Clases divulgativas – Parte II

por
M.ª Pilar Albert García
(IES Tiempos Modernos, Zaragoza)

En el anterior número de este boletín digital escribí un breve artículo en el que hablaba de dos clases divulgativas que había realizado con mis dos grupos de 1.º ESO durante la primera evaluación: *El joven Gauss sorprende a su maestro*, enmarcada dentro del tema de los números naturales y enteros, y *¿Puede doblarse un folio por la mitad más de siete veces?*, enmarcada dentro del tema de las potencias y raíces.

En esta segunda parte pondré como ejemplo dos clases divulgativas más, realizadas en la segunda evaluación, ambas encuadradas dentro del tema de la divisibilidad y los números primos. Como en el caso de las anteriores, cada una de estas clases ocupó una sesión y, después de las mismas, añadí en la prueba escrita del alumnado preguntas que hacían referencia a ellas y que les sumaban una pequeña puntuación adicional en caso de ser respondidas de forma correcta.

Clase divulgativa 3: *La criba de Eratóstenes*

En la tercera clase divulgativa hablamos un poco de Eratóstenes. Quién era (famoso matemático, astrónomo y geógrafo griego), cuándo vivió (200 a.C.), etc. Les comenté que se debían acordar de él porque lo nombraríamos más adelante, ya que haríamos una nueva clase divulgativa sobre este personaje, cuando viésemos los temas de geometría. Eratóstenes es conocido por ser la primera persona en calcular la medida de la circunferencia de la Tierra, y eso lo trataremos, como digo, con posterioridad.

Les entregué una hoja en la que aparecen los números desde el 1 hasta el 100 ordenados de 10 en 10 y utilizamos la sesión entera para realizar la criba de Eratóstenes. Recordamos primero varios aspectos: la definición de número primo, el hecho de que el número 1 no es ni primo ni compuesto, la definición de múltiplo de un número, etc. Buscamos también la definición de «criba» (casi nadie sabía lo que es), y luego comenzamos tachando los múltiplos de 2, los de 3, etc. Por cierto, definición de criba que aparece en el dicccionario de la RAE es «selección rigurosa».

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 1. Plantilla con los números del 1 al 100

Finalizada la criba, remarcamos bien los números que habían quedado sin tachar, y ya sabíamos que estos han de ser los primeros números primos. Este cuadro lo pegaron en su cuaderno ya que les será de gran utilidad pues en días posteriores echarán mano de él para averiguar si un cierto número (menor que 100) es primo o no, y también para contestar cuestiones tales como «averigua cuáles son los múltiplos de 2 y de 3 a la vez», etc.

Como nota comentar que suelo hablar de la criba de Eratóstenes siempre que introduzco el tema de los números primos en 1.º ESO, pero es la primera vez que invierto una sesión entera para dicha finalidad. Creo que a partir de ahora lo seguiré haciendo así, pues es interesante ver cómo el alumnado poco a poco va encontrando los números primos y descubre el sentido a la «receta» del «2, 3, 5, 7, 11, 13, 17, 19…».

Clase divulgativa 4: *Números primos y seguridad en internet*

Esta clase divulgativa comienza con una presentación mediante la que pretendo hacerles entender la importancia de codificar un mensaje para evitar que sea interceptado por personas no autorizadas. La primera diapositiva de dicha presentación es una imagen en la que se ven algunos de los principales elementos de la comunicación (emisor–mensaje–receptor), a los que en seguida nos damos cuenta de que hay que añadirle un par de conceptos más, la «codificación» y la «descodificación», para que esta comunicación sea segura en el caso de que estemos realizándola a través de internet.

