# MTHSC 412 Section 2.2 – Modular Arithmetic

Kevin James

Kevin James MTHSC 412 Section 2.2 – Modular Arithmetic

(E) < E)</p>

#### DEFINITION

We define addition and multiplication on  $\mathbb{Z}_n$  as follows.

[a] + [b] = [a + b] and [a][b] = [ab].

#### Note

We must check that this addition is well-defined since any congruence class can be represented as [a] in many ways. For example, if n = 5 then [1] = [6] = [11]. In fact, for any  $b \in [a]$ , [a] = [b].

・ 同 ト ・ ヨ ト ・ ヨ ト

#### Theorem

If 
$$[a] = [b]$$
 and  $[c] = [d]$ , then

$$[a+c] = [b+d]$$
 and  $[ac] = [bd]$ .

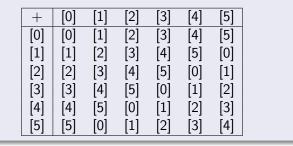
#### Proof.

Suppose that [a] = [b] and [c] = [d]. Then  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ . Thus from theorems of the previous section,  $a + c \equiv b + d \pmod{n}$  and  $ac \equiv bd \pmod{n}$ . Thus, [a + c] = [b + d] and [ac] = [bd].

- 4 同 6 4 日 6 4 日 6

### EXAMPLE

The addition table for  $\mathbb{Z}_6$  is as follows.



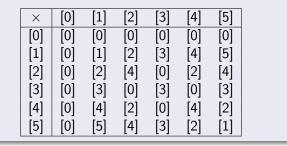
A (1) > A (1) > A

3

- ∢ ≣ ▶

## EXAMPLE

The multiplication table for  $\mathbb{Z}_6$  is as follows.



æ

3

## Theorem

Suppose that  $[a], [b], [c] \in \mathbb{Z}_n$ .

- **1** Closure of addition:  $[a] + [b] \in \mathbb{Z}_n$ .
- **2** Associativity of addition: ([a] + [b]) + [c] = [a] + ([b] + [c]).
- **8** Commutativity of addition: [a] + [b] = [b] + [a].
- 4 Additive Identity: [a] + [0] = [0] + [a] = [a].
- **6** Additive Inverses: [a] + [-a] = [-a] + [a] = [0].
- **6** Closure of Multiplication:  $[a][b] \in \mathbb{Z}_n$ .
- **7** Associativity of Multiplication: ([a][b])[c] = [a]([b][c]).
- **8** Commutativity of Multiplication: [a][b] = [b][a].
- Distributive Laws: [a]([b] + [c]) = [a][b] + [a][c] and ([a] + [b])[c] = [a][c] + [b][c].
- **(** Multiplicative Identity: [a][1] = [1][a] = [a].

イロト イポト イヨト イヨト 二日

# Note

 We will use positive integral exponents to denote repeated multiplication as usual.

**2** 
$$[a]^0 = [1].$$

**3** Given  $[a] \in \mathbb{Z}_n$ , if there is  $[b] \in \mathbb{Z}_n$  such that [a][b] = [1], then we say that [b] is the multiplicative inverse of [a] and write  $[b] = [a]^{-1}$ .

4 For 
$$n > 0$$
,  $[a]^{-n} = ([a]^{-1})^n$ .

向下 イヨト イヨト