Asociación Castellana y Leonesa de Educación Matemática Miguel de Guzmán

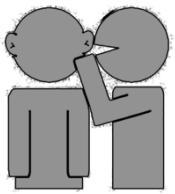
ESTÍMULO DEL TALENTO MATEMÁTICO

INT3GRID4D D3 LA TR4NSMSI0N D3 DATOS

INTRODUCCIÓN

Hay dos tipos de problemas que se plantean en la comunicación.

El primero consiste en la transmisión fiel de la información. Los canales de comunicación a través de los cuales se transmite un mensaje pueden tener algún tipo de "ruido" haciendo que el mensaje llegue al receptor modificado. Es necesario utilizar técnicas que nos permitan identificar si se ha producido algún error en el mensaje y, si es posible, corregirlo. Este tipo de estrategias puede utilizarse también para garantizar la integridad de un mensaje contra manipulaciones intencionadas.



Otro tipo de problema posible es la necesidad de transmitir mensajes de una manera segura. Si la información tiene un cierto valor es deseable que sólo el destinatario pueda entenderlo o utilizarlo.

Las matemáticas, especialmente el álgebra y la divisibilidad, tienen mucho que decir en ambos tipos de problemas, pero hoy vamos a centrarnos solo en el primero.

CONCEPTOS MATEMÁTICOS BÁSICOS

ARITMÉTICA MODULAR

Es el nombre que se le da a la forma de contar de las horas del reloj en matemáticas. La definición rigurosa es:

Dados dos números enteros a, b y un número natural m se dice que a es congruente con b módulo m si $a - b$ es divisible entre m. Se denota:

$$a \equiv b \; mod \; m$$

A modo de ejemplo $14 \equiv 2 \; mod \; 12$ porque $14 - 2 = 1\dot{2}$ cuando los tres son números naturales el concepto corresponde a tener el mismo **resto** al dividir entre m.

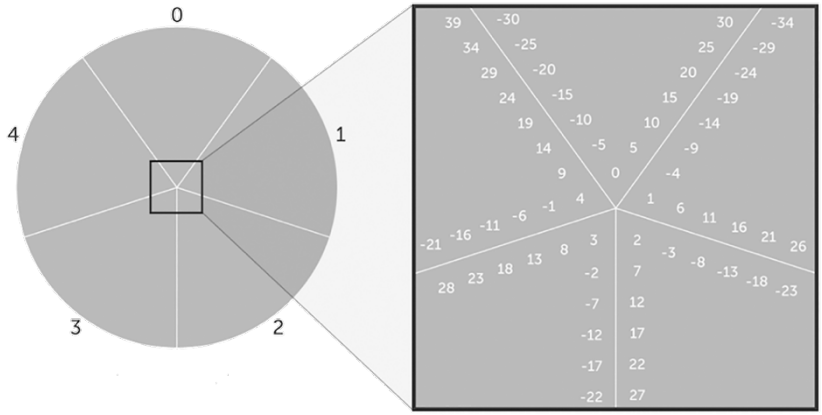
Ejemplo:

Si son las 10 ¿Qué hora será dentro de 8532h?

Respuesta: $10 + 8532 = 8542$ dividiendo entre 12 obtenemos 711 de cociente y 10 de resto, por tanto $8542 \equiv 10 \; mod \; 12$

¿Cómo podemos hacer esto con la calculadora?

La relación de igualdad módulo m separa los números enteros en grupos llamados *clases de equivalencia*, así las clases de equivalencia módulo 5 son



PRODUCTO ESCALAR

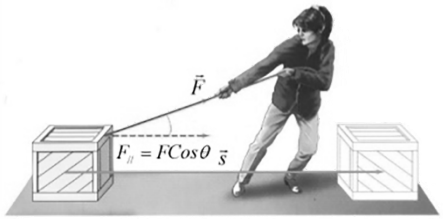
Dados dos conjuntos de n números reales $(a_{1,}\, a_{2,}, \dots, a_{n,})$ y $(b_{1,}\, b_{2,}, \dots, b_{n,})$ se llama producto escalar al número $a_{1,} \cdot a_1 \; + \; a_{2,} \cdot b_2 \; + \cdots + a_{n,} \cdot b_n$

