SUMA 20
noviembre 1995, pp. 77-84

La matemática que protege de errores a los números de identificación

María Candelaria Espinel Febles
Pino Caballero Gil

IDEAS Y RECURSOS

Con este material pretendemos divulgar la matemática implicada en los números de identificación tales como NIF, ISBN, EAN... La aritmética modular se utiliza para fijar el dígito de control, y algoritmos sencillos permiten al ordenador descubrir muchas falsificaciones o posibles errores en el número de identificación de la tarjeta, producto o persona. Los esquemas de codificación más usuales detectan todos los errores simples, esto es, cuando se confunde un dígito por otro pero, sin embargo, no descubren otros tipos de errores que, aunque son menos frecuentes, son posibles. El álgebra y la divisibilidad ayudan a elegir esquemas de codificación más seguros.

Introducción

Letra del DNI

Si tiene interés en conocer el procedimiento que se utilizó para obtener la letra de su NIF, tome el número de su DNI y calcule el resto módulo 23 y luego consulte el resultado en la siguiente tabla:

0	T	8	P	16	Q
1	R	9	D	17	V
2	W	10	X	18	H
3	A	11	B	19	L
4	G	12	N	20	C
5	M	13	J	21	K
6	Y	14	Z	22	E
7	F	15	S	23	T

En la práctica puede dividir el número del carnet entre 23, despreciar la parte decimal, multiplicar por 23 y restarlo al número del carnet, así obtendrá un número entre 0 y 23 que le permitirá fijar la letra según la lista anterior.

Por ejemplo, para el DNI 78694024,

$$78694024 : 23 = 3421479.3$$

$$3421479 \times 23 = 78694017$$

$$78694024 - 78694017 = 7$$

Por lo tanto, le corresponde la letra F.

Número de las tarjetas

Las tarjetas de bancos y cajas de ahorros utilizan procedimientos análogos para garantizar su seguridad. Supongamos un usuario cuya tarjeta tiene el número:

5 02065 000457195 3

pero por equivocación el cajero lee el número:

5 02065 000457165 3.

Esta errata, como veremos más adelante, se puede detectar gracias al dígito que va al final, llamado dígito de control.

Para calcular el dígito de control se utilizan los 14 dígitos centrales, y sus posiciones se entienden siempre contadas desde la derecha. El procedimiento es el siguiente:

Paso 1: Se suman los dígitos de las posiciones impares, esto es, las posiciones 1, 3, 5, 7, 9, 11 y 13, y el resultado se multiplica por 2.

Paso 2: Se cuentan el número de dígitos en las posiciones impares que son mayores que 4, y se suma al resultado del paso 1.

Paso 3: Se suman los dígitos de las posiciones pares y se añade al resultado del paso 2 más 1.

Paso 4: El último dígito de la tarjeta o dígito de control es la cantidad necesaria para que al sumarla al resultado del paso 3 quede un múltiplo de 10.

En la tarjeta citada, los pasos serían:

P1: 5 + 1 + 5 + 0 +0 + 6 + 2 = 19

19 x 2 = 38

P2: 3 + 38 = 41

P3: 9 + 7 + 4 + 0 + 5 + 0 + 0 = 25

25 + 41 + 1 = 67

P4: 67 + 3 = 70, por lo tanto, el 3 es el dígito de control.

En el caso de la equivocación citada, en la que se cambió el 9 por el 6, el dígito de control da 6 en lugar de 3 como figura en la tarjeta.

Con los procedimientos dados puede comprobar la letra de su NIF y el dígito de control de su tarjeta. No obstante, según la red de cajeros a la que pertenezca podrían existir diferencias en el procedimiento.

Código de barras (EAN)

Aunque los dos ejemplos citados son de ámbito nacional, la idea de añadir un dígito para controlar los errores que puedan cometer las personas o las máquinas se utiliza a nivel internacional. Este es el caso del código de barras o EAN (European Article Numbering). La mayoría de los artículos que compramos lo llevan. En la caja se rastrea el código del artículo mediante un escáner, de modo que se envía el precio almacenado en la memoria de un ordenador a la pantalla de la caja registradora y, por último, a la factura del cliente.

