gamma colaboracións

Eses números tan próximos

JOSÉ MARÍA BARJA PÉREZ

Fronte ao anumerismo que nos envolve, na vida cotiá manexamos constantemente números e códigos. Coñecelos forma parte tamén da formación cultural que debemos transmitir.

Palabras chave: Números, códigos, código de barras, IBAN.

Those close numbers

In everyday life we constantly handle numbers and codes, compared to innumeracy that surrounds us. Knowing them is also part of the cultural education we should transmit.

Key words: Numbers, codes, barcode, IBAN.

É tan característica da nosa época a abundancia de números que nos rodean, que apenas lles prestamos atención. E, con todo, unha mirada atenta permite espertar a curiosidade e xustificar a importancia que ten para calquera persoa un coñecemento dos números, algo superior ao necesario cómputo elemental.[1]

Billetes

Se algo chama a atención a pequenos e maiores é a simboloxía dos billetes, que é repetidamente explicada en termos de arte e achegas culturais. Pero nos billetes do euro descubrimos que cada un deles é identificado cunha cadea de números precedidos dunha letra, que aparecen dobremente impresos no dorso. Aparentemente arbitrarios, gardan con todo información curiosa e un antigo algoritmo de verificación de operacións aritméticas.

A letra identifica o país emisor do billete, segundo unha asignación[2] algo estraña: **Z**, Bélxica; **Y**, Grecia; **X**, Alemaña; **V**, España; **U**, Francia; **T**, Irlanda; **S**, Italia; **P**, Países Baixos; **N**, Austria; **M**, Portugal; **L**, Finlandia; **H**, Eslovenia; **G**, Chipre; **F**, Malta; **E**, Eslovaquia; **D**, Estonia [ademais están reservadas: **W**, Dinamarca; **R**, Luxemburgo; **K**, Suecia; **J**, Reino Unido; pero non se usarán I, O, Q evitando que se poidan confundir con 1 ou 0].

En canto aos 11 números, levan implícita unha verificación formal de validez: ao precedelos cos dous díxitos que corresponden á letra na orde alfabética usual, o número resultante de 13 díxitos **debe ter** resto **8** ao dividilo por 9. Para os descoidados, esa operación realizábana habilmente os mestres no século pasado para verificar de forma rápida que os seus alumnos foran capaces de realizar correctamente unha división. Chamada "proba do nove" (en inglés, *casting out nines*) aparecerá definida na 23ª edición[3] do DRAE como «cálculo sinxelo que serve para verificar o resultado das operacións aritméticas, especialmente na multiplicación e na división, fundado en que o resto de dividir un número por nove é o mesmo que o de dividir tamén por nove a suma das súas cifras.» Tamén chamada "redución a unha cifra", a reiterada suma das cifras ata que quede unha soa, é a descrición algorítmica do cálculo do resto de dividir por 9 unha cifra dada. Por exemplo o número do billete reproducido abaixo, que corresponde a Países Baixos, é P03200281138; como P é a 16ª letra, o número 1603200281138 "redúcese" a 35, que, á súa vez, dá 8, ou, $1603200281138 \equiv 8 \pmod 9$.[4]

A "proba do nove" aplicada para verificar a corrección de operacións aritméticas baséase no traslado homomórfico das contas á aritmética módulo nove. Dise que como *abjectio novenaria* foi coñecida polo bispo romano Hipólito no século III e que Ibn Sina (Avicena, nacido no actual Usbequistán) contribuíra ao desenvolvemento desa técnica, empregada polos matemáticos indios do século XII. Pero moitos non son conscientes de que esta "proba" pode dar falsos positivos.[5] Por seguir o exemplo recollido na páxina de instrucións do pasatempo *Murphyx*, a comprobación para a operación 21 x 38 = 798 sería 3 x 2 ≡ 6 (mod 9), pero a "proba" tamén daría por correcta esa multiplicación se se dese como resultado 708, 807 ou 816.

Aínda que non na forma actual, ese método de verificar o cálculo era mesmo anterior ao uso das cifras. Os romanos operaban non tanto con algoritmos senón mediante soportes físicos diversos como pedriñas, *calculus*, ou instrumentos asimilables aos máis recentes ábacos; pero a base decimal do sistema faría posible formular un procedemento análogo sen o estímulo da imaxe gráfica das cifras. Estas permiten unha explicación completa, verosimilmente formulada polos matemáticos indios, quen estableceron o sistema de notación que agora usamos. De feito, unha primeira explicación do sistema aparece en Occidente no libro de 1202, *Liber abbaci* de Fibonacci, que serviu para difundir por Europa o *Modus indorum* e os primeiros algoritmos do cálculo, e onde se detalla por que 37 x 37 = 1369.

As cifras

Sorprende a moitas persoas o descubrir que a representación dos díxitos non é a mesma en todo o mundo. De feito, a notación árabe, a bengalí e a chinesa son empregadas na actualidade por millóns de persoas e case esquecemos que as nosas cifras (de *sifr* "baleiro", ou cero) son tan só unha das evolucións dos símbolos orixinais indios, que eles manexaban seis séculos antes de que chegasen a Occidente. Do orixinal brahámico +, que representaba a cifra catro, derivaron (véxase a páxina 894 de [4]) tanto o noso **4**, como o **8** que empregan os 163 millóns de habitantes de Bangladesh, xunto a outros 83 millóns de persoas dos estados indios de Bengala Occidental e Tripura.[6]

Occidental	0	1	2	3	4	5	6	7	8	9
Arábigo	٠	١	٢	٣	٤	٥	٦	٧	٨	٩
Bengalí	০	১	২	৩	৪	৫	৬	৭	৮	৯
Chinés		一	二	三	四	五	六	七	八	九