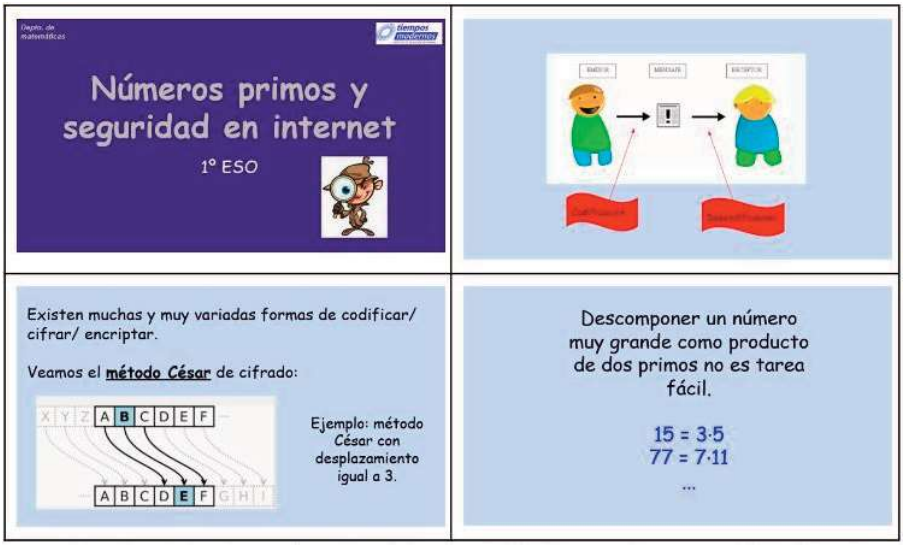


Figura 2. Portada y algunas diapositivas de la presentación *Números primos y seguridad en internet*

Para entender mejor en qué consiste esto de la codificación y la descodificación, les hablé del método César de cifrado, que les resulta muy fácil de entender y rápido de aplicar. Recuerdo aquí que este método simplemente consiste en sustituir cada letra de un determinado mensaje que se quiera enviar por la letra que le corresponde «tres lugares más hacia adelante» en el alfabeto. Así es como se comunicaba Julio César con sus militares cuando quería que sus mensajes no pudieran ser interceptados por el enemigo. Para descodificar un mensaje simplemente hay que hacer lo contrario: sustituir la letra del mensaje recibido por la que le corresponde «tres lugares más hacia atrás» en el alfabeto, y listo. Esto se conoce como usar desplazamiento igual a 3.

Les comenté a los alumnos/as que para el desplazamiento han de elegir un número mayor que uno (no necesariamente ha de ser tres) y por ejemplo menor que ocho (esto último para que no estén contando muchos lugares en el alfabeto y se puedan confundir), y les pedí que enviasen un mensaje a un compañero/a de clase para que lo descifre. Lo verdaderamente importante aquí es que tanto emisor como receptor son ambos conocedores del número que se va a utilizar para hacer el desplazamiento en el alfabeto (tres, o el que sea): el emisor para poder codificar correctamente su mensaje, y el receptor para poder descodificarlo sin problema. Y la verdad es que están bastante entretenidos/as haciendo esta labor.

Después de unos cuantos minutos haciendo esto, y cuando ya parece que hemos terminado, les pregunto: «¿pero qué relación tiene todo esto que estamos haciendo con los números primos?». Porque claro, no se ve la relación del cifrado César con el título de la sesión, que relaciona los números primos y la seguridad en internet.

