

Como $c > 1$, esto ofrece un factor propio de $2^m + 1$, que no es entonces primo.

V. Enviando mensajes secretos

LA CRIPTOGRAFÍA es la ciencia de las comunicaciones secretas. El problema es trasmisir a un destinatario de manera segura un mensaje de forma que sólo él pueda entender el contenido, a pesar de que todo mundo pueda leerlo. Cuando transformamos un mensaje de manera que sólo puede ser entendido por el destinatario, decimos que el mensaje ha sido *codificado* y que el destinatario conoce la *clave de decodificación*.

Todos hemos jugado cuando niños a enviar "mensajes secretos" escribiendo unas letras por otras, de forma que sólo el destinatario sepa cuál es el cambio de letras que utilizamos. Éste es el mismo método que utilizaban los emperadores romanos. Por ejemplo, Julio César usaba un desplazamiento cíclico de las letras del alfabeto de forma que la *A* se escribía como *D*, la tabla completa de las transformaciones sería:

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

Esta transformación de las letras del alfabeto se llama una *trasposición*. Si decidimos que los espacios en blanco se escriben como *A*, entonces la segunda frase de este capítulo en el código de Julio César se escribiría de la manera siguiente:

HOASUREOHPDAHVAWUDVPLWLUA
DAXQAGHVWLQDW
ULRAGHAPDQHUDAVHJXUDAXQAPHQVDMHAGHAIRUPD
ATXHAVRORAH
OA
SXHGDAHQWHQGHUA
HOAFRQWHQLGR
ADASHVDUAGHATXHAWRGRA
PQGRASXHGDAOHHUOR

¿Qué tan fácil sería para un ejército enemigo descifrar este mensaje? No sabemos qué tan hábiles fueron los enemigos de Julio César, pero este tipo de códigos secretos son fáciles de des- cifrar.

En efecto, en un idioma la frecuencia con que las diferentes letras aparecen no es la misma. Por ejemplo, la letra *E* es la que más frecuentemente se utiliza y, como bien sabemos, no hay muchos ejemplos de palabras que usen *W*. Pues bien, en el código de Julio César la frecuencia con la que aparece una letra en el mensaje original y la letra correspondiente en el mensaje codificado es la misma. Así, la letra *A* aparece 11 veces en el mensaje original y por lo tanto la *D* aparece 11 veces en el mensaje codificado. Esto nos da la clave para descifrar el código de una transposición: si tomamos un texto suficientemente largo y contamos cuántas veces aparece cada letra tendremos una idea aproximada de la frecuencia con la que esa letra se usa en el lenguaje, luego contamos las frecuencias de cada letra en el mensaje cifrado; frecuencias parecidas indican que probablemente se trate de una letra y su correspondiente codificación.

Tratemos de decodificar el mensaje de Julio César. Para ello usamos el texto de este capítulo (desde el inicio hasta este párrafo) para calcular la frecuencia con que se usan las letras en español. Obtenemos así la siguiente tabla:

<i>Letra</i>	<i>Número de ocurrencias</i>	<i>Frecuencia</i>	<i>Letra</i>	<i>Número de ocurrencias</i>	<i>Frecuencia</i>
<i>espacio</i>	395	.172	<i>U</i>	80	.034
<i>E</i>	316	.137	<i>M</i>	71	.030
<i>A</i>	247	.107	<i>P</i>	39	.017
<i>S</i>	170	.074	<i>F</i>	34	.015
<i>O</i>	162	.070	<i>B</i>	23	.010
<i>I</i>	131	.057	<i>Q</i>	19	.008
<i>N</i>	126	.054	<i>J</i>	18	.008
<i>L</i>	117	.050	<i>G</i>	18	.008
<i>R</i>	112	.048	<i>Y</i>	7	.003
<i>C</i>	105	.045	<i>V</i>	6	.003
<i>T</i>	91	.039	<i>H</i>	6	.003
<i>D</i>	90	.039	<i>Z</i>	4	.002

Contamos enseguida el número de veces que aparece cada letra en el mensaje cifrado. Obtenemos la siguiente tabla:

Letra	Número de ocurrencias	Letra	Número de ocurrencias
A	28	G	10
H	24	X	9
Q, R	12	U	7
D	11	V, P	6