A contribución matemática doutro oriúndo de Uzbekistan, *Abū Ja'far Muhammad Ben Mūsa Al Khuwarizmī*, non é suficientemente destacada (se o é en [4], páxs. 1230-1233; véxase tamén [1], páxs. 91-92). Nado no ano 783 en Jiva, no Jorezm (Usbequistán), viviu en Bagdad (cara ao 850, alí morreu), na corte do califa abasí *Al Ma'mūn*, pouco tempo despois de que Carlomagno fose nomeado emperador de Occidente. Era un dos membros máis importantes do grupo de matemáticos e astrónomos que traballaron na *Bayt al Hikma* (*Casa da Sabedoría*, que hoxe correspondería á Academia de Ciencias de Bagdad). A súa celebridade está unida a dúas das súas obras: *Al jabr wa'l muqābala* que refire as operacións preliminares para resolver ecuacións (*al jabr*, "compoñer", pasar os termos dun membro a outro da igualdade de modo que só haxa termos positivos na ecuación; *muqābala* "reducir", sumar os membros do mesmo tipo da ecuación); na segunda, *Kitab al jāmi' wa'l tafrīq b hisāb al hind*, explicaba como os indios, mediante a numeración decimal posicional, realizaban a adición e a subtracción, recomendando non esquecer escribir os ceros para non confundirse. Estes libros do século IX, coñecidos por traducións[7] ao latín realizadas a partir do século XII, introduciron eses avanzados métodos nun Occidente que aínda empregaba a numeración romana e calculaba con medios "pedestres". Ademais de dar significado matemático á **álxebra** (engadido ao común de "compor ósos", que xa estaba incorporado ao castelán e ao italiano)[8], o nome do autor pasa a designar xenericamente o sistema constituído polo cero, e nove cifras e os procedementos de cálculo procedentes da India. A transliteración do nome, e así a designación do sistema, vai variando desde *alchoarismi*, *algorismi*, *algorismus* e finalmente *algoritmo*, moito antes de alcanzar a acepción máis ampla e abstracta que hoxe lle atribuímos (a base mesma da teoría e práctica dos computadores).

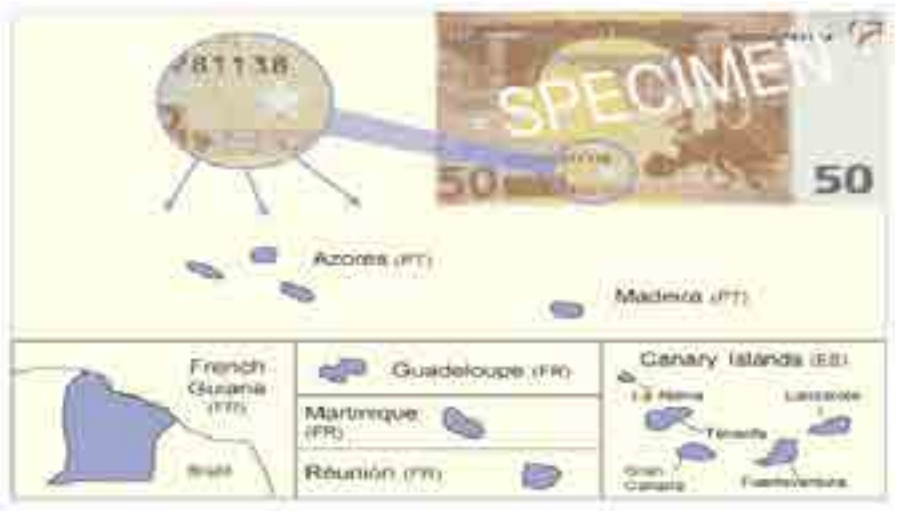
Como se pide a transversalidade das materias, aquí temos un bo exemplo de achegas lingüísticas da matemática. Variantes de nomes da obra e o "apelido" Al Khuwarizmī proporcionaron polo menos catro "lemas lingüísticos" nos nosos idiomas. Di o Dicionario da RAG [http://www.realacademiagalega.org/dicionario#inicio.do]: «*algarismo arábigo* Signo de orixe árabe que representa os números no sistema decimal»; «*algoritmo* Conxunto de regras que, ao aplicalas, permiten resolver un problema mediante un número finito de operacións»; «*álxebra* Rama das matemáticas que estuda a cantidade en xeral, as súas estruturas, relacións, operacións, etc., utilizando letras ou signos en lugar de números. Tratou de aplicar a álxebra aos problemas da lóxica; Asunto moi complicado ou difícil de entender. Para min o que estaba dicindo era álxebra pura»; «*alxebrista* Persoa versada en álxebra».

Esténdese máis o Dicionario da RAE: «*guarismo, ma* Perteneciente o relativo a los números; Cada uno de los signos o cifras arábigas que expresan una cantidad»; «*algoritmo* (quizá del latín tardío *algobarismus*, y este abrev. del ár. clás. *ḥisābu lgubār* 'cálculo mediante cifras arábigas'[9]) Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema; Método y notación en las distintas formas del cálculo»; «*álgebra* (del latín. tardío *algĕbra*, y este del ár. clás. *alǧabru* [*walmuqābalah*] reducción [y cotejo]') Parte de las matemáticas en la cual las operaciones aritméticas son generalizadas empleando números, letras y signos. Cada letra o signo representa simbólicamente un número u otra entidad matemática. Cuando alguno de los signos representa un valor desconocido se llama incógnita; desus. Arte de restituir a su lugar los huesos dislocados»; «*algebrista* Persona que estudia, profesa o sabe el álgebra (‖ matemática); desus. Cirujano dedicado especialmente a la curación de dislocaciones de huesos; germ. Alcahuete[10] (‖ persona que concierta una relación amorosa)» [http://lema.rae.es/drae/]

Unha curiosidade xeográfica

Continuando coa esixencia de buscar a transversalidade, invadamos un campo que require coñecementos de matemáticas.[11] Nos billetes, cales son as illas que aparecen nos recadros do bordo inferior do reverso, á beira de EYPΩ (as letras gregas para EURO)? A resposta é: os territorios ultramarinos dos estados membros da eurozona. Así están debuxados os Departamentos franceses de ultramar: **Guaiana** francesa (capital Cayena, entre Brasil e Surinam, cuxos bordos marítimos no debuxo dos billetes aparentan os cornos dun touro; non confundir con Guaiana británica); as illas caribeñas **Guadalupe** (Basse-Terre) e **Martinica** (Fort-de-France); a do océano Índico, **Reunión** (Saint-Denis). [A partir do 1 de xaneiro de 2014, será

Departamento tamén Mayotte (Mamoudzou) no Índico, aínda que só son 374 km^2]. Ollo, ademais destes Departamentos, Francia ten "colectividades de ultramar": no Pacífico, Nova Caledonia (Numea), Polinesia Francesa (Papeete) e Wallis e Futuna (Mata-Utu); no Atlántico Norte, Saint-Pierre-et-Miquelon (Saint-Pierre) e as caribeñas, San Martín (Marigot) e San Bartolomé (Gustavia).



