# Aritmética del reloj

Mate 3041

Profa. Milena R. Salcedo Villanueva

# Aritmética del Reloj

**El médico:** Ahora son las 10 de la mañana. Tome la próxima pastilla a las 2 de la tarde, y luego una cada 8 horas.

**El paciente:** OK. Entonces tomo la próxima a las 2 de la tarde, luego a las .... 2 más 8 ... eso es a las 10 de la noche, otra a las 10 más 8 ... a las 6 de la mañana, después a las 6 más 8 ... 14, ¡ah! de nuevo a las 2 de la tarde. Entonces sigo así: a las 2 de la tarde, a las 10 de la noche y a las 6 de la mañana. Muchas gracias (ver figura 4.1). Hasta luego.

***¡Qué manera de sumar! ¿Así que 10 + 8 = 6? ¡Qué bonito!***

# Aritmética del Reloj

Bueno.... Sí, en la aritmética del reloj sí.

No es difícil encontrar otras situaciones donde esta aritmética: la aritmética del reloj, cíclica o modular, aparece naturalmente.

**El médico:** Bueno, hoy es martes. A ver..., vuelva entonces en 10 días.

**El paciente:** Muy bien. No hay problema. Hoy es martes, en 10 días será..., perfecto viernes. Estaré desocupado. Muchas gracias.

Recopilando tenemos que:

En la aritmética del reloj

$$10 + 8 = 6$$

$$2 + 10 = 0.$$

En la aritmética de la semana

Si le ponemos números a los días de la semana, empezando con domingo = 0, lunes = 1, martes = 2, etc., resulta que martes + 10 = 2 + 10, que ya sabemos da viernes = 5. Es decir, en la aritmética de la semana 2 + 10 = 5.

$$2 + 10 = 5$$

# Aritmética del Reloj

Tenemos una aritmética finita cuando se utiliza un sistema de numeración que vuelve periódicamente sobre sí mismo. Por ejemplo:

Contar las horas de un reloj o minutos.

Gauss se dió cuenta que debía empezar a contar desde cero y con esta sencilla observación investigó este sistema llamado la Aritmética modular, tambien llamada aritmética del reloj.

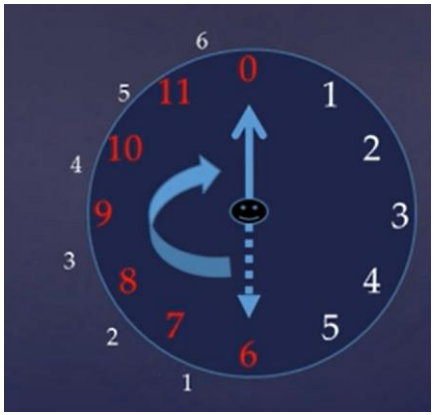
# Aritmética del Reloj

La aritmética del reloj está basada en la carátula de un reloj ordinario, con la diferencia qye el 12 es reemplazado por cero.

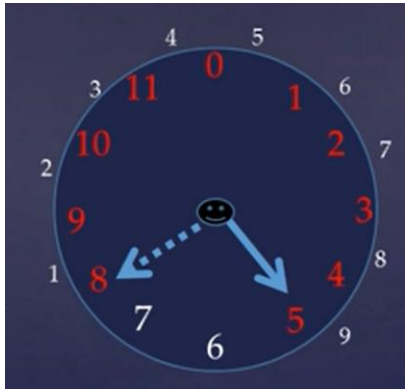
# Aritmética del Reloj

Notemos que en el Sistema del reloj:

$$5 + 2 = 7$$


$$6 + 6 = 0$$




$$8 + 9 = 5$$

# Tabla de la adición para un reloj de 12 horas

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 11 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Esta tabla presenta todas las posibles sumas para un Sistema finite de números $\{0,1,2,3,4,5,6,7,8,9,10,11\}$

La linea diagonal divide la tablaen dos partes iguales por tanto el Sistema cumple con la propiedad conmutativa

# Propiedades en la adición de la aritmética del Reloj

**Propiedad Conmutativa:**

$$a + b = b + a$$
$$5 + 9 = 9 + 5$$
$$2 = 2$$

**Propiedad Asociativa:**

$$(a + b) + c = a + (b + c)$$
$$(4 + 5) + 9 = 4 + (5 + 9)$$
$$9 + 9 = 4 + 2$$
$$6 = 6$$

# Propiedades en la adición de la aritmética del Reloj

**Propiedad Identidad:**

$$a + 0 = 0 + a$$
$$4 + 0 = 0 + 4$$
$$4 = 4$$

El elemento identidad para suma en la aritmética del reloj es cero “0”

# Sistemas Modulares

En matemática, la aritmética modular es un sistema aritmético para **clases de equivalencia** de números enteros llamadas **clases de congruencia**.