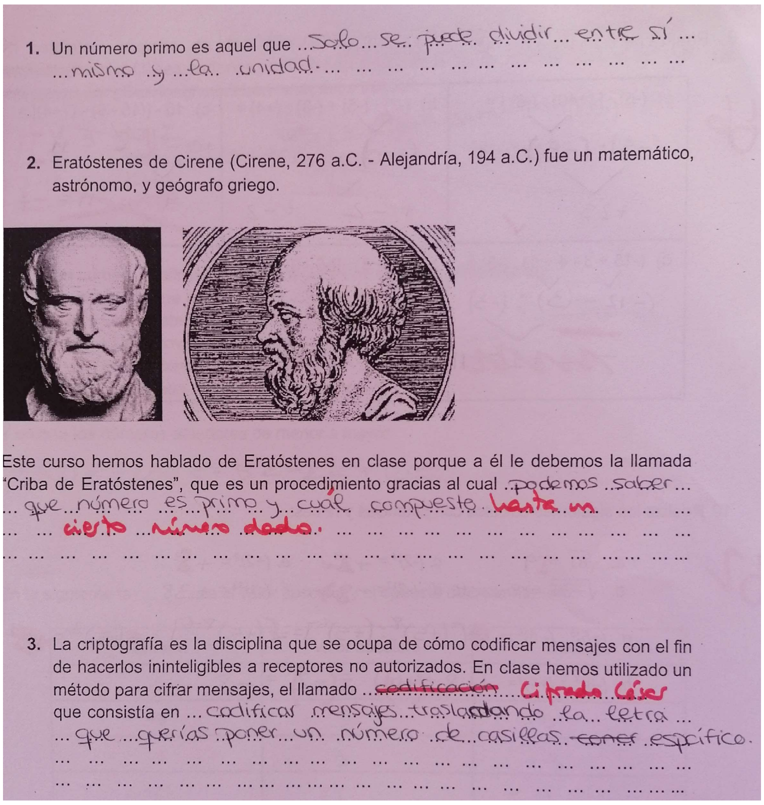
Aquí es cuando les expliqué que en internet, claro, las cosas no son tan sencillas. En primer lugar, con el cifrado César estamos utilizando un tipo de cifrado que es *simétrico*, en el sentido de que, como comentaba anteriormente, tanto el emisor como el receptor usan el mismo número como desplazamiento para codificar o descodificar mensajes. En internet el cifrado es *asimétrico*. La forma de codificar sería más bien, y simplificando mucho, algo así: podríamos decir que cada receptor puede decidir el desplazamiento con el que quiere que le sean codificados los mensajes que se le envíen, por ejemplo, desplazamiento igual a 15. Y esta información la conoce todo el mundo (es la *clave pública* del receptor). Pero dicho receptor o receptora, en realidad usará para descodificar los mensajes desplazamiento igual a 3, y eso, solo lo sabe él o ella (es su *clave privada*).

Más ejemplos serían:

clave pública para codificar 6 $\longrightarrow$ clave privada para descodificar 2
clave pública para codificar 21 $\longrightarrow$ clave privada para descodificar 3
clave pública para codificar 77 $\longrightarrow$ clave privada para descodificar 7
…

Es decir, conocida la clave pública, que es producto de dos números primos, la clave privada podría ser, por ejemplo, el divisor primo más pequeño. Pero eso solo lo sabría el receptor/a.

Claro, la clave privada es fácil de averiguar cuando tratamos con productos de dos primos pequeños ($2 \cdot 3$, $3 \cdot 7$, $7 \cdot 11$, …) pero en realidad en internet se usan números muy grandes para elegir estas claves (por muy grandes nos referimos a que cada primo que se multiplica puede tener 700 dígitos). Y gracias a esto el envío de mensajes y las transacciones que realizamos en internet son seguras: porque factorizar un número tan enorme es imposible. Y podríamos continuar hablando sobre eso y profundizar: si la clase da para más, se puede aquí continuar comentando los problemas del milenio, los que tienen que ver con los números primos, etc. Pero en una sesión, no suele dar mucho tiempo para llegar hasta aquí.



1. Un número primo es aquel que ...Solo... se... puede dividir... entre sí ... ...mismo y ...la... unidad.

2. Eratóstenes de Cirene (Cirene, 276 a.C. - Alejandría, 194 a.C.) fue un matemático, astrónomo, y geógrafo griego.

Este curso hemos hablado de Eratóstenes en clase porque a él le debemos la llamada "Criba de Eratóstenes", que es un procedimiento gracias al cual ...podemos saber... que número es primo y cuál compuesto hasta un cierto número dado.

3. La criptografía es la disciplina que se ocupa de cómo codificar mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. En clase hemos utilizado un método para cifrar mensajes, el llamado ...~~codificación~~ Cifrado César que consistía en ... codificar mensajes trasladando la letra ... que querías poner un número de casillas específico.

