Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Aritmética del Reloj

En las actividades 1.1 y 1.2 de la primera sesión has aprendido a cifrar y descifrar mensajes mediante uno de los métodos clásicos de llave simétrica: el cifrado de César.

Una de las características, y a la vez inconvenientes, de este tipo de cifrado es que la seguridad reside en la clave. Si por cualquier razón se descubre la clave basta con calcular la inversa para que cualquier persona pueda descifrar un mensaje aunque no vaya dirigido a él. Además si una persona necesita comunicarse de forma confidencial con bastantes personas el número de claves que necesita es muy grande. Hagamos un pequeño cálculo:

Si 6 personas se quieren comunicar entre sí con un método simétrico, pero de forma que sólo puedan descifrar los mensajes por parejas. ¿Cuántas claves necesitan?

Cada pareja debe seleccionar una clave diferente. ¿Cuántas parejas hay? El número de claves coincide con las diferentes formas de hacer parejas entre 6 personas, y esto es un problema de combinatoria muy fácil: $\binom{6}{2} = \frac{6!}{2! \cdot 4!} = \frac{6 \cdot 5}{2} = 15$

1. ¿Y si en lugar de 6 hay *n* parejas? _____

   ¿Puedes hacer un cálculo para conocer el número de claves para 1000 personas? _____

   ¿Y para 10000? _____

   ¿Y para 100000? _____

Estas cantidades te hacen una idea de la cantidad de claves diferentes que se necesitarían. Por eso han surgido otros métodos de cifrado que reciben el nombre de sistemas de clave pública que evitan este problema. Pero para estar al tanto el funcionamiento de estos sistemas es necesario conocer algunos resultados de teoría de números (una de las ramas de las matemáticas mas antiguas pero a su vez muy actual)

Algunos de estos resultados están relacionados con la Aritmética del reloj. No pienses que esta iniciativa es actual. Una de las primeras contribuciones del matemático alemán Karl Friederich Gauss (1777-1855) fue la invención de la calculadora del reloj. No era una máquina material (no olvides las fechas en que vivió Gauss), era más bien una idea que aportaba nuevas posibilidades para hacer determinadas operaciones con números eran inabordables con los métodos de cálculo que se manejaban en esa época.

Seguro que estás habituado a representar los números enteros como marcas dispuestas a lo largo de una línea recta que se extiende hasta el infinito:

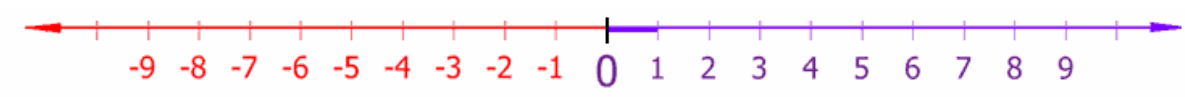


Figura 1

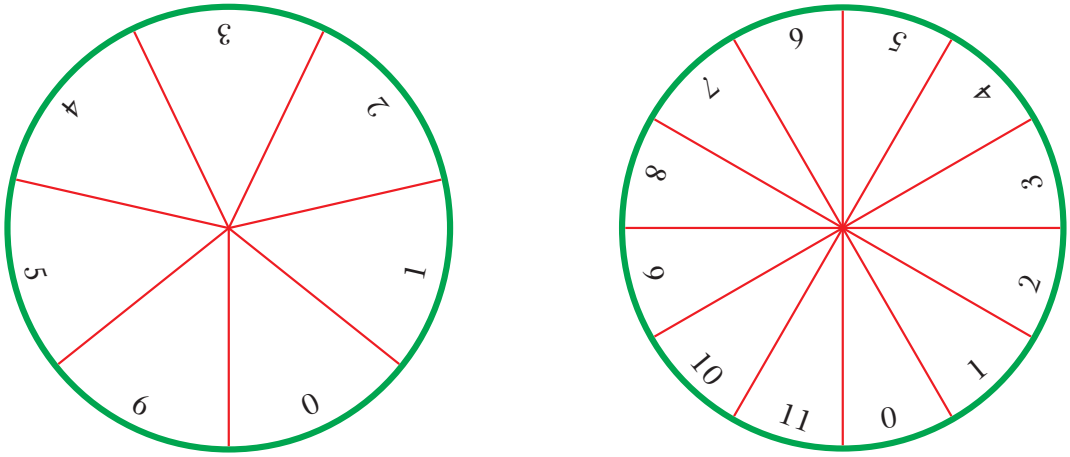
Elaborado por:
Profundiza
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

