

- Question 1:** (a)  $[18] = \{ 4n + 2 \mid n \in \mathbb{Z} \}$ .  
 (b)  $[31] = \{ 4n + 2 \mid n \in \mathbb{Z} \}$ .  
 (c) There are 4 equivalence classes.

**Question 2:** *Proof.* We prove that  $\equiv_n$  on  $\mathbb{Z}$  is an equivalence relation by showing that it is reflexive, transitive, and symmetric. Suppose  $n \in \mathbb{Z}^+$ .

**Reflexive** Let  $a$  be an arbitrary element in  $\mathbb{Z}$ . Clearly,  $a - a = 0 = kn, k \in \mathbb{Z}$ . So,  $\forall a \in \mathbb{Z}, a \equiv_n a$ .

**Symmetric** Let  $a, b$  be arbitrary elements of  $\mathbb{Z}$ . Suppose  $a \equiv_n b$ . By definition,  $a - b = kn, k \in \mathbb{Z}$ . Multiplying the equation by  $-1$ , we get

$$b - a = -kn.$$

$-k$  is still an integer, and thus by definition,  $b \equiv_n a$ .

**Transitive** Let  $a, b, c$  be arbitrary elements of  $\mathbb{Z}$ . Suppose  $a \equiv_n b$  and  $b \equiv_n c$ . By definition, we have  $a - b = kn, k \in \mathbb{Z}$  and  $b - c = gn, g \in \mathbb{Z}$ . Then,  $b = a - kn$ . Subbing in, we get that

$$\begin{aligned} a - kn - c &= gn \\ a - c &= (k + g)n \end{aligned}$$

By definition, we have  $a \equiv_n c$ .

□

**Question 3:** *Proof.* Suppose  $a, b, c, d \in \mathbb{Z}$ , and  $a \equiv_n c$  and  $b \equiv_n d$ . Then,

$$\begin{aligned} a - c &= nk, k \in \mathbb{Z} \\ b - d &= nl, l \in \mathbb{Z}. \end{aligned}$$

Adding the equations, we get

$$a + b - c - d = n(k + l).$$

Simplifying, we get

$$(a + b) - (c + d) = n(k + l).$$

Thus, by definition  $a + b \equiv_n c + d$ .

□

**Question 4:** (a) *Proof.* The theorem given in the proposition is equivalent to claiming that ‘If  $ab$  is even, then  $a$  is even or  $b$  is even’. We have proven this theorem to be true, so it is the case that if  $ab \equiv_2 0$ , then  $a \equiv_2 0$  or  $b \equiv_2 0$ . □

- (b) The answer is no.  $10 \times 2 = 20 \equiv_4 0$ , but  $10 \not\equiv_4 0$  and  $2 \not\equiv_4 0$ .
- (c) The answer to the question will be yes when  $n$  is a prime.

*Proof.* Suppose  $n$  is a prime, and  $a, b \in \mathbb{Z}$ . Also suppose that  $ab \equiv_n 0$ . This is equivalent to saying that  $n \mid ab$ . Because  $n$  is prime,  $\gcd(a, n)$  is either 1 or  $n$ . Consider two cases:

( $\gcd(a, n) = n$ ). Then,  $n \mid a$ .

( $\gcd(a, b) = 1$ ). luke said to appeal to the fundamental theorem of arithmetic

□