Question: What is the current time?

Answer: (For example) 10 AM (or 10:00 hours)

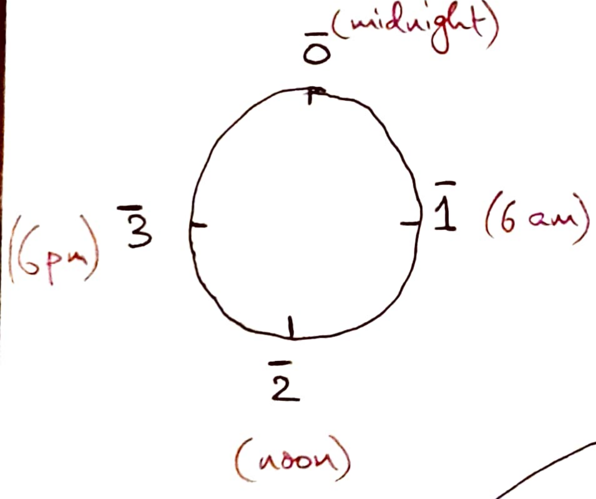
Question: What will the time be after 16 hours?

Answer: $10+16=26:00$ hours? Of course, NOT.

2 AM (or 02:00 hours).

Basically, we "reset to ZERO" at every 12/24 hours (depending on whether we're thinking about a 12 hour or a 24 hour clock). This brings us to RINGS.

Let's consider a simpler clock with just "4 times":



Questions:

① What is $\bar{2}+\bar{2}$? $\bar{0}$

② What is $\bar{1}+\bar{1}$? $\bar{2}$

③ What is $\bar{1}+\bar{3}$? $\bar{0}$

④ What is $\bar{3}+\bar{3}$? $\bar{2}$

⑤ What is $\bar{3}+\bar{0}$? $\bar{3}$

You get the point, right?

Addition Table:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$		$\bar{2}$		$\bar{0}$
$\bar{2}$			$\bar{0}$	
$\bar{3}$	$\bar{3}$			$\bar{0}$

DIY: Fill the rest yourself.

What are the properties of this "addition operation"?

① **Associativity**: $(a+b)+c = a+(b+c)$

② **Commutativity**: $a+b = b+a$

③ **Existence of Additive Identity** (generally denoted by 0)

$a+0=a$

($0+a=a$ by commutativity)

④ **Existence of Additive Inverse**

$\forall a \; \exists (-a)$ such that $a+(-a) = \underset{\text{additive identity}}{0}$

Required in definition of RING (coming soon)

Can we also define a reasonable/natural multiplication operation for our set $\{\bar{0},\bar{1},\bar{2},\bar{3}\}$? (Yes, you may think of it as repeated addition.)

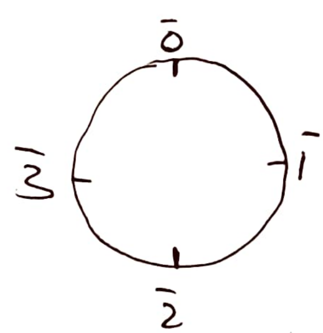
Questions:

① what is $\bar{3}*\bar{3}$? $\bar{1}$

② what is $\bar{2}*\bar{3}$? $\bar{2}$

③ what is $\bar{1}*\bar{3}$? $\bar{3}$

④ what is $\bar{2}*\bar{2}$? $\bar{0}$



Multiplication Table:

$*$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$			$\bar{0}$	$\bar{2}$
$\bar{3}$		$\bar{3}$		$\bar{1}$

You get the point, right?

DIY: Fill the rest yourself.

Question: What are the properties of this "multiplication operation"?