La aritmética que conoces se puede imaginar en términos de desplazamientos a derecha o izquierda a lo largo de esta recta. Ahora vas a trabajar con otra aritmética que intuitivamente lo que hace es cortar la recta en determinado punto obteniendo de esta forma un segmento (finito) y cerrar esta línea sobre sí misma para formar un círculo de números en vez de una línea.

Por ejemplo, la figura 2 muestra dos relojes de 7 y de 12 horas (la recta se ha cortado en el 7 y en el 12 respectivamente y se ha cerrado sobre sí misma). Si observas las horas empezamos a contar en el 0 y el número 7 (12) se borra ya que coincide con el 0.



Reloj 1: de 7 horas

Reloj 2: de 12 horas

Figura 2

Si vamos a trabajar con estos relojes los únicos números que podemos usar son: 0, 1, 2, 3, 4, 5 y 6 en el primero y desde 0 hasta 11 en el segundo.

Desde muy pequeño aprendiste a hacer operaciones con números enteros. La operación 3 + 2 = 5 la puedes simular como un desplazamiento a la derecha a lo largo de la recta dibujada en la figura 1: 5 es lo mismo que situarse en el 3 y moverse a lo largo de la recta 2 espacios hasta llegar al 5 (con la operación suma siempre nos movemos hacia la derecha).

Pero en la aritmética del reloj se trabaja de otra forma, por ejemplo para el reloj 1: 5 + 4 = 2 (si empezamos en el 5 y avanzamos 4 lugares en la esfera del reloj llegamos al 2). No es rara esta forma de contar, la usamos en los relojes para indicar las horas. Si ahora son las 11 de la mañana para referirnos a 4 horas más tarde no es habitual que digamos la hora 15 sino que se suele decir que serán las 3 de la tarde. El reloj es muy parecido a nuestro reloj 2 pero nosotros empezamos a contar en 0 y acabamos en 11. Esta similitud es probablemente la causa del nombre de aritmética del reloj. En ámbitos más teóricos de las Matemáticas recibe el nombre de *Aritmética modular*.

Igual que hemos trabajado con la adición podemos también representar el producto. ¿Cómo interpretamos en el reloj 2 la operación: 5 x 7? En aritmética habitual el resultado sería 35 pero esta hora no existe en nuestro reloj. Pero si meditas un poco ¿qué significa que transcurren 35 horas?: empezando a contar en 0, en la primera vuelta del reloj habrán pasado 12 horas, en una segunda vuelta otras 12 y así sucesivamente, es decir para 35 se dan 2 vueltas completas al reloj (24 horas) y aun quedan por recorrer 11 horas, por eso decimos que en esta aritmética $5 \times 7 = 11$

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
Profundiza
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Para multiplicar estos dos números no se han dado demasiadas vueltas pero si se van a multiplicar números grandes el método que acabamos de describir puede ser muy aburrido. Sin embargo existe otra operación que aprendiste en tus primeros años de formación matemática que te va a ayudar en este trabajo. Si ahora son las 12 en punto, ¿qué hora será cuando transcurran 357 horas? Debes averiguar el número de vueltas completas y caso de que sobren las que se recorren en la última vuelta. ¿Cómo dar el resultado de forma rápida? ¡Pues claro, dividiendo 357 entre 12! El cociente de la división (29) te indica el número de vueltas completas y el resto de la división (8) las horas de la última vuelta. Por eso la respuesta a la pregunta será 8 horas.

Para familiarizarte con estas operaciones usa los relojes del maletín del espía (discos 3 a 6) y piensa que hora indicará el reloj si han transcurrido las horas indicadas en la primera fila de las tablas:

Reloj de 7 horas	**0**	**4**	**7**	**11**	**127**	**536**	**–8**	**–13**	**–45**	**–536**

¿Cómo has resuelto los 4 últimos resultados?