Las demás letras aparecen cuando mucho en 3 ocasiones. Vemos entonces que el signo más usado en el mensaje codificado es *A* y es lógico esperar que esta letra debe representar el espacio entre palabras que es el signo más utilizado en el lenguaje escrito ordinario. La segunda letra más usada es la *H* y podemos concluir que probablemente se trate de la letra *E*. Hasta aquí las cosas van perfectamente. Las cosas comienzan a complicarse después, pues la tercera letra más usada en el mensaje codificado es la *Q* que no corresponde a la letra *A*, que es la tercera más usada en el lenguaje ordinario. Sin embargo, las letras más usadas en el mensaje: *Q, D, R, G* corresponden a las letras *N, A, O, D*, que están entre las letras más usadas ordinariamente. Después de ensayar entre varias sustituciones diferentes es fácil atinar con la sustitución correcta que nos permite llegar al siguiente mensaje:

eO SUoEOePa eV WUaVPLWLU a Xn de VWLnaWaULo de PaneUa
 VeJXUa Xn PenVaMe de IoUPa TXe VoOo eO SXeda en WendeU eO
 FonWenLdo a SeVaU de TXe Wodo PXndo SXeda OeeUOo

Hemos escrito con minúsculas las letras decodificadas y dejado en mayúsculas las que todavía no hemos tratado de descifrar. Un vistazo a las palabras cortas de este texto nos obliga a pensar que probablemente la *X* codifique a la *u*, la *O* a la *l*, la *V* a la *s*, la *T* a la *q*. Hechas esas sustituciones el mensaje puede terminarse de descifrar fácilmente.

Los problemas que encontramos en el desciframiento del mensaje anterior se deben a su longitud. El método que acabamos de ver para descifrar un mensaje sólo es útil si sabemos que el mensaje ha sido cifrado por medio de una transposición de letras y si el mensaje es relativamente largo. Un mensaje relativamente corto puede tener características especiales de forma que la frecuencia de las letras que utiliza no sean parecidas a

las del lenguaje ordinario. Por ejemplo, en un mensaje corto como: ATACA AHORA, la letra que más aparece es la *A*, mientras que no hay una sola *E*. Un mensaje así será prácticamente imposible de descifrar si no se conoce la clave de cifrado.

Al paso de los años quedó claro que la codificación de mensajes (largos) en la forma que lo hacían los romanos era fácil de ser descifrada por las personas que no deberían conocer el mensaje. Por ello se comenzaron a usar claves de codificación más y más complejas. Pero la mayor parte de los esfuerzos fueron inútiles pues la historia está llena de ejemplos de éxitos de analistas que logran violar los códigos del enemigo.

Durante la primera Guerra Mundial los británicos interceptaron un mensaje cifrado del ministro de Relaciones Exteriores de Alemania, Arthur Zimmermann, dirigido al embajador en México, Heinrich von Eckardt. Después de muchos esfuerzos los analistas británicos lograron romper el código del mensaje y descubrir un plan alemán de alentar al gobierno de México para que entrara a la guerra como aliado de Alemania asegurándole que, al triunfo, recuperaría los territorios perdidos en la guerra de 1847. El aviso que se envió al presidente de Estados Unidos, Woodrow Wilson, decidió a éste a entrar inmediatamente en la guerra del lado de los aliados, lo que probablemente permitió un fin más rápido del conflicto armado.

CODIFICANDO CON MATRICES

Una *matriz* de tamaño 2×2 es un arreglo de números:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

como las matrices A_0 y B_0 siguientes:

$$A_0 = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \quad B_0 = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}.$$

Hay muchas cosas que se pueden hacer con las matrices. Por ejemplo, se pueden sumar como sigue:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

De esta forma la matriz $A_0 + B_0$ resulta:

$$\begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix}.$$

Una matriz también se puede multiplicar por una columna $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ de forma que el resultado es otra columna. Esta multiplicación está dada por la siguiente regla:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a_{11}v_1 + a_{12}v_2 \\ a_{21}v_1 + a_{22}v_2 \end{pmatrix}.$$

Por ejemplo, si multiplicamos nuestra matriz A_0 por la columna $v = \begin{pmatrix} 2 \\ 11 \end{pmatrix}$, resulta la columna $A_0 \cdot v = \begin{pmatrix} 37 \\ 61 \end{pmatrix}$.