La aritmética modular fue introducida en 1801 por Carl Friedrich Gauss en su libro Disquisitiones Arithmeticae.

En otras palabras los sistemas modulares son un conjunto de métodos que permiten la solución de problemas sobre los números enteros.

Estos métodos surgen del estudio del residuo obtenido de una división.

Cuando queremos encontrar $15\ mod\ (4)$ lo que realmente queremos encontrar el residuo de divide $15$ entre $4$.

En otras palabras el modulo $(mod)$ corresponde al divisor que indica el numero de particiones que tendriamos que hacer de un número entero, así que si queremos calcular

$$a\ mod\ (n) = residuo\ de\ a \div n$$

# Ejemplos

Obtenga el residuo en cada caso

1. $13 \bmod (5) = 3$, puesto que $3$ es el residuo de la división de $13$ entre $5$
2. $49 \bmod (5) = 4$, puesto que $4$ es el residuo de la división de $49$ entre $5$
3. $75 \bmod (10) = 5$, puesto que $5$ es el residuo de la división de $75$ entre $10$

# Relación de Congruencia

La aritmética modular puede ser construida matemáticamente mediante la relación de congruencia entre enteros, que es compatible con las operaciones en el anillo de enteros: suma, resta, y multiplicación. Para un determinado módulo $n$, ésta se define de la siguiente manera:

***$a$ y $b$ se encuentran en la misma "clase de congruencia" módulo $n$, si ambos dejan el mismo resto si los dividimos entre $n$, o, equivalentemente, si $a - b$ es un múltiplo de $n$.***

# Relación de Congruencia

Esta relación se puede expresar cómodamente utilizando la notación de Gauss

$$a \equiv b \bmod(n)$$

Así por ejemplo:

$$63 \equiv 83 \bmod(10)$$

Ya que ambos, $63$ y $83$ tiene el mismo residuo al dividir entre $10$, o equivalentemente, $63 - 83$ da como resultado un múltiplo de $10$.

Se lee: “ $63$ es congruente con $83$ módulo $10$” o “$63$ y $83$ son congruentes uno con otro, módulo $10$”

# Relación de Congruencia

«Módulo» a veces se abrevia con la palabra «mod» al hablar, de la misma manera que como está escrito y proviene de la palabra *modulus* del **latín**, la lengua de los escritos originales de Gauss. Así, el número $n$, que en este ejemplo es $10$, sería el **modulo**

Cuando el módulo es $12$, entonces cualesquiera dos números que divididos entre doce den el mismo resto son equivalentes (o "congruentes") uno con otro. Los números

$$\ldots, -34, -22, -10, 2, 14, 26, \ldots$$

son todos "congruentes módulo $12$" unos con otros, ya que cada uno deja el mismo **residuo** $(2)$ cuando los dividimos entre $12$. La colección de todos esos números es una clase de congruencia.

# Propiedades

Para cualquier entero fijo $n \geq 1$ se verifican las propiedades:

1. Reflexiva: $a \equiv \mathrm{a} \bmod (n)$ para cualquier entero $a$
2. Simétrica: $a \equiv b \bmod (n) \Rightarrow b \equiv a \bmod (n)$
3. Transitiva: $\left.\begin{array}{l} a \equiv b\ mod\ (n) \\ b \equiv c \bmod (n) \end{array}\right\}$ entonces $a \equiv c \bmod (n)$

Estas tres propiedades definen una relación de equivalencia, por lo que para cada entero $n$, la congruencia modulo n es una relación de equivalencia en $\mathrm{Z}$.

# Ejemplos para verificar propiedades

Para cualquier entero fijo $n \geq 1$ se verifican las propiedades:

1. Reflexiva: $5 \equiv 5 \bmod (2)$ para cualquier entero a
2. Simétrica: $5 \equiv 8 \bmod (3) \Rightarrow 8 \equiv 5 \bmod (3)$
3. Transitiva: $\left.\begin{matrix} 5 \equiv 9\, mod\ (4) \\ 9 \equiv 13 \bmod (4) \end{matrix}\right\}$ entonces $5 \equiv 13 \bmod (4)$