Reloj de 12 horas	**0**	**4**	**7**	**11**	**127**	**536**	**–8**	**–13**	**–45**	**–536**

Esto mismo se puede hacer para un valor cualquiera n y se suele decir que se trabaja módulo n (recuerda que se llama aritmética modular). Para un valor n determinado, podemos considerar el conjunto A= {posibles horas que se pueden presentar} = {0, 1, 2,..., n–1}

Vamos a reflexionar un poco más sobre la forma de operar en estos conjuntos y las ventajas que tienen. Para saber el valor de n con el que se trabaja se indica (mod n), por ejemplo para el reloj 1

$$3 + 3 \equiv 6 \pmod 7$$

También usaremos esta representación para el producto: $6 \times 6 \equiv 1 \pmod 7$ (se han dado 5 vueltas completas y queda 1 hora)

Practica un poco con la suma:

$4 + 6 \equiv$ (mod 7)	$-4 + 6 \equiv$ (mod 7)	$8 + 9 + 2 \equiv$ (mod 7)
$9 + 11 \equiv$ (mod 12)	$9 + (-11) \equiv$ (mod 12)	$23 + 79 + 11 \equiv$ (mod 12)

Y ahora con el producto:

$4 \times 6 \equiv$ (mod 7)	$(-4) \times 6 \equiv$ (mod 7)	$8 \times 9 \times 2 \equiv$ (mod 7)
$9 \times 11 \equiv$ (mod 12)	$9 \times (-11) \equiv$ (mod 12)	$23 \times 79 \times 11 \equiv$ (mod 12)

¿Crees que se puede dividir en estos conjuntos? Aunque trabajemos con el conjunto de los números enteros esta pregunta no siempre tiene respuesta afirmativa. Por ejemplo en el conjunto de los números enteros no puedes dividir 5 entre 2 mientras que si puedes dividir 8 entre 2.

Elaborado por: Federación Española de Sociedades de Profesores de Matemáticas
Profundiza
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

¿Has oído alguna vez que la división es la operación inversa de la multiplicación? Esto quiere decir que $\frac{8}{4} = 8 \times \frac{1}{4} = 2$ (dividir es lo mismo que multiplicar por el inverso del denominador) pero ya sabemos que no siempre es posible encontrar este inverso.

Cuando los valores de n no son demasiado grandes resulta interesante reflejar los resultados de las dos operaciones suma y producto en una tabla. Completa las dos tablas siguiente:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3				
2							
3							
4							
5							
6							

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2				
2							
3							
4							
5							
6							

Te vamos a proponer un pequeño ejercicio: ¿puedes calcular los inversos de los valores 1 a 6 para un reloj de 7 horas. Intenta utilizar la tabla anterior para rellenar la siguiente:

número	0	1	2	3	4	5	6
inverso							

Piensa lo mismo para el reloj de 12 horas:

número	0	1	2	3	4	5	6	7	8	9	10	11
inverso												

¿Y para uno de 5 horas?

número	0	1	2	3	4
inverso					

¿Y de 6?

número	0	1	2	3	4	5
inverso						

¿Sabrías decir cuando un número cualquiera *a* tiene inverso módulo *n*?

Vamos a trabajar ahora con potencias, sabemos que para $6^2 = 6 \times 6 = 1 \pmod 7$

¿Y si ahora queremos calcular $6^3 = 6 \times 6 \times 6$ en el mismo conjunto? Una posibilidad es multiplicar estos valores y calcular el resto de la división entre 7, pero ¿se te ocurre otra idea más cómoda?

$$6 \times 6 \times 6 \equiv (6 \times 6) \times 6 \equiv 1 \times 6 \equiv 6 \pmod 7$$

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Hemos deducido el resultado sin necesidad de multiplicar $6 \times 6 \times 6$. Esta fue la idea que tuvo Gauss: podía saber, sin gran esfuerzo, que el resultado de esta operación daba de resto 6 al dividirlo por 7.

Piensa el resultado y explica la forma de usar el cálculo de uno de estos valores para el siguiente.