① **Associativity:** $a * (b * c) = (a * b) * c$

② **Existence of Multiplicative Identity** (generally denoted by 1)

$a * 1 = a$

$1 * a = a$

Required in definition of RING (coming soon)

ALSO:

③ **Commutativity:**

$a * b = b * a$

BUT $\boxed{\text{NOT}}$:

④ Existence of Multiplicative Inverse

$\forall a$ (except 0) — additive identity

$\exists\, a^{-1}$ such that

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

$a^{-1} * a = 1$ — multiplicative identity

NOT required in definition of RING (coming soon)

Note that, in our example, addition & multiplication also satisfy:

Distributivity of Multiplication over Addition:

$$a * (b + c) = (a * b) + (a * c)$$

$$(b + c) * a = (b * a) + (c * a)$$

Such an "algebraic set" R is called a RING.

(Full definition on next page)

Why NOT?

Observe that $\bar{2} * \bar{0} = \bar{0}$, $\bar{2} * \bar{1} = \bar{2}$, $\bar{2} * \bar{2} = \bar{0}$ & $\bar{2} * \bar{3} = \bar{2}$.

So, $\bar{2}$ has NO multiplicative inverse.

A set R — with an "addition" $(+)$ & a "multiplication" $(*)$ operation — is called a RING — often denoted as $(R, +, *)$ — IF it satisfies the following properties:

Properties of $+$:

1. Associativity: $\forall a,b,c \in R$,
   $(a+b)+c = a+(b+c)$
2. Commutativity: $\forall a,b \in R$,
   $a+b = b+a$
3. Existence of Additive Identity (0):
   $\exists\ 0 \in R$ such that
   $\forall a \in R,\ a+0 = a$
4. Existence of Additive Inverse:
   $\forall a \in R,\ \exists\ b \in R$
   such that $a+b = 0$ $\xrightarrow{}$ additive identity

   such b is also denoted as $-a$ since it is unique (DIY: prove)

Properties of $*$:

5. Associativity: $\forall a,b,c \in R$,
   $(a*b)*c = a*(b*c)$
6. Existence of Multiplicative Identity (1):
   $\exists\ 1 \in R$ such that
   $\forall a \in R$:
   $a*1 = a$
   & $1*a = a$

AND

7. Distributivity of Multiplication over Addition:
   $\forall a,b,c \in R$,
   $a*(b+c) = (a*b)+(a*c)$
   & $(b+c)*a = (b*a)+(c*a)$

ALSO closure properties (often NOT stated explicitly):
$\forall a,b \in R$,
$a+b \in R$ AND $a*b \in R$ & $b*a \in R$

What are some examples of rings?

① We just saw one: $(R := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, +, *)$ with $+$ & $*$ defined on previous pages.

This is a <u>finite ring</u> since R is a finite set.

② Do we know any infinite ring?

YES: $(\mathbb{Z}, +, *)$ → the set of all integers with addition & multiplication as we know them

This is an <u>infinite ring</u>.

<u>DIY</u>: $(\mathbb{N}, +, *)$ is NOT a ring. Why?

Let's consider the finite ring $(R := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, +, *)$ again, and consider a different way of looking at it. (We will assume <u>Euclid's division Lemma</u>.)

In particular, every integer on division by 4 leaves a remainder of <u>0, 1, 2 OR 3.</u>

The elements of R may be thought of as follows:

$\bar{0} := \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$\bar{1} := \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

$\bar{2} := \{\ldots, -6, -2, 2, 6, 10, \ldots\}$

$\bar{3} := \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

this gives us a partition of $\mathbb{Z}$

Given $a, b \in \mathbb{Z}$, where $b \neq 0$, $\exists$ unique integers q & r such that $a = bq + r$ and $0 \leq r \leq |b| - 1$

q aka quotient

r aka remainder

Wherever there is a partition, there IS an equivalence relation: we say that $a, b \in \mathbb{Z}$ are <u>congruent modulo 4</u> if $4 \mid (a-b)$, OR equivalently, if a leaves the same remainder on division by 4 as b does.

<u>DIY</u>: Prove that these two definitions are same (assuming Euclid's Lemma)

<u>DIY</u>: Prove that "congruence modulo 4" is an equivalence relation on $\mathbb{Z}$.

<u>DIY</u>: Generalize to "congruence modulo k" where $k \in \mathbb{N} - \{0,1\}$.

<u>DIY</u>: What does "congruence modulo 2" mean? What are the corresponding congruence/equivalence classes.

The corresponding equivalence classes are precisely $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ (as defined on previous page)

these are also called <u>congruence (modulo 4) classes</u> of $\mathbb{Z}$

Now, the addition & multiplication operations on $R := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ can be thought of in the following manner:

<u>Question</u>: What is $\bar{3} * \bar{3}$?

<u>Answer</u>:

$3 * 3 = 9$ (in integers)

9 gives remainder of 1 on division by 4.

Thus $\bar{3} * \bar{3} = \bar{1}$. :-)

The finite ring we have been discussing so far is generally denoted by $\mathbb{Z}/4\mathbb{Z}$ and is called the ~~ring~~ integers modulo 4 ring.

DIY: Generalize this to $\mathbb{Z}/k\mathbb{Z}$ $\forall k \in \mathbb{N} - \{0,1\}$.
(This gives us infinitely many finite rings. :-))

Now, let's discuss some more "special rings".

A ring $(R,+,*)$ that satisfies commutativity for multiplication ($*$) is called a commutative/Abelian ring.

$\forall a,b \in R$:
$a*b = b*a$

named after a mathematician called Abel of course!

Furthermore, a commutative ring $(R,+,*)$ is called a $\boxed{\text{FIELD}}$ if it satisfies:

Existence of Multiplicative Inverse:
$\forall a \in R - \{0\}$, $\exists$ an element $b \in R$ such that $a \cdot b = 1$ → multiplicative identity

additive identity

such an element is unique (DIY) and is denoted by a^{-1}

Do we know of any fields?

YES: $(\mathbb{Q}, +, *)$ & $(\mathbb{R}, +, *)$ — these are infinite fields

$\mathbb{Q}$ → rational #s; $\mathbb{R}$ → real #s

with addition & multiplication as we know them.

What about finite fields?

The smallest finite field is $\mathbb{Z}/2\mathbb{Z}$ with addition & multiplication defined below:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$*$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Some cool interpretations:

congruence modulo 2 classes of $\mathbb{Z}$

① Think of $\bar{0}$ as all EVEN #s & think of $\bar{1}$ as all ODD #s

$\bar{0} + \bar{1} \xleftrightarrow[\text{as}]{\text{same}}$ EVEN + ODD = ODD $\xleftrightarrow[\text{as}]{\text{same}} \bar{1}$

$\bar{1} * \bar{0} \xleftrightarrow[\text{as}]{\text{same}}$ ODD * EVEN = EVEN $\xleftrightarrow[\text{as}]{\text{same}} \bar{0}$

② Think of $\bar{0}$ as FALSE & think of $\bar{1}$ as TRUE

Now + is SAME AS XOR & * is SAME AS AND :-)

Question: Consider $q \in \mathbb{N} - \{0,1\}$.
When is the RING $\mathbb{Z}/q\mathbb{Z}$ a FIELD?

Answer:

$\mathbb{Z}/q\mathbb{Z}$ is a FIELD $\iff$ q is a prime.

This can be proved using Bezout's Lemma:

$\forall\, a,b \in \mathbb{Z},\ \exists\, x,y \in \mathbb{Z}$ such that $ax + by = \underline{GCD(a,b)}$

GCD of a & b

(For example, if $a = 15$ & $b = 69$;
consider $15 \cdot (-9) + 69 \cdot (2) = 3 = GCD(15, 69)$.)

TIY: (beyond CS1200)
Use Bezout's Lemma to prove that $\mathbb{Z}/q\mathbb{Z}$ is a field if and only if q is a prime.

Rings & Fields (and other such algebraic sets/structures such as Groups) find lots of applications in computer science – especially in Cryptography but also in other areas like Graph Theory.