Finalmente, observemos que también podemos multiplicar matrices si pensamos que una está formada por dos columnas. En efecto, si tenemos dadas dos matrices A y B de tamaño 2×2 y b_1 y b_2 son las dos columnas que forman la matriz B , entonces definimos la matriz $A \cdot B$ como la matriz cuyas columnas son $A \cdot b_1$ y $A \cdot b_2$. Podemos así calcular los productos:

$$A_0 \cdot A_0 = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix}$$

$$A_0 \cdot B_0 = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Vamos a ver cómo podemos usar estas operaciones de matrices para obtener una clave de cifrado más difícil de descifrar que la de Julio César.

Comencemos con asignar a cada letra del alfabeto un número. Por ejemplo, podemos elegir la siguiente sencilla asignación:

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

Supongamos que queremos codificar el mensaje: "El problema es comunicar de manera segura un mensaje".

Comenzamos partiendo este mensaje en pares de letras: "El pr ob le ma es co mu ni ca rd em an er as eg ur au nm en sa je", y formamos con estos pares columnas de números según la tabla de cifrado:

$$\begin{pmatrix} 5 \\ 12 \end{pmatrix} \begin{pmatrix} 16 \\ 18 \end{pmatrix} \begin{pmatrix} 15 \\ 2 \end{pmatrix} \begin{pmatrix} 12 \\ 5 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \end{pmatrix} \begin{pmatrix} 13 \\ 21 \end{pmatrix} \\
\begin{pmatrix} 14 \\ 9 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \begin{pmatrix} 18 \\ 4 \end{pmatrix} \begin{pmatrix} 5 \\ 13 \end{pmatrix} \begin{pmatrix} 1 \\ 14 \end{pmatrix} \begin{pmatrix} 5 \\ 18 \end{pmatrix} \begin{pmatrix} 1 \\ 19 \end{pmatrix} \\
\begin{pmatrix} 5 \\ 7 \end{pmatrix} \begin{pmatrix} 21 \\ 18 \end{pmatrix} \begin{pmatrix} 1 \\ 21 \end{pmatrix} \begin{pmatrix} 14 \\ 13 \end{pmatrix} \begin{pmatrix} 5 \\ 14 \end{pmatrix} \begin{pmatrix} 19 \\ 1 \end{pmatrix} \begin{pmatrix} 10 \\ 5 \end{pmatrix}.$$

Escogemos una matriz A de tamaño 2×2 que sea *invertible*, esto es, que exista otra matriz B de forma que $A \cdot B$ sea la *matriz identidad*:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por ejemplo, nuestra matriz A_0 definida antes es invertible. Para continuar, multiplicamos cada una de las columnas obtenidas por la matriz invertible A_0 , para obtener un sistema de 22 nuevas columnas como siguen:

$$\begin{pmatrix} 46 \\ 75 \end{pmatrix} \begin{pmatrix} 86 \\ 138 \end{pmatrix} \begin{pmatrix} 36 \\ 55 \end{pmatrix} \begin{pmatrix} 39 \\ 61 \end{pmatrix} \begin{pmatrix} 29 \\ 44 \end{pmatrix} \begin{pmatrix} 67 \\ 110 \end{pmatrix} \begin{pmatrix} 51 \\ 84 \end{pmatrix} \begin{pmatrix} 89 \\ 144 \end{pmatrix} \\
\begin{pmatrix} 55 \\ 87 \end{pmatrix} \begin{pmatrix} 60 \\ 97 \end{pmatrix} \begin{pmatrix} 48 \\ 74 \end{pmatrix} \begin{pmatrix} 49 \\ 80 \end{pmatrix} \begin{pmatrix} 44 \\ 73 \end{pmatrix} \begin{pmatrix} 64 \\ 105 \end{pmatrix} \begin{pmatrix} 59 \\ 98 \end{pmatrix} \\
\begin{pmatrix} 31 \\ 50 \end{pmatrix} \begin{pmatrix} 96 \\ 153 \end{pmatrix} \begin{pmatrix} 65 \\ 168 \end{pmatrix} \begin{pmatrix} 67 \\ 107 \end{pmatrix} \begin{pmatrix} 52 \\ 85 \end{pmatrix} \begin{pmatrix} 41 \\ 62 \end{pmatrix} \begin{pmatrix} 35 \\ 55 \end{pmatrix}.$$

Por último reescribimos estas columnas en un arreglo de números consecutivos para borrar toda huella de lo que hemos hecho. El mensaje cifrado que enviaremos es el siguiente:

46 75 86 138 36 55 39 61 29 44 67 110 51 84 89 144 55 87 60 97 48 74
49 80 44 73 64 105 59 98 31 50 96 153 65 168 67 107 52 85 41 62 35 55

La persona que recibe el mensaje y debe descifrarlo procede de la siguiente manera sencilla. Debe conocer la matriz B_0 que tiene la propiedad de que $A_0 \cdot B_0$ es la matriz identidad I , luego divide los números del mensaje en parejas y forma las columnas correspondientes. Luego multiplica las columnas por la matriz B_0 y obtiene columnas que le permiten leer el mensaje. En

nuestro ejemplo, comenzaríamos a descifrar así:

$$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} \begin{pmatrix} 46 \\ 75 \end{pmatrix} = \begin{pmatrix} 5 \\ 12 \end{pmatrix} = \begin{pmatrix} E \\ L \end{pmatrix},$$

$$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} \begin{pmatrix} 86 \\ 138 \end{pmatrix} = \begin{pmatrix} 16 \\ 18 \end{pmatrix} = \begin{pmatrix} P \\ R \end{pmatrix}.$$

Un mensaje cifrado de esta manera es muy difícil de descifrar si no se conoce la matriz A_0 o la matriz B_0 . Pero no es imposible, de hecho el mensaje dirigido al embajador de Alemania en México y descifrado por los servicios de inteligencia británicos durante la primera Guerra Mundial, estaba cifrado por medio de una matriz de tamaño 6×6 en la forma en que hemos trabajado antes.

Finalmente nos preguntamos, ¿de cuántas formas podemos elegir nuestra matriz invertible A_0 ? Contestamos esta pregunta por medio de un sencillo teorema.

Teorema. Una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tiene una inversa con entradas enteras si y solamente si $ad - bc$ vale 1 o -1.

El número $ad - bc$ se llama el *determinante* de A y se denota como $\det A$.

Demostración. Tomemos dos matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Sabemos que el producto de las matrices es:

$$A \cdot B = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

que tiene determinante:

$$\begin{aligned} \det A \cdot B &= (aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') \\ &= (ad - bc)(a'd' - b'c') = \det A \det B. \end{aligned}$$

Ahora estamos listos para la demostración. Si suponemos que B es una matriz con entradas enteras que es inversa de A , entonces $A \cdot B = I$ y $\det A \det B = \det A \cdot B = \det I = 1 \times 1$

$-0 \times 0 = 1$. Como además $\det A$ y $\det B$ son números enteros, debemos tener $\det A = 1 = \det B$, o bien $\det A = -1 = \det B$. Para el converso, supongamos que $\det A$ vale 1 o -1. Definimos la matriz B sencillamente de la manera siguiente:

$$B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

El producto de A y B resulta ser:

$$A \cdot B = \begin{pmatrix} ad - bc & -ab + ba \\ cd - dc & -cb + da \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

lo que completa la prueba. □

ECHANDO VOLADOS POR TELÉFONO

Juan y María viven en ciudades distintas y desean verse. Juan le habla por teléfono y le pide que lo visite. María piensa que Juan es quien debe viajar. No se ponen de acuerdo.

—Ya sé, echemos un volado y el que pierda hace el viaje —dice Juan.

—Perfecto —dice María sacando de su bolsa una moneda—. Elige: águila o sol.

—Sol —pide Juan, al tiempo que escucha a María decir:— perdiste, tu harás el viaje.

¿Puede Juan confiar en que María no hizo trampa?

La misma situación del volado telefónico se presenta en muchas situaciones de la vida moderna. Por ejemplo, un banco A hace una transferencia al banco B por vía electrónica. ¿Cómo sabe el banco A que la información enviada llegó correctamente? ¿Cómo pueden estar seguros los dos bancos de que alguien no leyó la información enviada y puede hacer mal uso de ella?

Una propuesta para poder echar volados telefónicos sin que nadie sospeche que le están haciendo trampa es de Michael Rabin y se basa en el uso de las computadoras y algunas sencillas ideas matemáticas. Veamos qué deben hacer Juan y María para echar un “volado moderno”.

María y Juan encienden sus computadoras. María elige dos números primos p y q y no se los comunica a Juan, pero sí le da el resultado $n = pq$ de multiplicarlos. Digamos que María eligió $p = 11$ y $q = 19$, entonces le dirá a Juan el número $n = 209$. La computadora de Juan tiene un programa muy eficiente para saber si un número dado es primo o no lo es. Cuando Juan le da el número 209, su computadora inmediatamente le dice que no es un número primo. Lo que la computadora de Juan no puede hacer es calcular la descomposición de 209 en producto de primos.