Como o tamaño mínimo para debuxar un territorio foi fixado en 400 km^2, nas illas **Canarias** faltan nos billetes El Hierro (278 km^2) e La Gomera (369,8 km^2), do mesmo xeito que nas Baleares non se debuxan Formentera (83,24 km^2) e Cabrera (15,69 km^2). Pero si aparecen nos billetes as Rexións Autónomas portuguesas, **Azores** e **Madeira**, representadas no Atlántico, á beira dunha da media ducia das estrelas brancas de cinco puntas. Sorpréndenos esa representación pois aparenta unha latitude moi alta, aínda que en realidade Azores está nunha latitude inferior a Madrid, e a latitude de Madeira, aínda que menor que a de Tarifa, é maior que a do arquipélago canario. A pesar de que Chipre e Malta se integraron na eurozona en 2008, non aparecen nos billetes, por pequena, Malta (316 km^2) e por non entrar no mapa, ao ser tan oriental, Chipre (9.250 km^2)[12].

Murphyx

Como xa se dixo antes, a "proba do nove" é a base do pasatempo *Murphyx* que aparecía na revista da compañía Iberia e agora é un xogo de mesa e en rede (www.murphyx.com). O sorprendente é que ten unha solución aritmética moi sinxela que, unha vez coñecida, converte cada reto nun cálculo elemental.

Unha descrición do ano 2008 dicía «*Murphyx*, es un juego de números, que desarrolla el potencial aritmético y el intelecto desde la primera partida. Este juego estimula la capacidad de calculo, memoria y rapidez. Es un poco difícil empezar a jugarlo, pero cuando le agarras la mano a unas operaciones aritméticas de ayuda (el metodo del 9), se hace mucho mas fácil. Viene en dos idiomas (ingles y español) y muy pronto saldrá a la venta como juego de mesa.» Nas instrucións explícase que temos fichas de dúas caras cos números do 1 ao 8, de modo que a suma de ambas as caras dunha ficha é sempre 9; e o obxectivo do xogo é lograr que a "redución a unha cifra" do número que presentan as fichas sexa unha cifra dada, o *nix*, volteando as fichas que sexa necesario para iso.

Analizando o problema, vemos que os cambios admisibles corresponden a un cambio de signo na aritmética modulo 9 [exemplo, voltear a ficha **1**|**8**, significa cambiar de 1 a $8 \equiv -1 \pmod 9$]. Así, podemos enunciar o problema doutro xeito: "Dadas cifras $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8$, determinar cal (ou cales) deben cambiar de signo para que a suma de todas elas módulo 9 sexa un valor dado *nix*." Supondo que só se precisará un

cambio de signo, pode reformularse como: "Se $a_1 + a_2 \ldots - a_i \ldots + a_8 \equiv nix \pmod 9$, cal é i?" A solución obtense, desa ecuación, restando a ambos os membros $sum = a_1 + a_2 \ldots + a_i \ldots + a_8$, a suma de todas as cifras, pois ocorre que $a_1 + a_2 \ldots - a_i \ldots + a_8 - sum \equiv nix - sum \pmod 9$, que é $-2a_i \equiv nix - sum \pmod 9$, e de aí $a_i \equiv 5\ (sum - nix) \pmod 9$. O cal nos permite identificar a ficha que hai que voltear; e o argumento tamén serve para o caso de que haxa que voltear dúas ou máis fichas, que serán as que sumen a devandita cantidade $5\ (sum - nix)$. E iso é todo o segredo do xogo, que foi obxecto dun taller nas *IX Jornades d'Educació Matemàtica da Societat d'Educació Matemàtica Al-Khwarizmi* da Comunidade Valenciana [Javier Muñoz Andújar[13], *Murphyx (el juego del 9) aplicado al aula de matemáticas*, 3/9/2010], descrito como «unha forma divertida para os alumnos de familiarizarse coa técnica de comprobación aritmética do esquecido "método do nove", conseguindo unha gran rapidez na comprobación de operacións e como resultado un aforro de tempo nos exames de matemáticas» (tamén a propaganda como xogo de mesa asevera «Ayuda a los niños a desarrollar su 'potencial aritmético". Novedad mundial, Feria del Juguete de Nuremberg 2010»).

NIF

O método de verificación dos billetes de euro segue os métodos de detección e corrección de erros, utilizando métodos de aritmética modular e díxitos de control, que se empregan en moitos ámbitos. Así o Real Decreto 1245/1985, de 17 de xullo, estableceu no seu Artigo 6.2, «al número del Documento Nacional de Identidad, sin modificación alguna, seguirá el correspondiente código de verificación, que será una letra mayúscula.» En consecuencia desde o 28 de xullo de 1985 levamos, incorporado ao número individual de identificación que se consigna no DNI[14], unha forma de verificar a súa validez. Ocorría que Facenda detectaba que, ao consignar o número do DNI en documentos e facturas, producíanse moitas "equivocacións" (principalmente transposición de dous díxitos contiguos), polo cal creou o NIF (acrónimo de "número de identificación fiscal"). O cálculo desa letra de control emprega o número primo 23 e unha permutación de letras do alfabeto (que foi coñecida moi pronto, e que era deducible dunha listaxe, como a de votantes). Aínda que sexa unha suposición persoal, case seguro que 23 xurdiu ao suprimir do abecedario as letras que poderían inducir a confusión (I por 1, O por 0, U por V) e a permutación só trataba de escurecer a asignación da letra. En notación de Mathematica© a función escríbese así:

