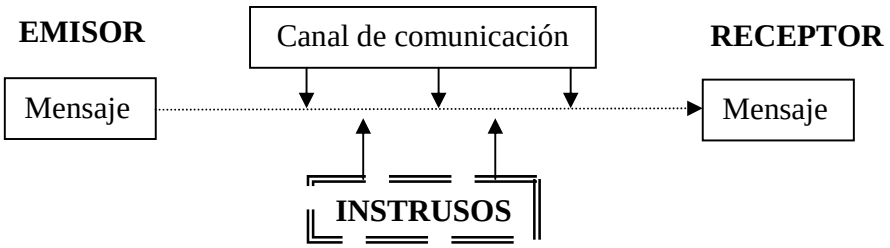
Aritmética modular y códigos secretos

Juana Contreras S.[1]
Claudio del Pino O.[2]
Instituto de Matemática y Física
Universidad de Talca

Desde que el hombre empezó a comunicarse, surgió la necesidad de proteger dichas comunicaciones. La idea es asegurarse, que el mensaje que envía una persona A (emisor) a una persona B (receptor), no pueda ser entendido ni alterado por otras personas. Tradicionalmente, las áreas en las cuales se ha necesitado (y hoy día, aún más) resguardar la información, han sido las relacionadas con las comunicaciones diplomáticas, militares[3] y financieras.

Los principales problemas asociados al envío de mensajes son:

- El emisor no tiene la seguridad, que sea solamente el receptor, quien esta recibiendo el mensaje.
- Que el mensaje recibido por el receptor, no haya sufrido alteraciones.
- Que el receptor tenga la seguridad, que el mensaje recibido provenga del emisor apropiado.



Una manera de tratar de asegurar la información, es tomar el mensaje que se desea enviar y mediante una *regla* apropiada esconderlo (mensaje cifrado), luego enviar el mensaje cifrado al receptor, y éste último aplicando una *regla inversa* a la usada por el emisor, recupera el mensaje original. Como es de suponer, esto presupone un acuerdo entre el emisor y el receptor, con respecto a las reglas que se usarán.

[1] e-mail: jcontres@pehuenche.utalca.cl
[2] e-mail: cdelpino@pehuenche.utalca.cl
[3] En Anexo se entrega una interesante historia relacionada con mensajes secretos en la primera guerra mundial.

El estudio de métodos para esconder (cifrar) mensajes, se conoce con el nombre de criptografía (del griego kryptos = oculto, y grafía = escritura). En cambio, el área de estudio que se preocupa de descifrar mensajes (obviamente, sin conocer el método del cifrado), criptoanálisis.

En este artículo, se revisarán algunos métodos para cifrar mensajes que están basados en la aritmética modular de los números enteros.

Método de Julio César.

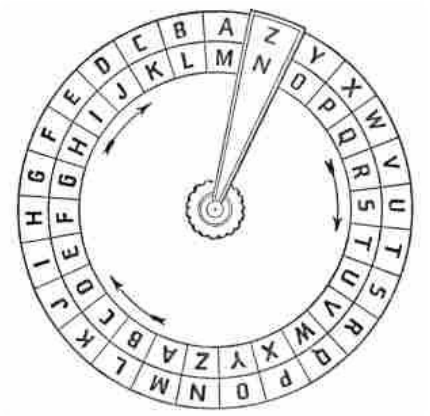
Julio César (12 dC-41dC)
Emperador Romano

Uno de los primeros métodos conocidos para esconder mensajes, es el que usaba Julio César, el cual consistía en sustituir cada letra por la letra que estaba tres lugares más a la derecha en el abecedario (volviendo a partir desde la primera letra después de la última). Vamos a ejemplificarlo, usando nuestro alfabeto. Para ello, cifraremos el mensaje: “Vamos bien”.

Para empezar, realicemos una tabla que muestre la correspondencia entre cada letra y la que le corresponde, de acuerdo al método comentado:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Por inspección de la correspondencia anterior, vemos que la V corresponde a la Y, la A corresponde a la D, etc. Luego el mensaje original, “Vamos bien”, quedaría cifrado por “Ydorv elhp”. Como es de suponer, la persona que recibe este mensaje, para entenderlo debe descifrarlo. Para ello basta que, tomando una tabla como la precedente, recupere las letras correctas realizando el proceso inverso. Como se puede observar este método, esconde razonablemente bien el mensaje original.



Rueda especial para cifrar y descifrar mensajes con reglas “tipo Julio César”

Para hacer más *operativo* el método de Julio César, le vamos a incorporar un poco de matemática. Con este fin realicemos los siguiente pasos:

Paso 1: Asignemos a la letra A el número 0, a la letra B el número 1, etc. Es decir:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	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

Paso 2: Sustituyamos cada letra de nuestro mensaje, por el número asignado:

v	**a**	**m**	**o**	**s**	**b**	**i**	**e**	**n**
22	**0**	**12**	**15**	**19**	**1**	**8**	**4**	**13**

Por lo tanto el mensaje original, numéricamente, se vería así:

22 0 12 15 19 1 8 4 13

Paso 3: Ahora, a nuestro mensaje numérico, apliquemos la regla de Julio César: **Sumar 3**:

22	**0**	**12**	**15**	**19**	**1**	**8**	**4**	**13**
+3	+3	+3	+3	+3	+3	+3	+3	+3
25	**3**	**15**	**18**	**22**	**4**	**11**	**7**	**16**

Paso 4: En nuestro mensaje numérico cifrado, sustituyamos los números por las letras correspondientes:

25	**3**	**15**	**18**	**22**	**4**	**11**	**7**	**16**
y	**d**	**o**	**r**	**v**	**e**	**l**	**h**	**p**

Paso 5: Finalmente, el mensaje que se enviaría, sería:

Ydorv elhp

Que obviamente no varía del encontrado anteriormente.

Como es de suponer, el receptor para *recuperar* el mensaje, deberá conocer la clave en cuestión, y aplicar la regla inversa, es decir, asignar a cada letra el número que le corresponde, luego a cada número *restarle 3*, y finalmente sustituir cada número por su letra correspondiente[4].

[4] En el método de Julio César, ¿qué otros números, en lugar del 3, se pueden usar para obtener cifrados distintos?

Al revisar con más cuidado el método descrito, nos damos cuenta que surgen algunos aspectos especiales, por ejemplo,

$$24 + 3 = 27 = 0$$
$$25 + 3 = 28 = 1$$
$$26 + 3 = 29 = 2$$

lo que está indicando que la *suma* que se usó en el método de Julio César, no es la suma usual de números enteros. En efecto, la suma usada en este método es la *suma módulo 27*. A continuación se aclara matemáticamente este punto.

Definición: Se dice que un entero a es congruente (igual) a b módulo m, lo que se escribe $a \equiv b (\text{mod } m)$, siempre y cuando, $a - b = k \cdot m$, para algún entero k.

Por ejemplo, si trabajamos con $m=27$, es decir en módulo 27, se tiene que: $27 \equiv 0 (\text{mód } 27)$, $28 \equiv 1 (\text{mód } 27)$ y $29 \equiv 2 (\text{mód } 27)$. Además, se puede observar que todo número entero es congruente a uno y sólo uno de los números del conjunto

$$M_{27} = \{0, 1, 2, ..., 26\}$$

En efecto, dado un entero positivo cualquiera s, al dividir s por 27, se obtiene un cierto cuociente c y un resto r (con $0 \leq r < 27$). De donde,

$$s = 27 \cdot c + r$$

o sea,

$$s - r = 27 \cdot c$$

es decir, s es congruente a r módulo 27, de donde r pertenece a M_{27}.

Actividad 1: ¿Cómo se encontraría el entero congruente módulo 27 de un número entero negativo?

Observación: La relación de congruencia en los enteros, tiene las mismas propiedades de la igualdad usual, en efecto:

Propiedad 1: En los números enteros, la relación de congruencia módulo m, tiene las siguientes propiedades:

1. **Refleja**: $a \equiv a (\text{mód } m)$
2. **Simétrica**: Si $a \equiv b (\text{mód } m)$, entonces $b \equiv a (\text{mód } m)$
3. **Transitiva**: Si $a \equiv b (\text{mód } m)$ y $b \equiv c (\text{mód } m)$, entonces $a \equiv c (\text{mód } m)$
4. Si $a \equiv b (\text{mód } m)$ y $c \equiv d (\text{mód } m)$, entonces $a+c \equiv b+d (\text{mód } m)$

Demostración. A modo de ejemplo, probaremos la propiedad 3. Las restantes son análogas.

Si $a \equiv b(\text{mód } m)$, entonces existe un número entero r tal que

$$a-b=r \cdot m \qquad (1)$$

Si $b \equiv c(\text{mód } m)$, entonces existe un entero s, tal que:

$$b-c=s \cdot m \qquad (2)$$

Sumando las relaciones (1) y (2) anteriores, se obtiene:

$$a-c=(r+s) \cdot m$$

de donde, se obtiene que:

$$a \equiv c(\text{mód } m)$$

que es lo que se quería demostrar.

Propiedad 2: La suma módulo 27, que denotaremos $\oplus_{27}$ (o simplemente $\oplus$, cuando no haya confusión), en el conjunto M_{27}, tiene las mismas propiedades algebraicas de la suma usual en los números enteros, es decir, si a, b y c pertenecen a M_{27}, entonces se cumple:

1. Clausura: $a \oplus b \in M_{27}$
2. Asociatividad: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. Elemento neutro: El 0, y tal que, para cada a en M_{27}: $a \oplus 0 = a$
4. Elemento neutro: Para cada x en M_{27}, existe un x' en M_{27} tal que: $x \oplus x' = 0$
5. Conmutatividad: $a \oplus b = b \oplus a$

Demostración. Propuesta.

Volvamos al método de Julio César, que tenía la clave "sumar 3". Es claro que, en lugar de esta clave se puede usar la clave "sumar n" para cada n, no nulo, de M_{27}. Como una manera de variar el método de Julio César, se puede intentar cambiar en la clave, "sumar" por "multiplicar". Exploremos esta variante. Elijamos, por ejemplo, la clave "multiplicar por 9", como es de suponer esta multiplicación se hace módulo 27. Veamos cómo se reasignarían, con esta clave, las letras del alfabeto.

Letra	A	B	C	D	E	F	G	H	I	J	...
Código numérico	0	1	2	3	4	5	6	7	8	9	...
Multiplicar por 9 (mód 27)	0	9	18	0	9	18	0	9	18	0	...
Letra cifrada	A	J	R	A	J	R	A	J	R	A	...

Por lo tanto, es claro que la clave de multiplicar por 9 (módulo 27) no sirve. Se tienen dos posibilidades:

- No se puede usar la multiplicación, o bien
- Se puede usar la multiplicación, pero el número 9 elegido, es el que no se comporta bien.

Veamos que sucede si elegimos otro número, digamos por ejemplo, el 5. En este caso las letras, manteniendo el esquema precedente, quedarían reasignadas de la siguiente manera:

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
Código numérico	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Multiplicar por 5 (mód 27)	0	5	10	15	20	25	3	8	13	18	23	1	6	11	16
Letra cifrada	A	F	K	O	T	Y	D	I	N	R	W	B	G	L	P

Letra	O	P	Q	R	S	T	U	V	W	X	Y	Z
Código numérico	15	16	17	18	19	20	21	22	23	24	25	26
Multiplicar por 5 (mód 27)	21	26	4	9	14	19	24	2	7	12	17	22
Letra cifrada	U	Z	E	J	Ñ	S	X	C	H	M	Q	V

Por lo tanto, usando la multiplicación por 5 (módulo 27), se obtiene una clave adecuada de cifrado, pues se ha obtenido una transposición de nuestras 27 letras.

Actividad 2: Cifrar, usando la clave de multiplicar por 5 (módulo 27), el siguiente pensamiento del matemático Henri Poincaré (Francés, 1854-1912):

Todo saber tiene de ciencia lo que tiene de matemática

Actividad 3: Al descifrar el siguiente mensaje, que ha sido cifrado con la clave de multiplicar por 5 (módulo 27), encontrará un pensamiento:

Bañ gastgasnkañ ñul ba gxñnka ot ba javul

Con el fin de intentar descubrir, porqué el sistema funciona con el 5 y no con el 9, se pueden analizar otros números. Al hacerlo se descubre que el método funciona bien con todos los números entre 1 y 26, excepto con el 3 y el 9. Al parecer la respuesta sería que, el sistema funciona bien con aquellos números que no tienen factores comunes con el 27, es decir, aquellos números que son primos relativos con el 27. En efecto, este resultado es un caso particular de la siguiente propiedad.

Propiedad 3: Sean a y n enteros, con $a<n$. Si a y n son primos relativos, entonces los siguientes números, módulo n, son todos distintos:

$$a,\ \ 2\cdot a,\ \ 3\cdot a,\ \ 4\cdot a,\ \ ...,\ \ (n\text{-}1)\cdot a$$

Demostración: Sean x e y dos números con $0 \leq x < y < n$. Se quiere probar ax no es congruente con ay, módulo n. Haremos una demostración indirecta. Para ello, supongamos que

$$ay \equiv ax \ (\text{mód } n)$$

Luego, existe un entero k, tal que:

$$ay - ax = kn$$

Es decir,

$$a(y-x) = kn$$

Luego, n divide a $a(y-x)$ y como a y n no tienen factores comunes, n divide a $y-x$, Esto es imposible pues $0<y-x<n$. Esta contradicción establece que la propiedad se cumple.

Ahora bien, supongamos que se ha cifrado un mensaje usando, por ejemplo, la clave de multiplicar por 5 (módulo 27) y se dispone del correspondiente código numérico, ¿cuál sería la clave inversa?, es decir, por cuánto habría que multiplicar cada número del mensaje cifrado, para recuperar la versión numérica del mensaje original?. Para obtener la respuesta, se puede observar la tabla precedente. Al hacerlo se descubre que le número buscado es el 11, pues en módulo 27, $5 \cdot 11 = 1$, es decir, en módulo 27 el número 11 es el inverso multiplicativo del número 5. Como ya se ha dicho, la clave de multiplicar por n módulo 27, funciona bien cuando n es primo relativo con 27, entonces surge la siguiente interrogante, ¿si n es primo relativo con 27, n tendrá siempre un inverso multiplicativo en M_{27}?. La respuesta es afirmativa, tal como estable la siguiente:

Propiedad 4: Si m es un entero positivo, entonces el conjunto

$$G(m) = \{n / n < m \text{ y } n \text{ es primo relativo con } m\},$$

conforma un grupo bajo la multiplicación módulo m.

Demostración: Se debe comprobar que en $G(m)$ la multiplicación módulo m cumple las propiedades de clausura, asociatividad, elemento neutro y elemento inverso. Se probará, a modo de ejemplo, la primera y la última.

Clausura: Sean a y b en $G(m)$, entonces $a<m$, $b<m$ y $(a,m)=(b,m)=1$. Sea $ab=k$ $(\text{mód } m)$ con $k<m$. Es claro que ab es primo relativo con m. Probaremos que k es primo relativo con m. En efecto, de $ab=k(\text{mód } m)$, se tiene que $ab-k=sm$. Pues bien, si existe un primo p que divide a k y m, luego como $ab=k+sm$, se tendría que p dividiría a ab. Situación que es imposible, por ser ab primo relativo con m.

Elemento inverso: Sea a en $G(m)$. Como a y m son primos relativos, existen enteros s y t tales que $as+mt=1$ (*), de donde $as \equiv 1 \ (mód\ m)$. Ahora, por el algoritmo de Euclides, existen enteros q y s', con $0 \leq s' < m$, tales que $s=mq+s'$. Por (*) s es primo relativo con m, luego 0<s'. Además como $(s',m)=1$, se tiene que s' pertenece a $G(m)$. Por lo tanto, s' es el inverso de a.