...la idea de añadir un dígito para controlar los errores que puedan cometer las personas o las máquinas se utiliza a nivel internacional.

El código de barras lo forman doce números que se reparten de la siguiente forma: dos para el país, cinco para la empresa, cinco para el producto y además un último dígito de control para detectar errores.

El texto de Montaner-Moyano que se cita en la bibliografía tiene un código de barras acompañado de los siguientes dígitos:

97 88420 51877 0

El último dígito, 0 en este caso, es de validación, y permite comprobar que los datos anteriores son correctos.

El dígito de control o validación se comprueba mediante el procedimiento siguiente, donde las posiciones se entienden contadas desde la derecha:

Paso 1: Se suman los dígitos que ocupan posición impar.

Paso 2: Se suman los dígitos que ocupan posición par y el resultado se multiplica por 3.

Paso 3: Se suman los resultados de los pasos 1 y 2.

Paso 4: Se divide la suma por un número elegido, conocido como el módulo, que en este caso es el 10.

Paso 5: Se obtiene el resto de esta división, llamado resto módulo 10 de la suma. Si esta cantidad es 0, el código es correcto.

En nuestro ejemplo:

P1: 0 + 7 + 1 + 0 + 4 + 8 + 9 = 29

P2: 7 + 8 + 5 + 2 + 8 + 7 = 37

37 x 3 = 111

P3: 29 + 111 = 140

P4: 140 : 10 = 14

P5: 140 = 0 módulo 10.

Por tanto, el dígito de control es efectivamente 0.

Código para el pasaporte

En muchos países el pasaporte contiene también dígitos de control. En las aduanas existen máquinas para chequear estos dígitos. No se reconoce ese dígito a simple vista ya que aparece al final de un número que sí tiene relevancia, como es la fecha de nacimiento, número de pasaporte o fecha de caducidad. Los dígitos de chequeo se calculan utilizando un conjunto de reglas estándar. El procedimiento más común consta de los siguientes cuatro pasos:

Paso 1: Se multiplica cada dígito del número original por unas cantidades llamadas pesos. Los pesos que se eligen para el pasaporte son los dígitos de la serie 1731731731...

Paso 2: Se suman los resultados de sus multiplicaciones.

Paso 3: Se divide la suma por un número elegido, por convenio muchos países utilizan el número 10.

Paso 4: Se especifica el resto de esta división como dígito de chequeo.

Utilizando por ejemplo la fecha de nacimiento 3 de Septiembre de 1978 tenemos 030978. Pueden surgir problemas entre el orden del día y el mes, pues en algunos países se anota el mes antes que el día, así en nuestro ejemplo sería 090378, e incluso si se toma primero el año, se tendría 780903.

Siguiendo la costumbre española, la aplicación del proceso sería:

P1: Núm. original:	0	3	0	9	7	8
Pesos:	1	7	3	1	7	3
Productos:	0	21	0	9	49	24

P2: $0 + 21 + 0 + 9 + 49 + 24 = 103$

P3: $103 \div 10 = 10$, y resto 3

P4: el dígito de chequeo es el 3.

El número aparece en el pasaporte como 0309783.

Cálculos similares se hacen con el número del pasaporte o con la fecha de caducidad e incluso, en los países donde los ciudadanos tienen asignado tal número, con el número del carnet de identidad. La máquina de la aduana lee la zona y ejecuta los cálculos casi instantáneamente. Este proceso asegura que el pasaporte sea fiable y siga las reglas.

[En el ISBN] las dos primeras cifras nos dicen el país y la lengua en que se editó, las tres siguientes identifican la editorial y las cuatro siguientes, identifican al libro en sí.