En realidad, un número tan pequeño como 209 puede factorizarse rápidamente "a mano". Pero lo que los matemáticos no han podido hallar es una forma eficiente de factorizar números grandes, por ejemplo, un número de 200 cifras puede tardar meses en ser factorizado en primos aun por las más poderosas computadoras del mundo. Para que el ejemplo de Juan y María fuera más realista deberíamos utilizar dos números primos de alrededor de 100 cifras (estos números se conocen, pero no sería cómodo para el lector que aquí los usáramos).

Continuemos. Juan elige un número cualquiera menor que 209 y comprueba si divide a 209. Si esto ocurre, ya ganó el "volado moderno". Pero es muy improbable que esto suceda así. Digamos que escogió el número 17. Juan calcula con su computadora el residuo de dividir entre 209 el número que eligió al cuadrado, esto es, el residuo de dividir $17^2 = 289$ entre 209, que resulta 80. Se dice que 289 es *congruente* con 80 módulo 209 y se escribe $289 \equiv 80 \pmod{209}$. Es el número 80 el que Juan deberá de comunicar a María. Ahora, María utiliza un programa de su computadora para calcular todos los posibles números a tales que $a^2 \equiv 80 \pmod{209}$. El resultado es que los únicos números posibles son 17, 93, 116 y 192 (ya que por ejemplo, $93^2 = 8649 = 41 \times 209 + 80$). Pero observemos que $-17 \equiv 192 \pmod{209}$, al igual que $-93 \equiv 116 \pmod{209}$, de forma que bastará con considerar los números 17 y 93.

Finalmente, María debe comunicar a Juan uno de los dos números que obtuvo de su computadora. Si le da el número 17, Juan no sabrá nada nuevo ya que ése fue el número que él eligió, en ese caso habrá perdido el "volado moderno". ¿Qué pasa si María le da el número 93? En ese caso, Juan calcula la diferencia de los dos números que conoce $93 - 17 = 66$ y usa

su computadora para calcular el máximo común divisor de 209 y 66, que resulta ser 11. Al conocer este factor de 209, el otro factor se calcula inmediatamente para obtener que $209 = 11 \times 19$ y con esto Juan gana el “volado moderno”.

Dados números a , b y n , se dice que a y b son *congruentes módulo n* si $a - b$ es divisible entre n . En ese caso escribimos $a \equiv b \pmod{n}$. La aritmética modular es muy útil para esconder secretos. Es fácil codificar módulo un número, pero decodificar no es tan sencillo. Por ejemplo, $200 \equiv 2 \pmod{11}$. Aunque todo mundo sepa que usé el 11 para codificar y que mi resultado fue 2, no sabrán si mi número era 13, 24, 101 o 200, salvo que tengan información adicional. ¿Cómo se hace esto? Supongamos que María quiere comunicarle a Juan el mensaje simple: “ven”. Primero lo cambia a un número usando el código: $A = 01, B = 02, \dots, Z = 26$. De forma que su número es 220514. Cada par de cifras en este número es ahora elevado a una potencia fija s , digamos $s = 7$ y escrito módulo nuestro número compuesto $n = 209$. Obtenemos el número 155168174 (ya que $22^7 = 249435788 = 209 \times 11934726 + 155$, etcétera). Los números que María comunica a Juan son: 209, 7 y 155168174 sin temor de que su mensaje sea interceptado. Para descifrarlo, Juan debe conocer la factorización $209 = 11 \times 19$ (por cierto, el número s elegido debe no tener divisores comunes con $p - 1 = 11 - 1 = 10$ y con $q - 1 = 19 - 1 = 18$, por esto María eligió $s = 7$). El procedimiento de desciframiento consiste en elevar cada grupo de tres cifras del número 155, 168 y 174 a una potencia t , donde el número t sólo puede ser calculado por alguien que conozca los factores 11 y 19 de 209.

