y and x interchanged. ‖

A.4 Theorem. *$\oplus_n$ is associative on $\mathbf{Z}_n$.*

Proof: Let $a, b, c \in \mathbf{Z}_n$. Then

$$a + b = n \cdot t + (a \oplus_n b) \text{ for some } t \in \mathbf{Z}. \tag{A.5}$$

$$b + c = n \cdot r + (b \oplus_n c) \text{ for some } r \in \mathbf{Z}. \tag{A.6}$$

$$(a \oplus_n b) + c = n \cdot s + ((a \oplus_n b) \oplus_n c) \text{ for some } s \in \mathbf{Z}. \tag{A.7}$$

$$a + (b \oplus_n c) = n \cdot w + (a \oplus_n (b \oplus_n c)) \text{ for some } w \in \mathbf{Z}. \tag{A.8}$$

By adding c to both sides of (A.5), we get

$$(a + b) + c = nt + ((a \oplus_n b) + c), \tag{A.9}$$

and by adding a to both sides of (A.6), we get

$$a + (b + c) = nr + (a + (b \oplus_n c)). \tag{A.10}$$

Replace $(a \oplus_n b) + c$ in (A.9) by its value from (A.7) to get

$$(a + b) + c = n(s + t) + ((a \oplus_n b) \oplus_n c) \tag{A.11}$$

and replace $a + (b \oplus_n c)$ in (A.10) by its value from (A.8) to get

$$a + (b + c) = n(r + w) + (a \oplus_n (b \oplus_n c)) \tag{A.12}$$

By (A.11) and (A.12) and the associative law in $\mathbf{Z}$,

$$n(s + t) + ((a \oplus_n b) \oplus_n c) = n(r + w) + (a \oplus_n (b \oplus_n c)).$$

the associativity of $\oplus_n$ follows from lemma (A.3). ‖

A.13 Theorem. *$\odot_n$ is associative on $\mathbf{Z}_n$.*

Proof: The proof is nearly identical with the proof that $\oplus_n$ is associative.

A.14 Theorem. *The distributive law holds in $\mathbf{Z}_n$; i.e., for all $a, b, c \in \mathbf{Z}_n$,*

$$a \odot_n (b \oplus_n c) = (a \odot_n b) \oplus_n (a \odot_n c).$$

Proof: We have

$$b + c = n \cdot t + (b \oplus_n c) \text{ for some } t \in \mathbf{Z}. \tag{A.15}$$

$$a \cdot (b \oplus_n c) = n \cdot s + (a \odot_n (b \oplus_n c)) \text{ for some } s \in \mathbf{Z}. \tag{A.16}$$

$$a \cdot b = n \cdot u + (a \odot_n b) \text{ for some } u \in \mathbf{Z}. \tag{A.17}$$

$$a \cdot c = n \cdot v + (a \odot_n c) \text{ for some } v \in \mathbf{Z}. \tag{A.18}$$

Multiply both sides of (A.15) by a to get

$$a \cdot (b + c) = n \cdot at + a \cdot (b \oplus_n c). \tag{A.19}$$

Replace $a \cdot (b \oplus_n c)$ in (A.19) by its value from (A.16) to get

$$a \cdot (b + c) = n(at + s) + (a \odot_n (b \oplus_n c)). \tag{A.20}$$

Now add equations (A.17) and (A.18) to get

$$a \cdot b + a \cdot c = n \cdot (u + v) + ((a \odot_n b) + (a \odot_n c)). \tag{A.21}$$

We know that for some $w \in \mathbf{Z}$,

$$(a \odot_n b) + (a \odot_n c) = n \cdot w + ((a \odot_n b) \oplus_n (a \odot_n c)),$$

and if we substitute this into (A.21), we obtain

$$a \cdot b + a \cdot c = n(u + v + w) + ((a \odot_n b) \oplus_n (a \odot_n c)). \tag{A.22}$$

From (A.20) and (A.22) and the distributive law in $\mathbf{Z}$, we conclude

$$n(at + s) + (a \odot_n (b \oplus_n c)) = n(u + v + w) + ((a \odot_n b) \oplus_n (a \odot_n c)).$$

The distributive law follows from lemma A.3. $\|$