Se denota con el mismo símbolo del producto de números reales: ·

Ejemplos:

$$(1, 3, -2) \cdot (2, 0, 5) = 1 \cdot 2 + 3 \cdot 0 + (-2) \cdot 5 = -8$$
$$(5, 7) \cdot (4, 2) = 5 \cdot 4 + 7 \cdot 2 = 34$$

Este concepto es fundamental en Matemáticas, uno de sus usos habituales es en los espacios vectoriales y afines, pues sirve para definir la medida, tanto de distancias como de ángulos (incluyendo paralelismo y perpendicularidad o proyecciones). También en Física donde se utiliza para en la definición de algunas magnitudes como el trabajo



$$\boxed{W = \vec{F} \bullet \vec{s}}$$

$$\boxed{W = FsCos\theta}$$

La aplicación que vamos a usar aquí de esta operación nos servirá para dar soporte matemático a algunos conceptos. Uno de los usos más interesantes (pese a lo simple) es el trabajo con números y separar sus cifras o cambiarlas de posición.

$$372 = (3, 7, 2) \cdot (10^2, 10^1, 10^0)$$
$$327 = (3, 2, 7) \cdot (10^2, 10^1, 10^0)$$

También se utiliza para asignar pesos a determinadas cantidades en algunos de los criterios que emplearemos para establecer dígitos y caracteres de control que permitan detectar (e incluso reparar) errores en la transmisión de datos.

CÓDIGOS

Llamaremos códigos a los sistemas que nos permitan identificar (o incluso corregir) errores en la transmisión de información. Algunos ejemplos:

REDUNDANCIA

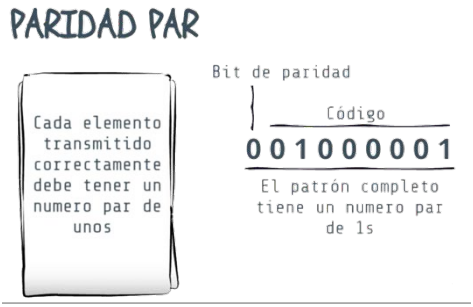
Son palabras o caracteres innecesarios para expresar un concepto por poder sobreentenderse sin ellas (p. ej. “hueco por dentro”). Los lenguajes naturales tienen un cierto grado de redundancia que nos permite interpretar el título de esta sesión a pesar de tener errores en algunas letras.

REPETICIÓN

Uno de los códigos más básicos consiste en la repetición de la información, enviando cada dato varias veces. Así si quiero aseguraros de que no confundís PABLO con PAOLO puedo enviar PABLO-PABLO de manera que si recibís PABLO-PAOLO podéis detectar que ha habido un error, aunque no podéis saber cual es el correcto. Una manera de solucionar esto sería enviar los datos tres veces PABLO-PABLO-PABLO, en este caso, la recepción PABLO-PAOLO-PABLO permitiría asegurar con un alto grado de certeza donde está el error.

El problema de este sistema es que es muy ineficiente, ralentiza mucho las comunicaciones ¿os imagináis teniendo que repetir tres veces cada información? (Y, aún así, la certeza al 100% no estaría garantizada).

¿Cómo podemos mejorarlo?



Las matemáticas pueden ayudarnos a crear códigos más eficientes con niveles de seguridad muy altos. Veamos ahora algunos ejemplos.

LETRA DEL DNI

Se calcula la clase de equivalencia módulo 23 y se consulta la siguiente tabla

Resto	0	1	2	3	4	5	6	7	8	9	10	11
Letra	T	R	W	A	G	M	Y	F	P	D	X	B
Resto	12	13	14	15	16	17	18	19	20	21	22	
Letra	N	J	Z	S	Q	V	H	L	C	K	E	

¿Qué letras faltan? ¿Por qué crees que se usan 23 letras en lugar de las 27?