$$\text{letraNIF[DNI\_]} := \{T, R, W, A, G, M, Y, F, P, D, X, B, N, J, Z, S, Q, V, H, L, C, K, E\}[[\text{Mod[DNI}, 23] + 1]]$$

isto é, da listaxe fixada extraer a letra que ocupa o posto que corresponde ao resto de dividir o número do DNI por 23 (nese sistema de computación simbólica as listas numéranse desde 1). Tan ben debeu de funcionar o NIF, que vinte anos despois da súa creación, o Consello de Ministros do 4 de febreiro de 2005, no Plan de Prevención da Fraude Fiscal, determinou que o NIF do arrendador debe ser consignado na declaración da renda dun inquilino; ademais volve definir a ONIF, a Oficina Nacional de Investigación da Fraude. Pero necesitan todos, xornalistas e políticos, un mínimo de coñecemento do NIF que evite afirmacións do tipo «99999999-R es un DNI ficticio»[15] cando só se precisa unha calculadora para verificar que 1= Mod[99.999.999, 23].

O número primo 23 foi unha boa elección: próbase facilmente que o NIF detecta todos os cambios dunha cifra do DNI e todas as transposicións de dúas cifras do DNI. En efecto, se se intercambian dúas cifras consecutivas x e z dun DNI, só se mantén o mesmo NIF se ambas son iguais pois para que $a_1 a_2 \ldots x\ z \ldots a_8$ e $a_1 a_2 \ldots z\ x \ldots a_8$ compartan o mesmo NIF, debe cumprirse:

$10^i(10x + z) – 10^i(10z + x) \equiv 0 \pmod{23}$, isto é, $10^i 9(x – z) \equiv 0 \pmod{23}$, e iso só se $x = z$

Con todo, o NIF non detecta[16] outros cambios de cifras do DNI, como moitos cambios de tres cifras, mesmo cando se trata dunha permutación circular de tres consecutivas.

Dorso do DNI

O descoñecemento destes mecanismos de verificación de códigos creou lendas urbanas como a que asegura que o último número que aparece na segunda fila de caracteres OCR-B para lectura mecanizada no dorso do documento do DNI corresponde ao número de persoas cos mesmos apelidos que se consignan na terceira fila. En realidade é un díxito de control segundo un algoritmo magnificamente exposto en http://josep-portella.com/es/escritos/desmitificando-los-numeros-del-dni/

No exemplo de imaxe de documento de DNI detéctanse algunhas diferenzas cun real: o campo aí rotulado DESP e con contido AAA-000000, nun verdadeiro documento vai marcado como IDESP e son tres letras adxuntas a seis díxitos o «número de serie do soporte físico do cartón»; no espazo da imaxe láser cambiante (CLI, *Changeable Laser Image*) o que debe aparecer é a data de expedición en formato **ddmmaa** (e noso usual formato de datas) e un acrónimo persoal de tres consoantes, a primeira de cada apelido e a do primeiro nome [moitos máis detalles poden consultarse na páxina oficial do DNI electrónico, en vigor desde 2006, [http://www.dnielectronico.es/Asi_es_el_dni_electronico/descripcion.html]

Aínda que se trata dun simple feito burocrático, non deixa de ser sorprendente a data de caducidade consignada no DNI permanente, o dispoñible para todos os que cumpriron 70 anos e para grandes inválidos maiores de trinta anos. Baixo o texto "Válido hasta", aparece escrito 01 01 9999 que, como data, é moi afastada[17] pero corresponde ao venres en que se abre a Porta Santa para o último Ano Santo Compostelán do noveno milenio[18].

Número do cartón de crédito

O número dos cartóns de crédito é 16 díxitos, divididos en grupos de catro, onde o último díxito é un díxito de control que permite detectar algúns erros. É fácil o cálculo dese díxito: o primeiro díxito á esquerda multiplícase por 2; o seguinte por 1, e así sucesivamente. Obtida a suma de todos eses díxitos, incluídos os 1 que eventualmente poidan xurdir na duplicación das cifras en posto impar, calcúlase o "complemento módulo 10" (o que falta ata o seguinte múltiplo de 10, isto é, o oposto módulo 10 desa suma) que será o díxito de control empregado. O algoritmo[19] foi deseñado polo científico de IBM Hans Peter Luhn e descrito na patente U.S. Patent 2,950,048 solicitada o 6 de xaneiro de 1954 e concedida o 23 de agosto de 1960. Detecta o 100 % dos erros nunha soa cifra e o 97,77 % das transposicións adxacentes (non detecta o cambio de 09 por 90), pero non descobre outros erros comúns, como unha transposición non adxacente do tipo cambiar *abc* por *cba*.

Este algoritmo é o empregado no código chamado CIF (código de identificación fiscal) para determinar o seu díxito de control[20], que precisamente é a letra que na orde alfabética ocupa o posto que corresponde ao díxito de control de Luhn (se este fose 0 usaríase a 10ª letra, un J). Tamén no código ISIN (*International Securities Identification Numbering System*), que serve para identificar de forma unívoca un valor mobiliario a nivel internacional, o último dos 12 caracteres alfanuméricos é un díxito de control calculado polo algoritmo

de Luhn; cada unha das letras que aparezan, incluídas as dúas primeiras que identifican o país segundo a norma ISO 3166, transfórmase en dous díxitos (sumando 9 á posición da letra na orde alfabética; así A convértese en 10, B en 11,..., Z en 35). Trátase talvez do primeiro código cuxo cálculo do díxito de control está especificado no BOE[21], incluíndo exemplos de como se calcula.

CCC e agora IBAN

As contas bancarias identifícanse polo Código Conta Cliente (C.C.C.), recomendado polo Consello Superior Bancario (17/12/1989) e a CECA (Confederación Española de Caixas de Aforro). É o código que estamos acostumados a utilizar nas relacións cos bancos, formado por 4 cifras que identifican a entidade, 4 para a sucursal, dúas rotuladas D.C. (díxitos de control) e 10 para o número de conta. Cada un dos díxitos de control (o primeiro verifica os 8 díxitos entidade-sucursal e o segundo, os 10 da conta) é, en aritmética módulo 11, o produto escalar do vector de díxitos por un vector de pesos que é a progresión xeométrica de razón 2 que comeza en 7 e en 10, respectivamente. Por mor desa definición, os campos deben ser completados sempre con ceros á esquerda; ademais, se o díxito de control vale 10 substituirase por 1, o cal é un erro de deseño que diminúe a eficacia do código. Outro erro de deseño é que o intercambio do segundo díxito de control e o primeiro díxito do número de conta resulta ser tamén un código válido, outra transposición que non detecta o protocolo C.C.C.

Ultimamente fálase do código IBAN (*International Bank Account Number*) deseñado para os pagos transfronteirizos pois facilita a validación de números de conta estranxeiras. O IBAN segundo a norma ISO 13616 de 1997, consiste en antepor información adicional ao formato de número da conta de cada país. Comeza co código de dúas letras do país, ES no caso de España, seguido polos dous díxitos de control e os 20 díxitos do C.C.C. (un total de 24 caracteres alfanuméricos). Os díxitos de control son 98 - Mod[CCC142800, 97], a diferenza entre 98 e o resto módulo 97 do gran número formado polo C.C.C. seguido de 14 (por E), 28 (por S) e dous ceros; se o resto é menor que 10, o primeiro díxito de control é un 0.

A única dificultade é o cálculo do resto módulo 97 dun enteiro de 26 cifras, que non pode ser realizado nunha calculadora ou directamente nunha folla de cálculo[22], pero si pode facerse cun elemental proceso recursivo (de fácil implementación nunha folla de cálculo). Usando dúas cifras cada vez, dado que Mod[100, 97] = 3 e mediante un esquema de Horner, o par de díxitos de control DC calcúlase así:

$$\text{DC} = (a_1\, a_2);\ \text{DC} := \text{Mod}[\text{DC*3} + (a_{2i+1}\, a_{2i+2}), 97],\ \text{para } i = 1, ..., 12;\ \text{DC} := 98 - \text{DC}$$

Por exemplo[23], para a conta en formato C.C.C. 2310-0001-18-0000012345, as operacións son:

DC = 23; DC := Mod[23* 3 + 10, 97] = 79; DC := Mod[79* 3 + 00, 97] = 43;

DC := Mod[43* 3 + 01, 97] = 33; DC := Mod[33* 3 + 18, 97] = 20;

DC := Mod[20* 3 + 00, 97] = 60; DC := Mod[60* 3 + 00, 97] = 83;

DC := Mod[83* 3 + 01, 97] = 56; DC := Mod[56* 3 + 23, 97] = 94;

DC := Mod[94* 3 + 45, 97] = 36; DC := Mod[36* 3 + 14, 97] = 25;

DC := Mod[25* 3 + 28, 97] = 6; DC := Mod[6* 3 + 00, 97] = 18 ; DC = 98 - 18 = 80

co cal o IBAN correspondente[24] resulta ser ES80 2310 0001 1800 0001 2345.

JOSÉ MARÍA BARJA PÉREZ

Barras que informan

Unha das vantaxes do invento de Joseph Woodland[25], os códigos de barras, é que simplemente fixándose nos dous ou tres primeiros díxitos dos códigos antes chamados EAN-13 e agora GTIN-13 (*Global Trade Item Number*), descubrimos os países que etiquetan os produtos que compramos. O 13º díxito que aparece na "liña de interpretación" do símbolo é un díxito de control deste. Para calculalo súmanse en aritmética módulo 10 os díxitos das posicións pares, cantidade que se multiplica por 3 e á que se engade a suma dos díxitos en posición impar. Se o resultado é 0, o 13º díxito tamén será 0, mentres que nos demais casos será a súa diferenza a 10 (o seu oposto en aritmética módulo 10). Talvez polo seu carácter de lectura mecánica, este modelo de díxito de control non é unha marabilla de deseño, pois apenas detecta os erros dun díxito, pero pode ser útil.

No suplemento Magazine do 9 de decembro de 2012 apareceu como ilustración unha tesoira cortando un código de barras. Cóntanse ben as 30 barras e aparecen 12 dos 13 díxitos dun EAN. Como o díxito de control 6 coincide coa súa correcta codificación nas barras, sabemos que o único que falta é o primeiro díxito. Ese díxito x para este exemplo calcúlase resolvendo a ecuación $x + 69 \equiv -6 \pmod{10}$; así obtense que x é un 5, o cal indica que o produto é do Reino Unido (50 é o seu prefixo). Realizando a procura do devandito código en `www.ean-search.org` salta a sorpresa: é un produto comercial chamado *Carob*[26] *Powder* que resulta ser "vainas de algarroba tostadas", presentado como un substituto do chocolate.

Incluso algúns billetes de aparcadoiro, con código de barras para lectura óptica, poden ser "descifrados". Aínda que no billete do aparcadoiro adoitan aparecer só as barras, sen a liña de interpretación, determinala é un exercicio escolar (como propuña, xa en 2005, Goyo Lekuona aos alumnos de terceiro e cuarto de ESO, seguindo *O método Lekuona: matemáticas con follas de cálculo*). E nalgúns casos xorde a sorpresa: aínda que é un correcto código de almacén (como marca o prefixo 20 e verifica o díxito de control) a información que contén é número do mes, do día e a hora de saída, cunha marxe de 10 minutos. Nada estraño, pero sen dúbida demasiado fácil.

Estes exemplos de álxebra e matemática discreta mostran cales son as matemáticas aplicadas na informática, e no día a día. E non é precisamente "o regreso ao ábaco"[27] o que mellorará as capacidades dos nosos estudantes de secundaria, pois ata os "campeóns mundiais de cálculo" deben comprender cómo se executa un algoritmo recursivo para facer o cálculo do IBAN, dados os límites de tamaño dos números que esa antiga ferramenta pode manexar.

Referencias bibliográficas

[1] P. Bayer Isant, *¿Para qué sirven hoy los números?*, Real Academia de Ciencias, http://www.rac.es/ficheros/doc/00355.pdf

[2] J. Beato Sirvent, "Códigos numéricos para la vida", *Suma*, nº 57 (febreiro 2008), páxs. 43-54.

[3] D. de Guadix, *Recopilación de algunos nombres arábigos (1593)[Dicionario de Arabismos, ed. Mª Agueda Moreno Moreno]*, Universidad Jaen, 2007.

[4] G. Ifrah, *Historia Universal de las Cifras. La Inteligencia de la Humanidad Contada por los Números y el Cálculo*, Editorial Espasa-Calpe, 1997.

Notas

[1] Nada menos que Michel Eyquem (señor de) Montaigne aseguraba en 1575, no libro II dos seus *Essais*, *«Je ne sçai compter ny a get nin a plume»* (non sei contar nin con fichas nin coa pluma) (en [4] páx. 1331, resáltase que se trataba dun home culto e viaxado con ampla biblioteca).

[2] A letra é asignada en orde decrecente (por iso se inicia en Z) atribuíndoa aos estados membros da Unión Europea antes da entrada en vigor do euro, segundo a orde alfabética do nome na súa lingua oficial (België/Belgique/Belgien, Danmark, Deutschland, Ellada, España, France, Ireland/Éire, Italia, Luxembourg/Luxemburg/Lëtzebuerg, Nederland, Österreich, Portugal, Suomi/Finland, Sverige, United Kingdom). As posicións de Dinamarca e Grecia foron intercambiadas, posto que o Y se parece á letra *ipsilón* do alfabeto grego, mentres que nese alfabeto non está o W. Foi reservada a letra mesmo aos que non adoptaron o euro, como Dinamarca, Reino Unido e Suecia, e tamén Luxemburgo que non emite billetes propios. A asignación seguiu para os que entraron no euro despois de 2002, incluído Estonia que comezou a imprimir en 2012.
Outro código moito menos evidente aparece na cara dos billetes case escondido (ocasionalmente nunha das estrelas). Neste caso a primeira letra do código dá a referencia do impresor. Nos billetes de España aparece **M** para indicar a Fábrica Nacional de Moeda e Timbre española; pero tamén **G** por *Koninklijke Joh. Enschedé* en Haarlem, Paises Baixos, **P** por *Giesecke & Devrient* en Munich, Alemaña, e **T** polo Banco Nacional de Bélxica en Bruxelas.

[3] Mellora amplamente a actual 13ª acepción de *prueba* na 22ª edición do DRAE, que se vai manter tamén: «Operación que se ejecuta para comprobar que otra ya hecha es correcta».

[4] Na numeración da nova versión dos billetes, a serie Europa, ademais da letra inicial que identifica ao país emisor, engadiu outra, sen ningún significado particular, só para ter números de serie. A verificación precisa agora transformar esa segunda letra no número de orde alfabética máis un. Por exemplo, para o billete belga con código ZB0200851269, ten que converter o Z en 26 (o número de orde alfabética); o B, en 3 (un máis que o seu número na orde alfabética) e, xa que 263 é "reducido" a 2, verificar que os dez números son "reducidos" a 6, para que todo o código de numeración do billete sexa "reducido" a 8. Como pola súa banda 1269 son "noves" e 020085 "se reduce" a 15 e este a 6, facilmente alcanzamos a comprobación da súa validez.

[5] Precisamente na 23ª edición do DRAE incluirase como segunda acepción de *prueba del nueve* «prueba clara que confirma la verdad o falsedad de una cuestión debatida».

[6] Aínda que nalgunhas referencias aparece que a cifra cero en chinés é 〇 (ou ben,零), non se emprega na representación de números de moitas cifras, así e todo empregan caracteres adicionais para representar decenas (十), centenas (百), milleiros (千), decenas de mil (万),... complexidade que indica que o ábaco é usado para realizar operacións (por exemplo o número 147.238 escríbese 十四万七千二百三十八).

[7] A tradución de Gerardo de Cremona titúlase *Liber Maumeti filii Moysi Alchoarismi de algebra et almuchabala*, o que mostra o termo matemático álxebra e nomea a Mohamed, fillo de Moisés (e pai de Ja'far) do Jorezm. Outra das traducións é atribuída a Robert de Chester, en Segovia, como parte da Escola de Tradutores de Toledo no ano 1145, como *Liber algebra et almuchabala*.

[8] En [3] páx. 69, tras expor que **álgebra** «llaman en España a 'cierta arte o sciencia de concertar huesos desconcertados'. [...] En Italia lo llaman: *aconchatori de ossi*, que —en italiano— significa 'concertador de huesos'», dáse como segunda acepción: «También llaman en España y en Italia a 'cierta regla o reglas de aritmética'. Es la misma algarabía y significa lo mesmo que acabo de dezir (combiene a saber) 'hallar o restituir cierta qüenta con número perfecto y verdadero'».

[9] En [4] páx. 1289 explícase polo miúdo que por hisāb al ghubār, "cálculo sobre el polvo", empregábanse as cifras arábigas no norte de África, o cal sería transmitido á Península Ibérica. Sen querer entrar en discusións etimolóxicas coa RAE, parece máis acertado derivar *algoritmo* das sucesivas deformacións do xentilicio Al Khuwarizmī.
Outra fonte de confusión é a proximidade fonética co termo *logaritmo* (do grego λόγος, razón, e αριθμός, número) termo creado por John Napier en 1614, no seu libro titulado *Mirifici Logarithmorum Canonis Descriptio*, derivado literalmente de describilo no seu «teorema fundamental» como «un número que indica unha relación ou proporción». Refírese a que a diferenza de dous logaritmos determina a relación dos números aos cales corresponden, de maneira que unha progresión aritmética de logaritmos corresponde a unha progresión xeométrica de números. As constantes erratas mediáticas, ao intercambiar algoritmo e logaritmo, talvez poderán chegar a desaparecer se na clase de matemáticas achegamos este tipo de información filolóxica aos xornalistas do futuro.

[10]Hai citas de escritores que xustifican que a RAE manteña esta terceira acepción: Quevedo describindo á nai do *Buscón, llamado don Pablos* como «algebrista de voluntades desconcertadas, [...] y por mal nombre alcagüeta»; Alonso de Castillo Solórzano no poema I.42 de *Donaires del Parnaso* alcuma a unha vella alcaiota, que actuou como mediadora nos amores entre Xúpiter e Dánae, de «algebrista de amores, que juntas voluntades separadas ...»

[11]Saber a medida en km^2 dalgún lugar coñecido evitaría describir a Cidade da Cultura como «un espacio de unos 148.000 kilómetros cuadrados» [*El delirio interrumpido*, El País, 29/3/ 2013], sen ser consciente de que esa cantidade corresponde a cinco veces a superficie de toda Galicia, en lugar de referirse a 14, 18 hectáreas.

[12]Na serie Europa foron incluídas no mapa tanto Malta coma Chipre, que se adheriron á UE despois de 2002. Dada a pequena dimensión de Malta (as illas habitadas de Malta, Gozo e Comino), a súa representación son dous puntiños por baixo da illa de Sicilia, sobrepostas nunha das estrelas do escudo en Europa. Criamos que Chipre ía no mapa anterior, ao confundir a maior illa grega, Creta (a súa capital Heraklion, chamada Candia ata principios do século pasado, ten 173.450 habitantes), coa illa, máis ao leste, que deu nome ao cobre, Chipre (cuxa capital, Nicosia, ten 47.832 habitantes).

[13]O centro virtual de divulgación das matemáticas da RSME (http://www.divulgamat.net) reproduce unha noticia de La Vanguardia 16/9/2011, *Un valenciano gana el premio 'Juego del Año' que concede una empresa inglesa por su creación 'Murphyx'*. Refire que Javier Muñoz xa gañara o premio Feira Valencia del Salón de Inventores Geniápolis 2004 e que a idea do xogo lle xurdiu falando cuns amigos ningún dos cales coñecía 'a proba do 9' que «se suprimió del sistema educativo español sobre mediados de los años 70 con la aparición de la calculadora y ahora los niños, cuando tienen que comprobar una operación aritmética, la tienen que hacer de nuevo con la consiguiente pérdida de tiempo en los exámenes de matemáticas».

[14]A existencia do DNI hoxe apenas é cuestionada. Di o Decreto 196/1976 (BOE 13/2/1976) asinado polo entón ministro da Gobernación, Manuel Fraga Iribarne: «Creado el documento nacional de identidad por Decreto de 2 de marzo de 1944, ha venido cumpliendo las misiones que le fueron asignadas como documento de identificación con eficacia plena en la acreditación de la personalidad individual.» Hai que subliñar que esa data de creación do DNI, 2/3/1944, é anterior en tres meses ao desembarco de Normandía e case un ano anterior a coñecerse publicamente os horrores dos campos de concentración, con prisioneiros identificados con números gravados na pel. No mundo futuro imaxinado polo inventor do termo ciberespazo William Gibson [*Mona Lisa Overdrive* (1988)], todos os habitantes do planeta teñen asignado un número individual SIN (*single identification number*); isto é, o pecado orixinal converteuse nun feito administrativo.

[15]«El DNI 99999999-R, que es ficticio, fue asignado a una de las personas que aparecen en las listas de adjudicatarios de las viviendas sociales de la Xunta en Novo Mesoiro y Eirís. El número, tal y como publicó ayer La Opinión, fue elaborado mediante un generador de DNI, un programa informático muy conocido entre los funcionarios, algo que niegan el delegado provincial de la Consellería de Vivenda e Solo y el concejal de Rehabilitación Urbana y Vivienda [quienes] aseguraron ayer, después de leer la información pública por este diario, que la R significa revisar. [...] El delegado de la Consellería aseguró desconocer la existencia de un generador de carnés de identidad. En las listas figuran más personas cuyo DNI existe y termina en R, pero sólo hicieron referencia a la R que acompañaba al número 99999999» [*Un DNI ficticio con R de "revisar"*, La Opinión, 5/4/2008]. Incluso o exemplo de DNI que adoita aparecer nos medios (reproducido arriba) leva ese NIF que sería o último en ser asignado co actual formato de 8 díxitos.

[16]O Número de Rexistro Persoal dos funcionarios españois, que son os dous díxitos resultantes de engadir 2 ao produto de 11 polo resto de dividir o número do seu DNI por 7, deseñado por algunha "prodixiosa" mente burocrática, non detecta nin un só erro, contrariamente ao NIF.

[17]A distancia de sete milenios é tan desmesurada que, nin comparando coas máis antigas civilizacións, somos conscientes da súa lonxitude. Segundo os exiptólogos, Keops comezou a reinar en 2589 a.C.. Teríamos que multiplicar por 1,73 o número de días entre hoxe e ese ano para alcanzar os 2.916.783 días que cara a diante separan a data de hoxe e a moi afastada impresa no DNI. Só Frank Herbert na súa saga *Dune*, imaxina un futuro a máis de 20.000 anos, iso si, como un gran imperio galáctico de estrutura feudal.

[18]Desde 2013 ata o 9999 incluído, haberá 1.117 Anos Santos Compostelláns (en cada ciclo de 400 anos hai 56). Aínda que para entón posiblemente se terá perfeccionado a regra gregoriana dos bisestos, fixando que os múltiplos de 4.000 **non o sexan**, manterase ese número porque a usual secuencia **6-5-6-11** (1993–1999–2004–2010–2021) alterarase ao pasar polo 4000 e 8000 en 6-**6**-6-**10** (3993–3999–4005–4011–4021; 7993–7999–8005–8011–8021).

[19]Este algoritmo é un dos explicados en [2], aínda que erroneamente o chama Codabar, que á súa vez é un tipo de código de barras. Curta, pero moi informativa, é a entrada do blog *Money, Matter, and More Musings* co explícito, e ao tempo coidadoso título, *How to generate *Valid* Credit Card Numbers*, http://www.thetaoofmakingmoney.com/2007/04/12/324.html

[20]O Artigo 3.4 do Decreto 2423/1975, publicado no BOE do 25 de outubro de 1975, só di «Dígito de control». Esta era a norma que rexeu o sistema de identificación de persoas xurídicas ou entidades ata o 1 de xaneiro de 2008, cando entra en vigor o Real Decreto 1065/2007, de 27 de xullo, en cuxo Artigo 22.1.c precísase que o «número de identificación fiscal de las personas jurídicas y entidades sin personalidad jurídica» inclúe «un carácter de control». Na Orde EHA/451/2008, de 20 de febreiro, «regula la composición del número de identificación fiscal de las personas jurídicas y entidades sin personalidad jurídica», precisando que estará formado por «a) Una letra, que informará sobre la forma jurídica, si se trata de una entidad española, o, en su caso, el carácter de entidad extranjera o de establecimiento permanente de una entidad no residente en España; b) Un número aleatorio de siete dígitos; c) Un carácter de control.» Non se explicita cómo se calcula o carácter de control, pero, en cambio, dedica os Artigos 3, 4 e 5 a detallar a letra que encabeza ese código que seguimos chamando CIF. En particular, empezan por N as entidades estranxeiras; por W, as permanentes non residentes en territorio español; ademais separa a antiga asignación de Q a «Organismos Autónomos, estatales o no, y asimilados, y Congregacionales e Instituciones Religiosas», en Q para os «organismos públicos» e R para as «congregaciones e instituciones religiosas».

[21] O 30 de setembro de 2010 a Comisión Nacional del Mercado de Valores publica no BOE a súa «Norma técnica 1/2010, de 28 de julio» expondo a «codificación de valores negociables y otros instrumentos de naturaleza financiera, sobre estructura de los códigos.» No artigo segundo apartado C descríbese en catro pasos o cálculo da «cifra de control», indicando que «en anexo se incluyen ejemplos aclaratorios de la aplicación de esta fórmula.» Nun anuncio de Santander Dividendo Elección (El País, 12/4/2013) aparece un código ISIN: ES0113900J37. O díxito de control, a última cifra **7**, sae das cifras (E, S, J substituíronse por 14, 28 e 19) 14280113900193 facendo o cálculo $-(8+1+6+2+6+0+2+6)-(1+2+0+1+9+0+9) \equiv -(31+22) \equiv \mathbf{7} \pmod{10}$

[22] A proposta de empregar o algoritmo da división con lapis e papel (aínda que se esqueceron da súa verificación coa "proba do nove") é o que se lle ocorreu a un presunto "Master en Banca y Finanzas (Online)" [http://www.finanzasybanca.com/iberfinanzas/index.php/C/Codigo-Internacional-de-Cuenta-Bancaria-IBAN.html]

[23] Na páxina web http://es.ibancalculator.com/ calcúlase o IBAN para códigos C.C.C. correctos e valídanse ambos. Ademais tamén proporciona a identificación dunha entidade bancaria segundo o ISO 9362, o BIC (Código Identificador de Banco), tamén chamado SWIFT (The Society for Worldwide Interbank Financial Telecomunications) pola entidade que xestiona estes códigos. Está formado por 4 caracteres que identifican a institución financeira a nivel mundial, 2 caracteres que identifican o país, 2 caracteres da cidade de localización da unidade central da entidade e, opcionalmente, 3 caracteres que identifican unha oficina (por defecto XXX refírese á principal). Por exemplo, o código SWIFT principal do Banco Santander é BSCHESMM, por ser español (ES) e con sede en Madrid (MM).

[24] Se se usan **6** díxitos de cada vez, como Mod[1 000 000, 97] = 27 e Mod[142 800, 97] = 16, o cómputo dese IBAN sería: Mod[**23*** 27 + **100 001**, 97] = 33; Mod[33* 27 + **180 000**, 97] = 83; Mod[83* 27 + **012345**, 97]= 36; 98 - Mod[36* 27 + 16, 97] = **80**

[25] O deseño do código de barras basicamente débese a Norman Joseph Woodland (falecido o pasado 9 de decembro de 2012 aos 91 anos), quen tivo que esperar ao desenvolvemento de lectores apropiados e á mellora dos sistemas de impresión (a tecnoloxía láser). A súa idea patentada en 1952 aínda que caducou, foi reutilizada por IBM, empresa para a que traballaba; usouse por primeira vez na venda dun paquete de chicle nun supermercado da cadea *Marsh* en Troy, Ohio, en 1974. En España a primeira venda así foi un estropallo da firma 3M, o 3 de outubro de 1977 no supermercado Mercadona en Valencia. No símbolo máis usado 13 díxitos aparecen codificados como 30 barras (incluídos os separadores de inicio, final e centro) e 29 espazos; para que non importe a dirección de lectura, a codificación é diferente nas partes esquerda e dereita do símbolo. Usualmente os 3 primeiros díxitos codifican o país; os díxitos 4º ao 7º, o fabricante (ata 10.000); os 8º ao 12º, o produto (ata 100.000) sendo o 13º o díxito de control.

[26] Segundo o DRAE, **algarroba** procede do árabe hispánico *alharrúba*, do árabe clásico *harrūbah* ou *harnūbah*, do persa *har lup* 'quijada de burro', froito do *algarrobo* [primeira aparición en castelán en 1269]; e defíneo como «una vaina azucarada y comestible, de color castaño por fuera y amarillenta por dentro, con semillas muy duras, y la cual se da como alimento al ganado de labor».

[27] «Las matemáticas son hoy, más que nunca, una herramienta básica para desenvolverse en un mundo revolucionado por las nuevas tecnologías [...] se comprende el creciente interés que los métodos didácticos orientales están despertando en España. Sus sistemas de cálculo (ábaco incluido) agilizan la mente y desarrollan los dos lados del cerebro.» [*De regreso al ábaco. La pedagogía de las matemáticas en España sigue ofreciendo resultados mediocres*, El País, 7/4/2013]; «Realizan sumas, restas, multiplicaciones y divisiones de hasta 17 dígitos y pueden recitar la tabla de multiplicar de cualquier número de dos dígitos, así como descubrir cuál fue el día del nacimiento de cualquier persona.» [*Las cuentas que vienen del pasado. Los hermanos Ronit y Samir Motwani, campeones del mundo de cálculo, demuestran sus habilidades en A Coruña*, La Opinión, 6/4/2013]

JOSÉ MARÍA BARJA PÉREZ
Facultade de Informática, UDC
<j.m.barja@udc.es>