MSEL
Modelling in Science Education and Learning

Modelling in Science Education and Learning
Volume 9 (2), 2016 doi: 10.4995/msel.2016.63380.
Instituto Universitario de Matemática Pura y Aplicada
Universitat Politècnica de València

Algunos secretos del documento nacional de identidad español: una aplicación de la aritmética modular a códigos detectores de errores

Some secrets of the Spanish national identity document: an application of modular arithmetics to error detecting codes

Ramón Esteban Romero[a]
Departament de Matemàtiques
Universitat de València.
Ramon.Esteban@uv.es

[a]Dirección permanente: Institut Universitari de Matemàtica Pura i Aplicada, Universitat Politècnica de València, resteban@mat.upv.es

Abstract

Presentamos algunos caracteres y dígitos de control que aparecen en el documento nacional de identidad español como ejemplo de aplicación de la aritmética modular al diseño de códigos detectores de errores. Esta actividad se ha desarrollado dentro del programa ESTALMAT de estímulo del talento matemático y en los campus científicos de verano organizados por VLC/Campus.

We present some control characters and digits present in the Spanish national identity document as an example of the application of modular arithmetics to the design of error correcting codes. This activity has been developed inside the ESTALMAT programme for the stimulation of mathematical talent and in the summer scientific campuses organised by VLC/Campus

Keywords: Modular arithmetics; control digit or character; coding theory.
Palabras clave: Aritmética modular; dígito o carácter de control; teoría de códigos.

1. Introducción

El objeto de esta nota es describir una actividad llevada a cabo con estudiantes de enseñanza secundaria obligatoria y de bachillerato en el ámbito del programa de estímulo del talento matemático ESTALMAT (Esteban Romero, 2011a), dirigido a alumnos entre 12 y 14 años, y del curso de matemáticas del campus científico de verano organizado por VLC/Campus (Crespo, Esteban, Miralles, & Thibaut, 2012), dirigido a alumnos de cuarto curso de ESO y primero de bachillerato. En estas actividades se presenta una breve introducción a la teoría de códigos y a la criptografía y se muestran algunos códigos y sistemas criptográficos basados en la aritmética modular.

Una de las tareas propuestas en dicho curso es el análisis de dígitos y caracteres de control presentes en el documento nacional de identidad (DNI) utilizado en España. Se pueden ver algunas de sus características en (Dirección General de la Policía, 2016). La motivamos con las tres líneas de caracteres que aparecen en el reverso. Una leyenda urbana afirma que el último dígito de la segunda línea se corresponde con el número de personas que comparten nombre y apellidos con el titular del documento. Parece un poco inútil codificar esta información, que puede cambiar según pasa el tiempo, en el documento. El objetivo de esta nota es presentar algunos de los resultados a los que se llega con el análisis del DNI que proponemos. Esta actividad también se puede plantear como aplicación de resultados sobre divisibilidad y aritmética modular.

2. La redundancia para detectar y corregir errores

En un proceso de comunicación, un emisor envía un mensaje a un receptor mediante un canal. El canal puede tener ruido que hagan que el mensaje no llegue con claridad al receptor o pueda venir modificado. Aquí el concepto de ruido abarca no solo el sonido, sino cualquier elemento que pueda transformar el mensaje o hacerlo ininteligible, como una interferencia electromagnética si el mensaje se transmite por un cable o por ondas electromagnéticas. Un ejemplo es la transmisión de un mensaje oral cuando hay otras personas gritando alrededor. En esta ocasión, el receptor solicita al emisor que repita el mensaje. Esta repetición puede hacer que el mensaje sea recibido correctamente y es clave en la teoría de códigos.

Otro ejemplo interesante es la lectura de textos con algunas faltas de ortografía, pero no demasiadas. A pesar de las faltas de ortografía, en muchas ocasiones el receptor puede encontrar el mensaje correcto más cercano y pensar que este es el mensaje que se deseaba enviar. Esta es otra muestra de que en el lenguaje habitual hay una redundancia que permite detectar y corregir errores.

3. Detección y corrección de errores

Para presentar de manera intuitiva las nociones de detección y corrección de errores, podemos hablar de los códigos de repetición. Supongamos que cada vez que queremos transmitir un mensaje, lo enviamos por duplicado. Por ejemplo, enviamos el mensaje «`HOLA`» como «`HOLAHOLA`». Supongamos que se produce un error en el envío y que la segunda «`H`» se recibe como «`S`», es decir, se recibe «`HOLASOLA`». El receptor observa que no ha recibido dos copias del mismo mensaje, con lo que sabe que se ha producido un error y puede pedir que vuelvan a enviar el mensaje, por ejemplo. Sin embargo, es incapaz de averiguar cuál era el mensaje correcto. De este código podemos decir que *detecta un error*, pero *no corrige errores*.

Una variación del código anterior consiste en enviar el mensaje por triplicado. Así, para enviar «HOLA» transmitiríamos «HOLAHOLAHOLA». En caso de saber que se ha producido un error, por ejemplo, enviando «HOLASOLAHOLA», sabemos que el mensaje se ha enviado con errores, ya que no se han recibido tres copias del mismo mensaje, sino que, además, somos capaces de identificar el mensaje correcto, ya que hay dos copias con el mensaje correcta. Por ello, podemos decir que este código permite *corregir un error*. Además, si se producen dos errores, por ejemplo, «BOLASOLAHOLA», sabríamos que se han producido errores, pero no siempre podríamos recuperar el mensaje exacto.

4. Dígitos o caracteres de control

Repetir el mensaje una o dos veces puede suponer tener que enviar demasiada información de una vez. Por eso a veces se envía un *resumen* de la información en forma de *dígito de control* o *carácter de control*. El código de paridad usado en informática es un ejemplo. Dada una secuencia de unos y ceros, se transmite la secuencia seguida de un uno si el número de unos es impar, y de un cero si el número de unos es par. De este modo, en un mensaje correcto recibido se tiene que recibir siempre una cantidad par de unos. Este método detecta un error, pero no permite corregir errores.

5. La letra del DNI

El artículo 113 de la ley 33/1987 de presupuestos generales del estado para 1988 dispuso que las personas físicas o jurídicas debían tener un número de identificación fiscal (NIF) para sus relaciones de naturaleza o con trascendencia tributaria. En el real decreto 338/1990 de 9 de marzo se regula la composición y la forma de utilización del NIF. En él se indica que consistirá del *número de su documento nacional de identidad seguido de un código o carácter de verificación, constituido por una letra mayúscula que habrá de constar en el propio documento nacional de identidad, de acuerdo con sus disposiciones reguladoras*. En la orden ministerial del 14 de marzo de 1990 del Ministerio de Economía y Hacienda se aprueba el modelo de tarjeta donde constará el NIF. Sin embargo, en ninguno de estos documentos publicados en (Agencia Estatal Boletín Oficial del Estado, 2016) se indica cómo se obtiene la letra del NIF, que posteriormente fue incorporada al DNI.

La letra del DNI se obtiene simplemente calculando el resto de la división del número del DNI entre 23. La letra se calcula siguiendo la tabla 1.

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

Tabla 1: Letra del DNI

No resultará muy difícil darse cuenta de que 23 es un número primo, concretamente, es el mayor primo menor que el número de letras del alfabeto (27). Además, las letras que eliminamos son la «Ñ», fácilmente confundible con la «N», la «I» y la «O», que se pueden confundir fácilmente con cifras, y la «U».

Nuestro objetivo ahora es comprobar que la letra del DNI sirve para verificar el número, esto es, que el código correspondiente a añadir al número del DNI la letra permite detectar un error.

Para ello tenemos que recurrir a resultados de divisibilidad y aritmética modular. Algunos de estos resultados se pueden encontrar en (Fuster, 2009; Vera López & Esteban Romero, 1995). Concretamente, necesitaremos los siguientes resultados:

Teorema 1 *Dados dos números enteros a y b y un natural m, los restos de las divisiones de a y b entre m coinciden si, y solo si, m es divisor de $b-a$.*

Teorema 2 *Supongamos que m es un natural divisor del producto ab, con a, b enteros, y que* $\mathrm{mcd}(a,m)=1$. *Entonces m es un divisor de b.*

También nos interesa recordar la interpretación de la escritura de un número natural en una base, en nuestro caso, la decimal.

Notación 3 *El número a con representación decimal $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ es*

$$a = \sum_{i=0}^{n} a_i 10^i,$$

donde $0 \le a_i \le 9$ para $0 \le i \le n$.

Teorema 4 *La letra del DNI permite detectar un error.*

Demostración. Consideremos dos números de DNI

$$a = \sum_{i=0}^{7} a_i 10^i, \qquad b = \sum_{i=0}^{7} b_i 10^i$$

que se diferencian en la cifra $a_j \neq b_j$ y $a_i = b_i$ para $0 \le i \le 7$, $i \neq j$. Supongamos que tienen asociada la misma letra. Entonces los restos de las divisiones de a y b entre 23 coinciden. Por el teorema 1, 23 es divisor de $a-b$. Pero $a-b=(a_j-b_j)10^j$. Como 23 divide $(a_j-b_j)10^j$ y $\mathrm{mcd}(23,10)=1$, se sigue por el teorema 2 que 23 divide a_j-b_j. Pero a_j y b_j son números entre 0 y 9, con lo que su diferencia a_j-b_j será un entero entre -9 y 9. El único entero múltiplo de 23 entre -9 y 9 es 0, pero en este caso se tiene que $a_j=b_j$, en contra de nuestra hipótesis. Esto nos permite concluir que la letra del DNI nos permite detectar un error. □

La letra del DNI no permite detectar dos errores. Para ello, nos basta con observar que los números 23232323T y 23232300T son correctos y se diferencian en dos cifras. También vemos que no nos permite corregir errores, ya que si cambiamos en 23232323T la última cifra por 0, obtenemos 23232320T, que es incorrecto, pero tanto 23232323T como 23232300T son números de DNI correctos que se distinguen solo en una cifra de nuestro número.

Otro error típico es el de intercambiar dos cifras consecutivas a la hora de escribir el DNI. Veamos que el código del DNI también nos permite identificar este error.

Teorema 5 *La letra del DNI permite detectar el intercambio de dos cifras consecutivas.*

Demostración. Supongamos que tenemos dos números de DNI

$$a = \sum_{i=0}^{7} a_i 10^i, \qquad b = \sum_{i=0}^{7} b_i 10^i$$

de manera que $a_j = b_{j+1}$, $a_{j+1} = b_j$, donde $0 \leq j \leq 6$, y que $a_i = b_i$ para $0 \leq i \leq 7$, $i \notin \{j, j+1\}$. Como en la demostración del teorema 4, se tiene que 23 divide

$$\begin{aligned} a - b &= (a_{j+1} - b_{j+1})10^{j+1} + (a_j - b_j)10^j = (a_{j+1} - a_j)10^{j+1} + (a_j - a_{j+1})10^j \\ &= (a_{j+1} - a_j)(10^{j+1} - 10^j) = (a_{j+1} - a_j)(10 - 1)10^j = (a_{j+1} - a_j) \cdot 9 \cdot 10^j. \end{aligned}$$

Por el teorema 2, como $\mathrm{mcd}(23, 9) = 1$ y $\mathrm{mcd}(23, 10) = 1$, se sigue que 23 es divisor de $a_{j+1} - a_j$. Como $a_{j+1} - a_j$ es la diferencia entre dos cifras, es un entero entre -9 y 9. Pero la única posibilidad para que un entero así sea múltiplo de 23 es que $a_{j+1} - a_j = 0$, es decir, $a_{j+1} = a_j$. En este caso, el intercambio de las dos cifras deja iguales los números del DNI. Concluimos que la letra del DNI permite detectar el intercambio de dos dígitos. □

6. La zona de lectura óptica del DNI

El reverso del DNI contiene tres líneas de caracteres diseñadas para su lectura por dispositivos de reconocimiento de texto (OCR). La primera línea contiene las letras «IDESP» que indican que es un documento de identidad expedido por España. A continuación aparece el el número de la tarjeta, que consta de tres letras y seis cifras, y un dígito de control. Seguidamente, aparece el número del DNI con su letra de control. A continuación aparecen caracteres «<» para completar. En la segunda línea aparecen los dos últimos dígitos del año de nacimiento, el mes de nacimiento (con dos cifras) y el día de nacimiento (con dos cifras), seguidos de un dígito de control. A continuación aparece la letra «M» o «F», según el titular sea hombre o mujer, respectivamente. Las siguientes seis cifras corresponden a la fecha de caducidad del documento, en el mismo formato que la fecha de nacimiento, seguidas de un dígito de control. Este último dígito es el que ha sido objeto de la leyenda urbana a la que aludíamos en Las tres letras siguientes corresponden a la nacionalidad del titular, habitualmente «ESP». Después vienen unos caracteres de relleno «<». La tercera línea contiene los apellidos, separados con un separador «<», y el nombre, separado del apellido con dos caracteres «<<», y más caracteres «<» para rellenar.

El procedimiento para calcular el dígito de control asociado a una fecha $abcdef$ consiste en multiplicar sucesivamente las cifras por 7, 3, 1, 7, 3, 1, sumar los resultados, y quedarse con la última cifra. Esto coincide con el resto de la división de $7a + 3b + c + 7d + 3e + f$ entre 10. Notemos que, en el caso de la letra del DNI, los coeficientes son las potencias de 10 en vez de 7, 3, 1, ... y el número entre el cual había que dividir era 23 en lugar de 10. El dígito de control del número de tarjeta se calcula de manera parecida, considerando las tres letras y las seis cifras del número de tarjeta, asignando valores a las letras según la tabla 2, multiplicándolas por 7, 3, 1, 7, 3, 1, 7, 3, 1, sumando los resultados y quedándonos con la última cifra.

A	10	K	20	U	30
B	11	L	21	V	31
C	12	M	22	W	32
D	13	N	23	X	33
E	14	O	24	Y	34
F	15	P	25	Z	35
G	16	Q	26		
H	17	R	27		
I	18	S	28		
J	19	T	29		

Tabla 2: Asignación de valores a letras en la zona de lectura óptica del DNI

Nos queda el dígito de control de la segunda fila. Este dígito se obtiene considerando la secuencia formada por el número de tarjeta (letras y números), su dígito de control, el número de DNI con su letra de control, la fecha de nacimiento con su dígito de control y la fecha de caducidad con su dígito de control. No consideramos «IDESP», el sexo o la nacionalidad. Se asignan valores a las letras según la tabla 2. Se multiplican sucesivamente por 7, 3, 1, 7, 3, 1, ..., se suman los resultados y la última cifra corresponde al dígito de control. La leyenda urbana a la que aludíamos queda desmontada.

Una pregunta razonable es por qué se usan los dígitos 7, 3 y 1. Parece que estos dígitos tengan alguna relación con la posibilidad de detectar errores y así es. Es claro que la sustitución de letras por otras cuyo número asociado acabe en la misma cifra nos dará el mismo dígito de control, así que nos fijaremos únicamente en las cifras. Razonamos como con el DNI. Supongamos que sustituimos una cifra a por otra cifra b. La diferencia entre los números obtenidos al multiplicar por 7, 3, 1, ... y sumar los resultados será de la forma $7(a-b)$, $3(a-b)$ o $a-b$, según el factor sea 7, 3 o 1, respectivamente. Estos números tienen que ser múltiplos de 10. Como $\mathrm{mcd}(10,7) = \mathrm{mcd}(10,3) = 1$, en los tres casos se tiene que 10 ha de ser divisor de $a-b$. Pero como $a-b$ es un entero entre -9 y 9, la única posibilidad es que $a-b=0$, es decir, $a=b$. Esto nos muestra que la sustitución de una cifra por otra queda detectada por estos códigos. También vemos que el hecho relevante aquí es que el factor por el que multiplicamos cada cifra ha de ser primo con 10. Esto nos da las posibilidades 1, 3, 7 y 9 para los coeficientes. Este último valor también nos valdría. No se podría aplicar este argumento con 2, 4, 5, 6, 8, 0: por ejemplo, con el coeficiente 8 se tendría que las cifras 2 y 7 contribuirían a la suma en $8 \cdot 2 = 16$ y $8 \cdot 2 = 56$, cuya diferencia es múltiplo de 10.

Debemos notar que este código no siempre detecta el intercambio de cifras consecutivas. Supongamos que intercambiamos las cifras a y b con coeficientes 7 y 3, respectivamente. Entonces la diferencia es $7a + 3b - (7b + 3a) = 4(a-b)$, que es múltiplo de 10 siempre que $a-b$ sea múltiplo de 5. Esto permite, además de $a=b$, las posibilidades $a = b+5$ y $a = b-5$. Por ejemplo, el intercambio de dos cifras consecutivas 3 y 8 no lo distingue el código. Pero no parece que este sea un problema muy grave, ya que estas tres líneas están diseñadas para ser leídas con sistemas de reconocimiento de caracteres y parece más fácil que haya una duda en la lectura de un carácter que en la lectura automatizada se produzca un intercambio de dos cifras.

7. Otros códigos

Otros códigos, como los asociados a los códigos de barras que se leen con lectores láser en tiendas o los dígitos de cuentas bancarias, se basan en estos mismos principios. Se puede analizar con estas mismas técnicas su capacidad de detectar errores. En los talleres de Estalmat (Esteban Romero, 2011b, 2011a) o de VLC/Campus (Crespo et al., 2012) analizamos también estos códigos.

Agradecimientos: El autor agradece la financiación del proyecto MTM2014-54707-C3-1-P del Ministerio de Economía y Competitividad (España) y FEDER (Unión Europea).

Referencias

Agencia Estatal Boletín Oficial del Estado (2016).
Boletín Oficial del Estado.
http://www.boe.es

Bravo, P., Ferrando, J. C., Martínez Pastor, A. (1994).
Complementos de matemática discreta. Curso práctico (Vol. SPUPV-94.756).
Valencia: Servicio de Publicaciones UPV.

Crespo, R., Esteban, R., Miralles, A., Thibaut, E. (2012).
Campus científico VLC/Campus 2012: Matemáticas, criptografía y códigos, cómo usar las matemáticas para entendernos. el extraño caso del inspector Scorpe.
Notas del curso. Valencia.

Dirección General de la Policía. (2016).
DNI electrónico.
http://www.dnielectronico.es

Esteban Romero, R. (2011a).
Criptografía y códigos.
Estalmat Comunitat Valenciana.

Esteban Romero, R. (2011b).
La aritmética del reloj.
Estalmat Comunitat Valenciana.

Fuster, R. (2009).
Matemàtica discreta.
València: Editorial Universitat Politècnica de València.

Vera López, A., Esteban Romero, R. (1995).
Problemas y ejercicios de matemática discreta.
Bilbao: AVL.