$6 \times 6 \times 6 \times 6 \equiv$ (mod 7)	$6 \times 6 \times 6 \times 6 \times 6 \equiv$ (mod 7)
$6 \times 6 \times 6 \times 6 \times 6 \times 6 \equiv$ (mod 7)	$6 \times 6 \times 6 \times 6 \times 6 \times 6 \times 6 \equiv$ (mod 7)

La calculadora del reloj demostró que era muy potente para trabajar con grandes números. Por ejemplo, sin tener que calcular el valor de 6^{99} su calculadora de reloj le permitía calcular que era 6 el resto de la división entre 7. ¿Puedes explicar como se llega a este resultado?

Los estudios de Gauss sobre este nuevo tipo de aritmética revolucionaron la matemática de principios del siglo XIX y ayudaron a descubrir nuevas estructuras en los números. Actualmente esta aritmética es necesaria para garantizar la seguridad en Internet donde se usan valores de n muy grandes, por ejemplo serían mayores que el número de átomos que existen en el mundo que nosotros podemos observar.

Vamos a trabajar un poco más con potencias para el reloj de 7 horas, es decir mod 7, aunque en la tabla se omite la notación todas las potencias las debes calcular con nuestro reloj

$2^0\equiv$	$2^1\equiv$	$2^2\equiv$	$2^3\equiv$	$2^4\equiv$	$2^5\equiv$	$2^6\equiv$	$2^7\equiv$	$2^8\equiv$	$2^9\equiv$	$2^{10}\equiv$	$2^{11}\equiv$
$3^0\equiv$	$3^1\equiv$	$3^2\equiv$	$3^3\equiv$	$3^4\equiv$	$3^5\equiv$	$3^6\equiv$	$3^7\equiv$	$3^8\equiv$	$3^9\equiv$	$3^{10}\equiv$	$3^{11}\equiv$
$5^0\equiv$	$5^1\equiv$	$5^2\equiv$	$5^3\equiv$	$5^4\equiv$	$5^5\equiv$	$5^6\equiv$	$5^7\equiv$	$5^8\equiv$	$5^9\equiv$	$5^{10}\equiv$	$5^{11}\equiv$
$6^0\equiv$	$6^1\equiv$	$6^2\equiv$	$6^3\equiv$	$6^4\equiv$	$6^5\equiv$	$6^6\equiv$	$6^7\equiv$	$6^8\equiv$	$6^9\equiv$	$6^{10}\equiv$	$6^{11}\equiv$

Observa los resultados y expresa lo que ha pasado

.....

Ya Gauss había usado esta propiedad para trabajar con números grandes pero incluso antes que él, otro matemático francés, Pierre de Fermat (1601-1655) había hecho un gran descubrimiento, el pequeño teorema de Fermat trabajando con relojes que tuvieran un número primo de horas, que vamos a representar por p. Para estos relojes, igual que ha pasado en nuestro ejemplo, para cualquier hora a, al calcular a^p siempre da por resultado el propio valor a.

Para p = 5, al calcular las diferentes potencias se obtiene 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1... de forma iterativa, pero si p=13 sale 3, 9, 1, 3, 9, 1, 3, 9, 1... la aguja del reloj no se detiene en todas las horas pero lo hace siguiendo un modelo iterativo. Usando la notación de Gauss el pequeño teorema de Fermat lo podemos expresar: para cualquier número primo p y cualquier valor a sobre la esfera del reloj de p horas $a^p \equiv a \pmod{p}$.

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Posteriormente, otro gran matemático el suizo Leonard Euler (1707-1783), generalizó el resultado de Fermat para relojes de N horas con la peculiaridad de que $N=p \times q$ siendo p y q dos números primos.

Estos dos resultados encontraron aplicación posteriormente cuando en 1978, Ron Rivest, Adi Shamir y Len Adleman los rescataron para idear un sistema criptográfico, conocido por RSA en su honor, y que quizás sea el cifrado de clave pública más extendido. Si quieres saber más sobre este tema, puedes acudir a la sección *para saber más*.

Elaborado por:
Profundiza
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL