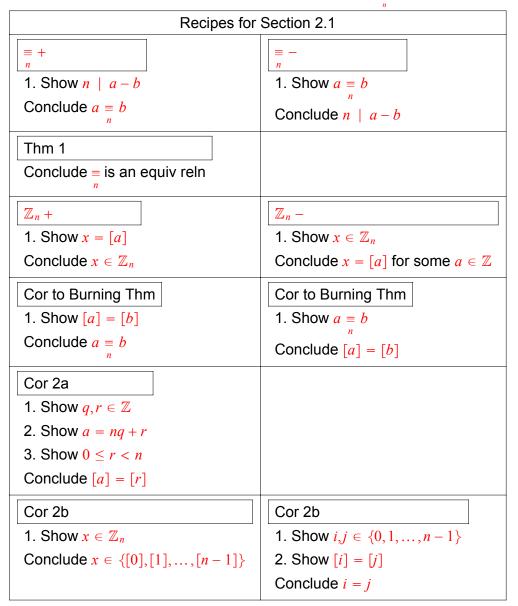
## Section 2.1: Congruence in $\mathbb{Z}$

In the following recipes,  $n \in \mathbb{N}^+$ ,  $a, b \in \mathbb{Z}$ , and [ ] is [ ]<sub>=</sub>.



## Section 2.2: Arithmetic in $\mathbb{Z}_n$

In the following recipes let  $n \in \mathbb{N}^+, a, b, c, d \in \mathbb{Z}$  and [ ] denote [ ].

Recipes for Section 2.2	
Sec 2.2 Thm 1	
1. Show $a \equiv b$	
2. Show $c \equiv d$	
Conclude $a + c \equiv b + d$	
Conclude $ac = bd$	
Mod +	Mod -
1. Show $q, r \in \mathbb{Z}$	1. Show $r = a \mod n$
2. Show $a = nq + r$	Conclude $r \in \mathbb{Z}$
3. Show $0 \le r < n$	Conclude $a = nq + r$ for some $q \in \mathbb{Z}$
Conclude $r = (a \mod n)$	Conclude $0 \le r < n$
binary operator +	binary operator –
1. Show $f: X \times X \to X$	1. Show $f$ is a binary operator on $X$
Conclude $f$ is a binary operator on $X$	$Conclude f: X \times X \to X$
Sec 2.2 Thm 2	
Conclude $\oplus$ : $\mathbb{Z}_n \to \mathbb{Z}_n$	
Conclude $\otimes : \mathbb{Z}_n \to \mathbb{Z}_n$	
Def ⊕	Def ⊗
Conclude $[a] \oplus [b] = [a+b]$	Conclude $[a] \otimes [b] = [ab]$
Sec 2.2 Thm 3	Mult by 0 in $\mathbb{Z}_n$
1. Show $A, B, C \in \mathbb{Z}_n$	1. Show $A \in \mathbb{Z}_n$
Conclude $A \oplus (B \oplus C) = (A \oplus B) \oplus C$	Conclude $[0] \otimes A = [0]$
Conclude $A \oplus B = B \oplus A$	
Conclude $[0] \oplus A = A \oplus [0] = A$	
Conclude $\exists X \in \mathbb{Z}_n, A \oplus X = [0]$	
Conclude $A \otimes (B \otimes C) = (A \otimes B) \otimes C$	
Conclude $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$	
Conclude $A \otimes B = B \otimes A$	
Conclude $A \otimes [1] = [1] \otimes A = A$	