ISBN para libros

Un código de ámbito internacional que se utiliza para identificar los libros es el llamado ISBN (International Standard Book Numbers). Por ejemplo, el texto de Montaner-Moyano (1989) que se cita en la bibliografía tiene el código:

ISBN 84-205-1877-8

Las dos primeras cifras, 84, nos dicen el país y la lengua en que se editó, las tres siguientes, 205, identifican la editorial y las cuatro siguientes, 1877, identifican al libro en sí. Además se añade un último dígito, 8, que informa de posibles errores al escribir alguno de los dígitos.

La última cifra de verificación se comprueba mediante el siguiente algoritmo:

Paso 1: Se multiplica cada dígito del número original por unos valores llamados pesos, que vienen dados por 10, 9, 8, 7, 6, 5, 4, 3, 2 y 1.

Paso 2: Se suman los resultados de sus multiplicaciones.

Paso 3: Se calcula el resto módulo 11 de la cantidad anterior.

Paso 4: Si ese resultado es 0 el dígito de control queda comprobado.

En el ejemplo anterior, el dígito de control 8 queda comprobado de la siguiente forma:

P1: Núm. original:	8	4	2	0	5	1	8	7	7	8
Pesos:	10	9	8	7	6	5	4	3	2	1
Productos:	80	36	16	0	30	5	32	21	14	8

P2: $80 + 36 + 16 + 0 + 30 + 5 + 32 + 21 + 14 + 8 = 242$

P3: $242 \equiv 0$ módulo 11

P4: El dígito 8 es correcto.

Sin el último dígito el resultado del Paso 2 sería 234, así que el 8 es el menor entero que permite conseguir un múltiplo de 11. Si fuese necesario un 10 como dígito de control se representaría por una X.

En los cinco ejemplos propuestos se han presentado cinco códigos actuales siguiendo la siguiente estructura. El NIF se describe de forma sencilla. El código de las tarjetas se presenta en forma de algoritmo. El código de barras se introduce como algoritmo que usa las clases residuales. El código para el pasaporte se presenta como un algoritmo que utiliza el producto escalar. El ISBN se describe en forma de algoritmo que utiliza a la vez las clases residuales y el producto escalar.

Con una lectura atenta de la descripción de los cinco procedimientos se puede deducir un método de funcionamiento común, que se pondrá de manifiesto en el siguiente apartado. Sin embargo, queremos hacer patente la diversidad en sus presentaciones puesto que de esta forma se abren más posibilidades en sus aplicaciones didácticas.

Clases residuales y producto escalar

En realidad casi todos los procedimientos anteriores se pueden describir en forma de algoritmos matemáticos que utilicen las clases residuales y el producto escalar para asignar un dígito de control (letra o número) para intentar detectar los errores que pudieran ocurrir en la transmisión de información. Por ello damos las siguientes definiciones básicas:

En general, si dos números enteros se diferencian en un múltiplo de un número entero n, se dice que son congruentes módulo n. En álgebra se utiliza la notación que sigue:

Si x e y son números enteros y $x - y$ es divisible por n se expresa como

$$x = y \pmod n$$

esto se lee, x es congruente con y, módulo n.

Se define el producto escalar de la cadena $x_1, x_2,\ldots, x_k$ y el vector de pesos $(\lambda_1,\lambda_2,\ldots,\lambda_k)$ como

$$(x_1,x_2,\ldots,x_k)\ (\lambda_1,\lambda_2,\ldots,\lambda_k) = x_1\lambda_1 + x_2\lambda_2 +\ldots+ x_k\lambda_k$$

Así, en general para obtener el dígito de control x_k, para una cadena $x_1, x_2,\ldots, x_{k-1}$ y un módulo n el dígito x_k se asigna de forma que cumpla la condición siguiente

$$(x_1,x_2,\ldots,x_k)(\lambda_1,\lambda_2,\ldots,\lambda_k) = 0 \pmod n$$

Veamos cómo quedan los esquemas de los cinco números de identificación descritos, utilizando ambas herramientas.

Letra del DNI

$$(x_1,x_2,\ldots,x_8,x_9,x_{10})(10^7,10^6,\ldots,10^0,-10^1,-10^0) =$$
$$= 10^7x_1+10^6x_2+\ldots+10^0x_8-10^1x_9-10^0x_{10} = 0 \pmod{23}$$

Donde x_9 y x_{10} representan la letra del NIF.

Número de las tarjetas

No es posible utilizar vectores ya que en el Paso 2 del algoritmo se impone la condición de elegir los dígitos mayores que 4 y este hecho no es posible expresarlo mediante un vector.

Código de barras

$$(x_1,x_2,x_3,\ldots,x_{12},x_{13})(1,3,1,\ldots,3,1)=$$
$$=x_1+3x_2+x_3+\ldots+3x_{12}+x_{13}=0 \pmod{10}$$

...casi todos los procedimientos anteriores se pueden describir en forma de algoritmos matemáticos que utilicen las clases residuales y el producto escalar

Aquí el dígito de control x_{13} se elige de forma que:

$$x_1+3x_2+x_3+\ldots+3x_{12}=-x_{13} \pmod{10}$$

Pasaporte

$$(x_1,x_2,x_3,x_4,x_5,x_6,x_7)(1,7,3,1,7,3,-1)=$$
$$=x_1+7x_2+3x_3+x_4+7x_5+3x_6-x_7=0 \pmod{10}$$

Luego el dígito de control x_7 se obtiene según:

$$x_1+7x_2+3x_3+\ldots+3x_6=x_7 \pmod{10}$$

ISBN

$$(x_1,x_2,\ldots,x_9,x_{10})(10,9,\ldots,2,1)=$$
$$=10x_1+9x_2+\ldots+2x_9+x_{10}=0 \pmod{11}$$

De manera que el dígito de control x_{10} viene dado por:

$$10x_1+9x_2+\ldots+2x_9=-x_{10} \pmod{11}$$

Otros códigos que se utilizan para chequear dígitos de control son los siguientes.

$$(x_1,x_2,\ldots)(7,3,9,7,3,9,\ldots)=0 \pmod{10}$$
$$(x_1,x_2,\ldots)(12,11,10,\ldots,3,2,1)=0 \pmod{10}$$
$$(x_1,x_2,\ldots)(1,2,3,4,5,6,7,8,1)=0 \pmod{10}$$
$$(x_1,x_2,\ldots)(2^1,2^2,2^3,\ldots,2^k)=0 \pmod{11}$$

Cálculo de probabilidades de detección de errores

Los esquemas anteriores permiten calcular dígitos que detectan errores. Los errores más frecuentes son los siguientes:

Error simple:

$$x \rightarrow y$$

Errores por transposición:

$$xy \rightarrow yx$$

Errores de transposición por salto:

$$x.y.z \rightarrow z.y.x$$

Error doble:

$$x\ldots y \rightarrow z\ldots t$$

Obviamente tanto los errores por transposición como los de transposición por salto son errores dobles.

A continuación calculamos las probabilidades de detección de algunos de estos errores en los cinco números de identificación presentados. Para su evaluación se cuentan los casos de no detección de error. En cada caso se considera la diferencia entre las cantidades resultantes de los productos escalares correspondientes al número correcto y al incorrecto. No se detecta aquel error que produzca una diferencia que sea múltiplo del módulo.

Letra del DNI

El código usado para el NIF, dada la ley de asignación de la letra, detecta el 100% de *errores simples,* pues un error de este tipo sobre un dígito que esté en la posición i produce un nuevo número cuya diferencia con el original viene dada por

$$k\,10^i,\ 0 < k < 10,\ i = 0,\dots,7$$

que de ninguna forma es múltiplo de 23. Por tanto, este nuevo número no puede tener asignada la misma letra que el anterior.

Por ejemplo, 78**6**94024F con un error simple en el 6 da 78**8**94024F. La diferencia 78894024 - 78694024 = 200000, de manera que la letra que le toca a 78894024 es E por ser 22 su módulo 23.

Este código también detecta el 100% de *errores por transposición.* Si es la letra la trasladada, se detecta automáticamente, y en el resto de casos, un número con dos dígitos adyacentes xy situados en posiciones i e $i-1$ respectivamente, que son traspuestos, difiere del original en una cantidad

$$(x-y-1)10^i + (10+y-x)10^{i-1} = 9(x-y)10^{i-1}$$

que nunca puede ser múltiplo de 23.

La evaluación de la probabilidad de *error de transposición por salto* es más complicada aunque tal como veremos en el próximo apartado, es 1.

En cuanto a los *errores dobles* existen casos que no se detectan. Así, por ejemplo, si la diferencia entre los números coincide exactamente con la diferencia entre las letras, el error no se descubre. También hay casos de error doble sin incluir la letra que no son detectados. Por ejemplo cuando 78**69**4024F se sustituye por 78**46**4024F no se detecta ningún error; esto ocurre siempre que la diferencia entre los números es múltiplo de 23.

...debemos fijarnos cuando realizamos la compra en el supermercado ya que [el código de barras] sólo se detectan los errores simples, aproximadamente un 89% de los errores de transposición y no muchos más errores.

Número de las tarjetas

Este código detecta el 100% de *errores simples.* Se tienen dos casos según si el error se comete en un dígito de posición impar o de posición par.

- Si el error se produce en un dígito de posición impar, la diferencia de la cantidad Q, resultante al final del Paso 3 del algoritmo de formación, con la del número original es una cantidad entre 1 y 19. Luego si resulta una diferencia de 10 tiene que ser porque el número ...x... se cambió por el número ...y... siendo $x - y = 5$ o $y - x = 5$, y simultáneamente los dígitos x e y son menores que 4 o mayores que 4, pero esto es imposible.
- Si el error se produce en un dígito de posición par, la diferencia de las cantidades Q es un valor entre 1 y 9, luego nunca es múltiplo de 10.

Las tarjetas de los bancos detectan el 99% de *errores de transposición.* Efectivamente, dado que si los dígitos xy se convierten en yx, la diferencia entre las cantidades Q viene dada por las tres posibilidades siguientes:

$y - x$, $y - x + 1$, $y - x - 1$ donde la primera corresponde al caso en que x e y son simultáneamente mayores o menores que 4. Pero salvo en el segundo caso y cuando el dígito en posición impar y, es el 9 y el dígito x en posición par es el 0 esas cantidades nunca son múltiplos de 10. Luego utilizando la regla de Laplace y dado que hay $14 \times 10 \times 9 = 1.260$ posibles errores por transposición entre los 14 dígitos del código y hay sólo 7 casos de no detección, la probabilidad de detección de error por transposición viene dada por 0,99.

En cuanto a *errores dobles,* esto es ...x...y... en lugar de ...z...t..., existen casos en los que el error no se detecta. Por ejemplo el código 4**50**8450122981109 que por un error doble de lugar al número 4**10**2450122981109 no se detecta, pues este último número también cumple satisfactoriamente las reglas de formación.

Código de barras

Este código detecta el 100% de *errores simples,* ya que si el dígito x se confunde con y se tiene una diferencia en el valor Q resultante del Paso 3, dada por:

- la cantidad $x - y$ si la posición del dígito es impar; y esta cantidad nunca puede ser múltiplo de 10,
- la cantidad $3(x - y)$ si la posición del dígito es par; cantidad que tampoco puede ser múltiplo de 10.

Sólo detecta el 88,9% de los *errores por transposición* porque si el error se produce sobre los dígitos x e y, se tiene una diferencia en Q dada por:

$$(x - y) + 3(y - x) = 2(y - x)$$

que es múltiplo de 10 siempre que $x - y=5$, o $y - x =5$, luego, dado que hay 10 casos favorables y 90 casos posibles, la probabilidad de no detección de errores es 10/90=0,1111, y la de detección de errores: 1 – 0,1111 = =0,889.

En cuanto a *errores dobles*, hay muchos que no se detectan, por ejemplo si 978847**6**15560**8** se confunde con 978847**2**15560**2**, el error no se detecta.

Como conclusión, debemos fijarnos cuando realizamos la compra en el supermercado ya que sólo se detectan los errores simples, aproximadamente un 89% de los errores de transposición y no muchos más errores.

Pasaporte

Se detecta el 100% de *errores simples* pues un error de sustitución de x por y produce una diferencia en la cantidad Q resultante del Paso 2, dada por una de las tres posibles expresiones

$$7(x - y),\ 3(x - y),\ x - y$$

que nunca puede ser múltiplo de 10.

En cuanto a los *errores por transposición xy* por *yx* la diferencia en Q viene dada por una de las siguientes expresiones:

$$7(x - y) + (y - x) = 6(x - y)$$

$$3(x - y) + y - x = 2(x - y)$$

$$x - y + 7(y - x) = 6(y - x)$$

que sólo es múltiplo de 10 cuando $x - y=5$ o $y - x=5$. Luego de forma idéntica al código de barras se tiene una probabilidad de detección dada por 0,88.

Este código no detecta todos los *errores dobles*, por ejemplo si el código 0**3**097**8**3 se confunde con 0**2**097**7**3, el error no se detecta.

ISBN

Este código detecta el 100% de los *errores simples* puesto que si el dígito i-ésimo x se confunde con y, la diferencia entre las cantidades Q resultantes del producto escalar, viene dada por $(x - y)i$ que nunca puede ser múltiplo de 11 puesto que $0 < i < 11$.

También detecta el 100% de *errores por transposición* ya que si los dígitos x e y en las posiciones $i-1$ e i se transponen, se produce una diferencia en las cantidades Q dada por

$$(x - y)(i - 1) + (y - x)i = y - x$$

que tampoco puede ser múltiplo de 11.

Los *errores de transposición por salto* también son detectados al 100% ya que como ocurría en el caso anterior si el error se produce sobre los dígitos x e y en posiciones i y j, la diferencia viene dada por

$$(x - y)i + (y - x)j = (x - y)(i - j)$$

que tampoco puede ser múltiplo de 11, ya que $0 < i, j < 11$.

En cuanto a *errores dobles* si los dígitos x e y en posiciones i y j se confunden con los dígitos z y t, la diferencia mencionada viene dada por

$$(x - z)i + (y - t)j$$

de manera que para que no se detecte, dicha cantidad tiene que ser múltiplo de 11. Por ejemplo, si el número 84**2**05187**7**8 se sustituye por 84**1**05186**7**8, el error no se detecta.

Resumimos en la siguiente tabla estas probabilidades de detección de error:

Error	*NIF*	*Tarjeta*	*EAN*	*Pasaporte*	*ISBN*
Simple	1	1	1	1	1
Transposición	1	0,99	0,89	0,89	1
Transp. por salto	1				1

De esta tabla se deduce que, a pesar de la diversidad de métodos, algunos están concebidos de manera que no detectan algunos errores.

Condiciones que deben cumplirse para detectar errores

La capacidad de detectar errores por medio de códigos lineales viene dada por el siguiente resultado.

TEOREMA. *Si un número de identificación $x_1x_2...x_k$ satisface la condición $(x_1,x_2,...,x_k)(\lambda_{1},_{2},...,\lambda_k) = 0 \ (mod\ n)$, entonces un error simple $x_i \rightarrow x_i'$ no se detecta si y sólo si $(x_i - x_i') = 0\ (mod\ n)$.*

Y un error de intercambio de dígitos de las posiciones i-ésima y j-ésima no se detecta si y sólo si $(x_i - x_i')(\lambda_i - \lambda_j) = 0\ (mod\ n)$

Como consecuencia del teorema anterior, las condiciones que debe cumplir el módulo n para proteger contra los distintos tipos de error son:

Error simple:

$$\text{mcd } (\lambda_i, n) = 1$$

Error por transposición:

$$\text{mcd } (\lambda_{i+1} - \lambda_i, n) = 1$$

Error de transposición por salto:

$$\text{mcd } (\lambda_i - \lambda_j, n) = 1$$

Según el teorema anterior se tienen las certificaciones siguientes sobre las capacidades de detección de error calculadas en el apartado anterior:

Letra del DNI

- mcd (10k, 23) = 1, luego detecta los errores simples.
- mcd (10i + 1 – 10i, 23)=1, luego detecta los errores por transposición.
- mcd (10i – 10j, 23)= 1, siendo $0 < i - j < 7$, luego detecta los errores de transposición por salto.

Código de barras

- mcd (3, 10) = mcd (1, 10) = 1, luego detecta los errores simples.
- mcd (2, 10) = 2, luego no detecta todos los errores por transposición ni los de transposición por salto.

Pasaporte

- mcd(7,10) = mcd(3,10) = mcd(1,10) =1, luego detecta los errores simples.
- mcd(4,10)=mcd(2,10)=mcd(6,10)=2, luego no detecta todos los errores por transposición ni los de transposición por salto.

ISBN

- mcd (k, 11) = 1, siendo $0< k< 10$, luego detecta los errores simples.
- mcd (1, 11)= 1, luego detecta los errores de transposición.
- mcd (i – j, 11)= 1, siendo $0 < i - j < 10$, luego detecta los errores de transposición por salto.

Según lo anterior resulta lógica la tendencia a usar como módulo un número primo, como son el 11 y el 23, ya que con éstos es más probable la detección de errores.

Reflexiones para el aula

A veces es difícil encontrar aplicaciones de las matemáticas que sean lo suficientemente sencillas y que puedan tener interés para el estudiante. Los códigos presentan ambas ventajas, por un lado, la matemática que necesitan es perfectamente asequible para los jóvenes y, por otro, los códigos tienen algo de misterio que les seduce.

Los contenidos matemáticos implicados en los códigos de identificación considerados en este trabajo son primordialmente los siguientes:

- Divisibilidad.
- Clases residuales.
- Algoritmos.
- Producto escalar.
- Álgebra.
- Probabilidad.

Encontrar el *resto de una división*, utilizando la tecla de memoria de la calculadora, es una habilidad que el joven debe adquirir superando el cálculo rutinario. Utilizar el número del DNI para obtener la letra que le corresponde en el NIF, como se muestra en el primer apartado, ofrece una oportunidad para ello.

Las *clases residuales* tienden a ser tema de un curso de álgebra de primero de carrera pero pensamos que se pueden introducir mucho antes. La aplicación más cotidiana de las clases residuales está en el reloj. Cuando son las 9 y pasan 8 horas decimos que son las 5, y sin embargo 9 + 8=17. Esto se escribe de la forma: 17 = 5 (mod 12), notación debida a Gauss. De la misma forma 9–11 = -2 = 10 (mod 12), y decimos que «–2 es congruente con 10 módulo 12».

Los restos módulo de los cinco números de identificación considerados se presentan mediante distintas formas. Unas veces se trata de calcular el dígito de control para que dé lugar a un múltiplo de 23, 10, 11,...; en otros se comprueba mediante un algoritmo la validez del dígito de control. Creemos que el concepto de divisibilidad debe estar por encima de la formalización algebraica de la teoría de congruencias que efectivamente puede reservarse para la enseñanza superior.

La idea de *algoritmo* se suele asociar casi siempre a las cuatro reglas y al algoritmo de Euclides. El concepto de algoritmo como proceso paso a paso aún tiene poca aceptación en la enseñanza, lo cual es una situación absurda, pues es una necesidad del presente en el manejo de ordenadores.

La matemática escolar introduce el *producto escalar* en el bachillerato. Los vectores aparecen en fuerzas, velocidades, aceleraciones, desplazamientos; mientras que del producto escalar se trabaja primordialmente el aspecto geométrico.

El concepto de algoritmo como proceso paso a paso aún tiene poca aceptación en la enseñanza, lo cual es una situación absurda, pues es una necesidad del presente en el manejo de ordenadores.

El producto escalar se puede trabajar a partir de la multiplicación ordinaria. Así aparece en el problema de hallar la cuenta a partir de un vector cantidad y un vector precio. Por ejemplo al calcular la cuenta de la siguiente compra:

	Garbanzos	*Lentejas*	*Patatas*
Cantidad	3	5	10
Precio	210	108	80

Vector cantidad: (3, 5, 10),

Vector precio: (210, 108, 80),

Producto escalar: (3x210 + 5x108 + 10x80).

De esta forma los vectores aparecen como cadenas sin necesidad de intervenir la magnitud con su dirección.

En este trabajo se han presentado varios códigos como productos escalares. Los alumnos podrían trabajar en la identificación de distintos códigos que se utilizan en la sociedad y expresarlos si es posible como un producto escalar tal como se muestran aquí. Esto les permitirá observar cómo el *álgebra* se puede utilizar para almacenar información de forma esquemática, en definitiva aprenderán la utilidad de los algoritmos algebraicos.

Seguramente a los jóvenes les resultará atractivo jugar a diseñar sus propios códigos pues el auge que éstos tienen en la compleja sociedad actual no descarta un posible uso comercial de alguna idea brillante.

Sorprende conocer lo poco seguros que resultan códigos que se utilizan con gran profusión en todo el mundo. Encontrar la *probabilidad* de un tipo de error en un código determinado resulta mucho más atractivo e incitante que resolver ese mismo problema pensando en urnas y bolas. En el apartado 3 de este trabajo se muestran algunos de estos cálculos. Confesamos que algunos suponen cierta dificultad, pero pensamos que ése es otro papel que tenemos que asumir los profesores ante los alumnos, que no lo sabemos todo.

Los profesores necesitamos abrir la matemática al mundo exterior, para alejar el peligro que supone la separación entre el aula y la sociedad.

Sin embargo, las matemáticas tienen ese encanto. A veces alguien encuentra un teorema que nos facilita el trabajo. Esto queda reflejado en el teorema del apartado 4 que ofrece una aplicación a la vida real de los números primos y la divisibilidad.

Los profesores necesitamos abrir la matemática al mundo exterior, para alejar el peligro que supone la separación entre el aula y la sociedad. Los matemáticos corremos el riesgo de que si no cambiamos nuestros métodos, los ciudadanos terminarán buscando su formación en otro lado. En definitiva, pensamos que los profesores debemos asumir que nuestros jóvenes necesitan de una matemática útil e interesante.

M.ª Candelaria Espinel
Pino Caballero
Universidad de La Laguna

Bibliografía

BARNES, S. y K. MICHALOWICZ (1994): «Bar-Code Activity Sheet. Mathematics», *Teaching in the Middle School*, 1,1, 59-65

GALLIAN, J. y S. WINTERS (1988): «Modular Arithmetic in the Marketplace», *The American Mathematical Monthly*, 95, 6, 548-551.

GALLIAN, J. (1991): «The Mathematics of Identification Numbers», *The College Mathematics Journal*, 22, 3, 194-202.

MONTANER, P. y R. MOYANO (1989): *¿Cómo nos comunicamos?*, Breda, Alhambra.

WHEELER, M. (1994): «Check-Digit Schemes», *The Mathematics Teacher*, 87, 4, 228-220.

SUMA

AVISO A SUSCRIPTORES

Se ruega a los suscriptores que tienen domiciliación bancaria remitan, si no lo han hecho ya, los siguientes datos:

1. Código de caja o banco.
2. Código de agencia.
3. DC.
4. Código cuenta (10 dígitos)

Revista SUMA. ICE Universidad de Zaragoza. Pedro Cerbuna, 12. 50009 ZARAGOZA