Ahora bien, ya se ha establecido que para cifrar la versión numérica de un mensaje se pueden usar las claves de sumar (módulo 27) cualquier número entero positivo, o bien multiplicar (módulo 27) por cualquier elemento de $G(27)$. Del primer caso se tienen 26 claves diferentes, del segundo, 17 claves distintas. A continuación se comentan algunas opciones que se pueden usar para generar otras claves de encriptación, a partir de las claves comentadas.

- En la clave de sumar un número (módulo 27), se puede ir variando el número clave de mensaje en mensaje. Por ejemplo, se puede usar como número clave el número correspondiente al día del mes (módulo 27) en que se envía el mensaje. ¿Se le ocurren otras variantes?.
- Una variante similar se podría usar con la clave de multiplicar.
- Otra posibilidad sería que, en sucesivos mensajes alternar ambos métodos.
- Una alternativa diferente sería tomar la versión numérica del mensaje, y aplicar a los números que ocupan una posición impar una clave con suma y en los otros aplicar la clave del producto.

Actividad 4: Encontrar otras variantes para ocultar mensajes usando las claves de sumar y/o multiplicar.

Una idea interesante es tratar de combinar ambos métodos, por ejemplo, elegir un número entero positivo a, y un número b de $G(27)$, y usar como clave de encriptación el cambiar cada número N de la versión numérica del mensaje por $b \cdot N+a$, es decir, aplicar la transformación:

$$N \rightarrow b \cdot N+a$$

La pregunta que surge naturalmente en la opción precedente es, si ella se comporta bien; es decir, si al aplicarla al abecedario se obtiene o no una permutación del abecedario. Como es de suponer, el problema estaría en el caso que existan dos letras diferentes, que con esta clave, se cifren por una misma letra. El siguiente resultado da la respuesta.

Propiedad 5: Sean a y n enteros positivos, y b un entero positivo tal que $(b,n)=1$. Los siguientes números

$$b+a,\ 2 \cdot b+a,\ 3 \cdot b+a,\ ...,\ (n-1) \cdot b+a$$

son, módulo n, todos distintos.

Actividad 5:

a) ¿Cuántas claves distintas se obtienen con el método de encriptación precedente?
b) Encriptar, usando la regla $N \rightarrow 11 \cdot N + 7$, el siguiente pensamiento de Pablo Picasso (Pintor Francés, 1881-1973):

"La inspiración existe, pero tiene que encontrarte trabajando"

c) Una vez encriptado el pensamiento anterior, determinar la clave que hay que usar para descifrarlo.
d) Descifrar el siguiente mensaje sabiendo que ha sido *escondido* usando la clave $4n+5$:

NEZE DE AFJRFD SIU UWF RZOLARJVU VE GRNRUWLD

Anexo[5]

La siguiente historia ocurrió durante la primera guerra mundial.

En el año 1914, un profesor de la Universidad de Cambridge, Sir Alfred Ewing, fue destinado a colaborar con el almirantazgo británico en la educación de la escuela naval, momento que coincidió con el inicio de la guerra. En estas circunstancias, un oficial de inteligencia le mostró un cierto número de telegramas que habían sido interceptados en las comunicaciones radiales entre barcos alemanes. Como es de suponer estaban cifrados, y se le asignó la tarea de intentar descifrarlos. Se establecieron puestos de escucha y así pronto se contaba con 2000 mensajes por día.

Una simple inspección de estos comunicados permitió clasificarlos 4 o 5 clases distintas. Un primer tipo era claramente de códigos de transposición, donde las letras de un mensaje se habían rearreglado para formar grupos ininteligibles. Estos presumiblemente eran mensajes militares, pues un código de transposición era factible de usar en terreno, mientras que usar un libro de códigos es altamente riesgoso. Un libro de códigos es una especie de diccionario en el cual hay una lista de palabras y frases, tendiendo al frente de cada una un grupo arbitrario de letras o signos. La persona que envía el mensaje debe tener el libro para seleccionar las letras o signos; la persona que recibe el mensaje debe también tener el libro para interpretarlo. Además se obtiene un mejor resultado si se usa una "clave" o "llave" adicional, que significa usar un sistema pre-asignado de alterar las letras o signos. Se pueden usar varias claves distintas en un mismo libro, de modo que los mensajes destinados a una persona no puedan ser leídos por otros agentes. Los alemanes usaban un solo Libro Naval de Señales, tanto para los comunicaciones ordinarias entre barcos como para las órdenes confidenciales a los almirantes, con claves diferentes en cada caso.