¿Cuál es este número t ? Como s no tiene divisores comunes con $(p - 1) \cdot (q - 1) = 180$, entonces hay números a y b de forma que $as + b(p - 1)(q - 1) = 1$, en nuestro caso $-77 \times 7 + 3 \times 180 = 1$, o sea, $a = -77$. Una aplicación del llamado *pequeño teorema de Fermat* nos dice que si $x^s \equiv y \pmod{n}$, entonces $y^a \equiv x \pmod{n}$. También se tiene que $x^a \equiv x^{(n+a)} \pmod{n}$. En nuestro caso, $n+a = 103$ y éste es el número t que buscábamos. En conclusión tenemos que $155^{103} \equiv 22 \pmod{209}$, $168^{103} \equiv 5 \pmod{209}$ y que $174^{103} \equiv 14 \pmod{209}$, cálculos que Juan lleva a cabo con su computadora para leer el mensaje que María envió.

Hemos oido muchas veces decir que algo "es tan cierto como que $2+2=4$ ". Qué sorpresa se llevarían muchos si supieran que se puede tener también que $2+2=1$. Por supuesto, esto no puede pasar en el mundo de la aritmética que hemos aprendido desde niños. Pero puede pasar en el mundo de la aritmética módulo 3.

En la aritmética módulo 3, tenemos que $3 \equiv 0 \pmod{3}$, que $4 \equiv 1 \pmod{3}$, que $5 \equiv 2 \pmod{3}$, que $6 \equiv 0 \pmod{3}$, y así sucesivamente. De hecho, todo número es congruente con algún 0, 1 o 2 módulo 3. Es como clasificar a todos los números en tres clases, dependiendo de con quién son congruentes. Todos los números congruentes con 0 módulo 3 forman una clase a la que llamaremos 0; todos los números congruentes con 1 módulo 3 forman otra clase a la que llamaremos $\bar{1}$; y finalmente los congruentes con 2 módulo 3 forman la clase $\bar{2}$.

¿Qué sucede con las operaciones de sumar y multiplicar en este mundo?

Por ejemplo, $1+2=3$, luego la suma de 1 y 2 módulo 3 deberá valer 0. Esto lo escribimos $\bar{1}+_3\bar{2}=\bar{0}$. También tenemos que $2\times 2=4$, luego deberemos tener que el producto de 2 y 2 módulo 3 es 1. Esto lo escribimos como $\bar{2}\times_3\bar{2}=\bar{1}$. Podemos obtener así tablas de sumar y multiplicar módulo 3 de la siguiente manera:

$+_3$	$\bar{0}$	$\bar{1}$	$\bar{2}$	\times_3	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Diremos que los números $\bar{0}$, $\bar{1}$, $\bar{2}$ con las operaciones de suma $+_3$ y de multiplicación \times_3 forman el *anillo* \mathbb{Z}_3 .

Por supuesto, el número 3 no tiene nada de especial. Podemos hacer aritmética módulo cualquier número. Por ejemplo, en la aritmética módulo 8 tenemos el anillo \mathbb{Z}_8 cuyos elementos son los números $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$ con la suma $+_8$ y la multiplicación \times_8 . Aquí se tiene, por ejemplo que $\bar{3}+_8\bar{6}=\bar{1}$ y que $\bar{4}\times_8\bar{5}=\bar{4}$. ¿Puede el lector calcular las tablas de sumar y multiplicar módulo 8?

CÓMO PARTIR
UN NÚMERO EN CUBOS

Considérese el número 19^{19} . ¿Puede este número escribirse como suma del cubo y la cuarta potencia de dos enteros?

Solución. No es posible. Por supuesto, no deseamos calcular explícitamente el valor de 19^{19} y todos los cubos y cuartas potencias menores.

Trabajaremos en la aritmética módulo 13. Aquí, $19 \equiv 6 \pmod{13}$ y $19^{19} \equiv 6^{19} \equiv 6^{12} \times 6^7 \equiv 1 \times 7 \pmod{13}$.

Calculando los cubos i^3 en \mathbb{Z}_{13} , resulta que un número a^3 , con a entero, puede ser congruente con 0, 1, 5, 8 o 12 módulo 13. Similarmente, un número b^4 , con b entero, puede ser congruente con 0, 1, 3 o 9 módulo 13. Luego la suma $a^3 + b^4$ puede ser congruente con cualquier número módulo 13, excepto el 7. Luego, el problema tiene respuesta negativa.