Figura 3. Preguntas adicionales en prueba escrita de 1.º de ESO

Como en otras ocasiones, días después en la prueba escrita sobre el tema de divisibilidad y números primos, añado unas preguntas opcionales sobre estas clases divulgativas que suman 0,3 puntos a la nota obtenida en dicha prueba.

Como comentario final debo decir que esta clase divulgativa me dio muy buen resultado con el alumnado de mis dos grupos de 1.º de ESO, por lo que decidí ofertarla como taller para el programa de Conexión Matemática, de modo que otros institutos pudieran trabajar este tema tal y como lo había hecho yo en mis clases. Fueron dos los institutos que solicitaron el taller, el IES Pilar Lorengar de Zaragoza y el IES Benjamín Jarnés de Fuentes de Ebro (en el segundo caso, el taller estuvo enmarcado dentro de su semana matemática, que culminó el sábado con

Figura 4. Momento de la sesión con los alumnos/as de 2.º de ESO del IES Benjamín Jarnés

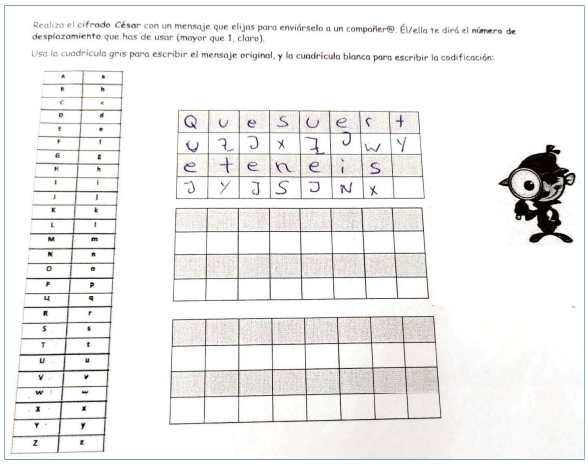


Figura 5. Codificación mediante el cifrado César de un mensaje de uno de los alumnos/as

el ya conocido *Concurso matemático Carlos Pina* de Fuentes de Ebro). Desde aquí deseo aprovechar para dar las gracias a ambos centros por el maravilloso trato que en ambos me ofrecieron y también a su alumnado, por lo bien que se comportaron.

Una última observación. Al igual de lo que ya comenté en la parte I de este artículo, creo que las clases divulgativas hay que realizarlas un día que estén en clase todos los alumnos/as si es posible. Si no lo es, entonces las preguntas opcionales de las pruebas escritas no pueden proponerse ya que los alumnos/as que no estaban presentes ese día, estarían obviamente en desventaja.

Me gustaría indicar que la lista de recursos bibliográficos, que sigue a continuación, contiene algunos de los materiales que he utilizado para preparar estas sesiones. Entre ellos destacaría un recurso de Geogebra que permite comenzar a realizar de forma interactiva la criba de Eratóstenes, y una sección de la web CREA de la Consejería de Educación de la Junta de Extremadura en la que explica de forma resumida cómo es el funcionamiento del algoritmo de encriptación RSA y además proporciona un *applet* de generación de claves públicas y privadas muy entretenido de utilizar. Esto último, por ser de mayor complejidad que lo que yo les quería explicar a los alumnos/as, no lo usé en estas sesiones, pero lo utilicé para documentarme y lo anoté como referencia para alguna clase posterior. Como me parece muy interesante, lo pongo aquí también.

Referencias bibliográficas

Álvarez, J. L., «Criba de Eratóstenes», *Proyecto Gauss, Materiales didácticos* <http://geogebra.es/gauss/materiales_didacticos/primaria/actividades/aritmetica/naturales_y_enteros/criba_de_eratostenes/actividad.html>, recuperado el 24 de mayo de 2022.

«Cifrado César», *Wikipedia*, <https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar>, recuperado el 24 de mayo de 2022.

Colera, J., I. Gaztelu y R. Colera (2016), *Matemáticas 1.º ESO*, Ed. Anaya.