Let n be in $\mathbb{N} \setminus \{0\}$. Let k, x be in $\mathbb{Z}$. We define the congruence class $\overline{\mathrm{k}}$ of the integer k as the set

$$\overline{\mathrm{k}} = \{x \in \mathbb{Z} \mid x - k = 0 (\operatorname{mod} n)\}$$

$$x \in \mathbb{Z} \mid \exists a \in \mathbb{Z} : (x - k = n \cdot a)\}$$

We now define $\mathbb{Z}/n\mathbb{Z}$(sometimes written $\mathbb{Z}_n$) as the set of all congruence classes modulo n. Euclidean divison implies that this set is a finte set containing n elements:

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, ..., \overline{\mathrm{n - 1}}\right\}$$

For all $\overline{\mathrm{a}}, \overline{\mathrm{b}} \in \mathbb{Z}_n$, we define

$$a \oplus b := \overline{\mathrm{a+b}}$$

a . Show that $(\mathbb{Z}_n, \oplus)$ is a group. Is it abelian?

b . We now define another operation $\otimes$ for all a and b in $\mathbb{Z}_n$ as

$$a \otimes b = \overline{a \times b}$$

where $a \times b$ represents the usual multiplication in $\mathbb{Z}$.

Let $n = 5$. Draw the times table of the elements of $\mathbb{Z}_5 \setminus \left\{\overline{0}\right\}$ under $\otimes$.

Conclude that is an Abelian group.

c . Show that $\left(\mathbb{Z}_8 \setminus \left\{\overline{0}\right\}, \otimes\right)$ is not a group.

d. We recall that the ‘Bézout theorem states that two integer a and b are relatively prime (i.e $(\gcd(a, b) = 1)$if and only if there exist two integers u and v such that $au + bv = 1$. Show that $(\mathbb{Z}_n, \oplus)$ is a group if and only if $n \in \mathbb{N} \setminus \{0\}$ is prime.

We now show that $(\mathbb{Z}_n, \oplus)$ is a group

to be a group the mathematical structure must hold the following properties

- identity element
- closure for the provided operator
- each element in the set has an inverse
- associativity property

We start by proving the associativity property, $a * (b * c) = (a * b) * c$

$$a * (b * c)$$

$$x - a \oplus (x - b \oplus x - c)$$

$$x - a \oplus \overline{x - b + x - c}$$

$$\overline{x - a + \left(\overline{x - b + x - c}\right)}$$

$$\overline{x - a + \overline{(2x - b - c)}}$$

$$\overline{x - a + (0 - b \bmod n - c \bmod n)} \text{ , apply mod n operation}$$

$$\overline{x - a - \overline{b} - \overline{c}}$$

$$\overline{x - \left(a + \overline{b} + \overline{c}\right)}$$

$$\overline{x - \overline{d}}$$

$$0 - \overline{d}$$
$$\overline{d}$$

$$(a * b) * c$$

$$(x - a \oplus x - b) \oplus x - c$$

$$\overline{x - a + x - b} \oplus x - c$$

$$\overline{\overline{x - a + x - b} + x - c}$$

$$\overline{(2x - a - b) + x - c}$$

$$\overline{(0 - a \bmod n - b \bmod n) + x - c}$$

$$\overline{-\left(\overline{a} + \overline{b} + c\right) + x})$$

$$\overline{\overline{d} + x}$$

$$\overline{d}$$

we know that $\overline{d}$ must each belong to a congruence class, thus must be a number in $\mathbb{Z}_n$ so associativity holds.

now we prove identity element, $a * e = a$

$$a * e$$

$$a \oplus e$$

$$\overline{a + e}$$

$$\overline{a + 0} \text{ , set e to 0}$$

$$\overline{a}$$

note that $a \in \mathbb{Z}_n$ thus $a < n$ it must be the case that $a = \overline{a}$, thus identitiy property also holds.

now we prove the inverse property, $a * a^{-1} = e$

$$a * a^{-1}$$

$$a \oplus a^{-1}$$

$$\overline{a + a^{-1}}$$

$$\overline{a} + \overline{a^{-1}} \text{ , set the second term to be n - a}$$

$$\overline{b} = 0 = \overline{0}$$

thus note that $0 < (n - a) < n$, thus it must be the case that $\forall (n - a) \in \mathbb{Z}_n$, so inverse property holds.

now we prove closure property, $a * b \in \mathbb{Z}_n$

$$a * b$$

$$a \oplus b$$

$$\overline{a + b}$$

$$\overline{c}$$

note that $\overline{c} \in \mathbb{Z}_n$ it must be one of the congruent classes by definition of congruent class, thus closure property holds.

all previous mentioned property holds, thus this structure must be a group, now we check if such group is abelian.

to prove is abelian, is enough to $a * b = b * a$, that is check for commutativity.

$$a * b$$

$$a \oplus b$$

$$\overline{a + b}$$

$$\overline{c}$$

$$b * a$$

$$b \oplus a$$

$$\overline{b + a}$$

$$\overline{c}$$, due to commutativity of addition

note that both expressions result in the same value and such value belongs to $\mathbb{Z}_n$ thus the group is indeed abelian.

now we check the second group, $\left(\mathbb{Z}_5 \setminus \left\{\overline{0}\right\}, \otimes\right)$

first we "draw" the table for $n = 5$

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

note that is closed, by inspection, note also that identity element is preset $\overline{1}$ which is 1. each element has indeed an inverse, defined as the following pairs $(1, 4)$, $(2, 3)$, now we prove associativity

$$a * (b * c)$$

$$a \otimes (b \otimes c)$$

$$a \otimes \left(\overline{b \times c}\right)$$

$$a \otimes \left(\overline{b} \times \overline{c}\right)$$

$$\overline{a \times \left(\overline{b} \times \overline{c}\right)}$$

$$\overline{a} \times \overline{b} \times \overline{c}$$

$$(a * b) * c$$

$$(a \otimes b) \otimes c$$

$$\overline{a \times b} \otimes c$$

$$\left(\overline{a} \times \overline{b}\right) \otimes c$$

$$\overline{\left(\overline{a} \times \overline{b} \times c\right)}$$

$$\overline{a} \times \overline{b} \times \overline{c}$$

we also know that the matrix is closed, so this multipliation must be one of the congruence classes.

thus the mathematical structure is a group, now we prove is abelian, $a * b = b * a$

$$a * b$$

$$a \otimes b$$

$$\overline{a \times b}$$

$$\overline{c}$$

$$b * a$$

$$b \otimes a$$

$$\overline{b \times a}$$

$\overline{c}$, note that multiplation is commutative

thus this group is indeed abelian, so $(\mathbb{Z}_5 \setminus \{\overline{0}\}, \otimes)$ is an abelian group.

now we prove $(\mathbb{Z}_8 \setminus \{\overline{0}\}, \otimes)$ is not a group

we prove by counterexample

	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	6
7	7	6	5	4	3	6	1

note that multiple times $a * b \equiv 0$ thus belongs to $\overline{0}$ and such congruence class is restricted in the set $\mathbb{Z}_8 \setminus \{\overline{0}\}$, so is not a group, lacks closure.

now we prove d)

we need to prove that $\mathbb{Z}_n \setminus \{\overline{0}\}$ is a group $\Rightarrow n$ is prime and if n is prime $\Rightarrow \mathbb{Z}_n \setminus \{\overline{0}\}$ is a group

let's do a contrapositive proof

suppose n is not prime, then it must be the case that

$$x \equiv 0 \bmod n$$

that is one of the numbers must be a divisor of n, by definition of being composite but note that would invalidate $x \in \mathbb{Z}_n \setminus \{\overline{0}\}$, that would put $x \in \overline{0}$, but the set restricts this congruence class, thus it must be the case that n is prime, otherwise a contradiction happens.

now we prove the other proposition

recalling Bézout's identity

$\gcd(a, b) = 1 \Leftrightarrow au + bv = 1$

thus

$xu + bn = 1$

meaning that $xu - 1 = bn \Rightarrow x \equiv 1 \mod n$

note that $x, x + 1, ...x + (n - 2)$ must be present in this set

meaning every number in the congruence class $\overline{1}$ to $\overline{n - 1}$ is present thus $\left(\mathbb{Z}_n \setminus \{\overline{0}\}, \otimes\right)$ is a group, note that is closed, has identity, has inverse and also is associative. ■