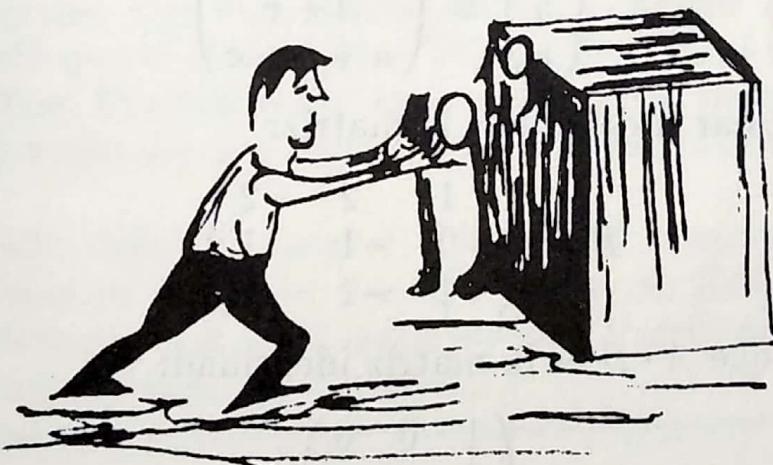


Figura V.1.

¿FUPNWB NWBUIRTJKCRDGXLUF?

Pocas personas pueden creer que es difícil inventar un método de escritura secreta que desafie la investigación. Sin embargo, puedo asegurar que el ingenio humano no puede crear un cifrado que el ingenio humano no pueda descifrar.

EDGAR ALLAN POE

¿Podrá usted descifrar el mensaje del encabezado de la sección? Para ayudarlo diremos que está codificado de forma que cada

letra tiene un valor numérico de la siguiente manera: $A = 1$, $B = 2$, $C = 3, \dots, Z = 26$.

El mensaje que se iba a codificar fue dividido en bloques de tres letras y codificado usando la matriz:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Finalmente el resultado numérico volvió a ser “traducido” a letras usando la aritmética módulo 26.

Solución. En primer lugar debemos tener claro que las operaciones que describimos antes para matrices de tamaño 2×2 pueden también efectuarse con matrices de tamaño 3×3 . Por ejemplo, el producto de la matriz A con una matriz columna se lleva a cabo en la siguiente forma:

$$A \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a + 2c \\ a + c \\ a + b + c \end{pmatrix}$$

En particular si definimos la matriz:

$$B = \begin{pmatrix} 1 & 2 & -2 \\ 0 & -1 & 1 \\ -1 & -1 & 2 \end{pmatrix}$$

calculamos que $A \cdot B$ es la matriz identidad:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Es la matriz B la que tenemos que usar para decodificar nuestro mensaje. Hay por supuesto la dificultad adicional de que el mensaje fue “traducido” a letras usando la aritmética módulo 26. Esto quiere decir que la letra F con la que comienza el mensaje puede corresponder a cualquier número n con la propiedad de que $n \equiv 6 \pmod{26}$. Entonces el primer bloque de tres letras FUP por decodificar corresponden a una columna de la forma:

$$v = \begin{pmatrix} 6 + 26a \\ 21 + 26b \\ 16 + 26c \end{pmatrix}$$

para algunos números a, b, c . Al multiplicar esta columna por la matriz B obtenemos:

$$B \cdot v = \begin{pmatrix} 16 + 26a + 52b - 52c \\ -5 - 26b + 26c \\ 5 - 26a - 26b + 52c \end{pmatrix}$$

Sabemos además que estos números deben estar entre 1 y 26. ¿Podemos encontrar los valores de a, b y c ? Del primer renglón de la columna deducimos que $a + 2(b - c) = 0$, del segundo renglón vemos que $-b + c = 1$ y del tercero que $-(a+b) + 2c = 0$. De esto es fácil deducir que $a = 2, b = 0$ y $c = 1$. Entonces FUP se decodifica como PUE. El resto del mensaje lo dejamos al lector interesado.

Por supuesto, hay muchas combinaciones de mecanismos para cifrar un mensaje. En 1839 Edgar Allan Poe desafiaba a sus lectores del *Alexander Weekly Messenger* a que le enviaran criptogramas que él descifraría. En febrero de 1840 un lector envió un criptograma que Poe afirmó no tenía ningún sentido. Fue sólo en 1975 que el matemático Winkel descifró el mensaje del lector de Poe. El cifrado era una combinación de métodos, un poco en el estilo del que hemos utilizado para el título de esta sección.

El método descrito para el cifrado del mensaje "ven" de María a Juan es el usado por el ejército de Estados Unidos (y probablemente por el de otros países). Parece ser el método más seguro de cifrado actualmente.