[5] Extraído del texto [3].

Este era pues el problema tal como se presentaba a Sir Ewing, quien formó un grupo de personas que trabajaban con él, todos los cuales sabían alemán y eran muy discretos. Visitaron las oficinas de correos, de seguros y el museo británico para familiarizarse con las colecciones de Libros de Códigos, y pudieron formarse una idea de la manera como se construían estos libros. Al mismo tiempo se desarrolló un sistema para interferir, en distintas frecuencias, todas las comunicaciones de los alemanes.

Apenas a fines de agosto de 1914, cuando ni siquiera se cumplía un mes del conflicto, un crucero ligero alemán, el Magdeburgo, encalló en una isla de Finlandia y fue destruido por los barcos rusos. Los rusos encontraron el cuerpo de un oficial ahogado que aún abrazaba su libro confidencial de señales.

Este libro fue entregado a las autoridades navales británicas, los cuales lo hicieron llegar a Sir Ewing. Este texto consistía en grupos de 3 letras y usaban 31 letras, las 26 usuales más 5 agregadas. El proceso de codificación consistía en reemplazar cada letra por otra de acuerdo a una plan preestablecido. Asociado a este libro de señales había un mapa en el cual el mar del norte se había parcelado en cientos de pequeños cuadraditos, que permitían señalar una posición rápida y secretamente (se indicaba simplemente el número del cuadrado, en lugar de la latitud y longitud).

El éxito inglés consistió en descubrir las claves que se usaban en cada caso, y así en noviembre de 1914, podían traducir rápidamente todas las órdenes navales secretas que interceptaban.

Como se sabe, los alemanes protegían su flota de guerra en los estuarios del Heligolandia, detrás de un campo de minas defensivo, y desde allí enviaban sus barcos, de tiempo en tiempo, para efectuar raids sobre Inglaterra o atacar convoyes de carga. Pero gracias al departamento de criptografía inglés, cada vez que los alemanes hacían una salida los barcos ingleses estaban esperándolos. Esto tuvo una importancia crucial en la estrategia naval, pues permitió a los barcos ingleses descansar en los puertos hasta que una señal de alarma les fuera entregada, puesto que no había necesidad de patrullar incesantemente el mar, el ahorro de combustible y descanso de las tripulaciones fue crucial a la hora de evitar minas y los ataques de los torpedos. Es fácil imaginarse la confianza que desarrollaron los ingleses, cuando sabían positivamente que se iban a encontrar con barcos enemigos, en vez de encontrarse con ellos por sorpresa.

De todos los mensajes interceptados y traducidos, quizás el más importante fue enviado por un submarino alemán que decía “hemos hundido en la costa sur de Irlanda un barco, un

velero, dos vapores y el transatlántico Lusitania". Una copia de este mensaje fue enviado a Estados Unidos, y provocó que éste entrara en la segunda mundial, llevando finalmente a la derrota de los alemanes.

Bibliografía

[1] Bilgot, Jean- Francois, *Arithmétique en terminale S*, CRDP d'Aubergne, 1998.

[2] Riera L., Gonzalo. *Códigos secretos*, Coloquios del Instituto de Matemática y Física, Universidad de Talca, 1990.

[3] Riera L., Gonzalo. *Matemática Aplicada*, Tercero Medio. Editorial Zig-Zag, 1999.

[4] Vinogradov, I.., *Fundamentos de la teoría de números*, Editorial Mir, Moscú, 1977.

[5] http://leo.worldonline.es/jlquijad/
Interesante sitio de Internet, contiene antecedentes históricos, métodos clásicos de encriptación y juegos relacionados.