NÚMEROS DE TARJETAS DE CRÉDITO Y NÚMEROS DE CUENTA CORRIENTE

Las tarjetas de crédito se identifican con un número de 16 cifras (que por facilidad de lectura se agrupan de 4 en 4). Los 4 primeros identifican la entidad financiera, el quinto el tipo de tarjeta (Visa, American Express…) los 10 siguientes dígitos identifican al usuario y el último es un dígito de control. Para calcular el dígito de control (o para comprobar si un número de tarjeta es correcto) se usa el algoritmo de Luhn (se consideran las posiciones de las cifras siempre de izquierda a derecha)

Se toman las cifras que están en posición impar y se calcula su producto por 2 (si el resultado tiene mas de una cifra, estas se suman) y se suman los resultados. Se añade la suma de las cifras que están en posición par (excepto el dígito de control) y, llamamos X al resultado anterior módulo 10. El dígito de control debe ser tal que, al sumarlo a X el resultado sea congruente con 0 módulo 10

Comprueba que la tarjeta de la imagen es falsa ¿Cuál debería haber sido el dígito de control para que fuera "*creíble*"?

OTRA POSIBLES APLICACIONES

El **código EAN** (European Article Numbering) es un código, habitualmente de 12+1 cifras, que permite identificar de forma única un artículo y facilita el escaneo de los mismos para agilizar el paso por caja.

Los dos o tres primeros dígitos corresponden al país y el resto, excepto el último, identifican la empresa y el producto, siendo el último un dígito de control para evitar lecturas erróneas de los escáneres.

El código ISBN (International Standard Book Number) es un sistema similar empleado para libros, originariamente constaba de 10 dígitos (9 +1 de control), pero en 2007 se añadieron 3 dígitos al principio, para ponerlo a la par con el EAN-13 además de para evitar que se agotaran los códigos disponibles, para ello se añadió el prefijo “978” que al agotarse cambiará a “979”… y se cambió la fórmula de cálculo del dígito de control.

Los **pasaportes** disponen de varios dígitos de control que faciliten su lectura electrónica, puedes comprobarlo en la última línea en la que se pueden ver varios.

CONDICIONES QUE DEBEN CUMPLIRSE PARA DETECTAR ERRORES

La capacidad de detectar errores de estos códigos viene dada por el siguiente resultado:

TEOREMA:

Si un número de identificación $x_1x_2 \dots x_k$ satisface la condición

$$(x_1, x_2, \dots, x_k) \cdot (\lambda_1, \lambda_2, \dots, \lambda_k) = 0 \ (mod\ n)$$

Entonces, se detectarán errores por el código si:

Tipo de error	Condición para ser detectado
Error simple	$mcd(\lambda_i, n) = 1$
Error por trasposición	$mcd(\lambda_{i+1} - \lambda_i, n) = 1$
Error de trasposición por salto	$mcd(\lambda_i - \lambda_j, n) = 1$

Para garantizar esto es por lo que se suelen emplean en los pesos números primos (2, 3, …) y se emplea aritmética modular con valores de n que no tengan divisores comunes con estos como el 23 de las letras del DNI.

ACTIVIDADES:

1. Las tablas de sumar y multiplicar módulo 2 son:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Comprueba que las tablas funcionan bien:

$7 \equiv 1\ (mod\ 2), \quad 6 \equiv 0\ mod(2) \quad \Rightarrow \quad 7 \cdot 6 = 1 \cdot 0 = 0$

($7 \cdot 6 = 42$ que es par, es decir, su resto al dividirlo por 2 es 0)

a. $87653199825 + 25931244524$

b. $87653199825 \cdot 25931244524$

Describe cómo le podrías explicar a un estudiante de 2.º de primaria (que acaba de aprender a multiplicar) los resultados obtenidos.

Realiza tú las tablas de sumar y multiplicar módulo 5

2. Describe, utilizando el concepto de producto escalar el aspecto que debe tener un número de 3 cifras para ser capicúa. Intercambia la cifra de las unidades y la cifra de las decenas (el nuevo número no será capicúa). Escribe una ecuación que describa que la diferencia entre el número capicúa y el segundo número es -27. Escribe una ecuación que describa que la suma de las 3 cifras del número original sea 9. Resuelve el sistema anterior y calcula el único número que cumple dichas condiciones.
3. Encuentra el DNI falso, ¿puedes garantizar la validez del otro?

4. Comprueba si la tarjeta de crédito siguiente está correctamente escaneada:

pablo1996@gmail.com
@PabloMartinPi

Este documento ha sido creado como parte de un curso de formación del profesorado del CFIE de León. Corresponde a una sesión del programa de Estímulo del Talento Matemático y su objetivo es mostrar a los docentes participantes en el curso estrategias de atención al alumnado con AA.CC.