Códigos detectores y correctores de errores
¿Tienen lugar en la escuela?

Omar Gil | Doctor en Matemática por la Universidad Autónoma de Madrid (1996). Prof. Agregado (Gr. 4) del Instituto de Matemática y Estadística de la Facultad de Ingeniería (UdelaR). Investigador del programa PEDECIBA. Autor de diversos artículos de investigación, de divulgación y periodísticos, y de varios libros.

Beatriz Rodríguez Rava | Maestra y Lic. en Ciencias de la Educación. Especialista e Investigadora en Didáctica de la Matemática. Coordinadora del Equipo de Investigación en Didáctica de la Matemática de la Revista *QUEHACER EDUCATIVO*. Autora de numerosos artículos de Didáctica de la Matemática.

1. Protección contra errores y teoría de la información

La protección automática de la información contra errores en su transmisión y reproducción está presente en muchos aspectos de nuestra vida cotidiana. La mayor parte de las veces no reparamos en ello, justamente porque estos procedimientos tienen éxito en asegurar la buena calidad de nuestras comunicaciones, tanto cuando trasmitimos información a través del espacio, por ejemplo, al bajar archivos de internet o hablar por un teléfono móvil, como cuando lo hacemos a través del tiempo, almacenando registros que se leerán más tarde. Por ejemplo, los números de nuestros documentos de identidad, de nuestras cuentas corrientes y tarjetas de crédito incorporan estas técnicas; también todos los sistemas de comunicaciones y los lectores de discos compactos y DVD.

Es bastante conocido el hecho de que buena parte de la información que nuestra sociedad procesa es digital, y se representa en registros que son largas series de ceros y unos. La unidad mínima de estos registros es el bit, que puede tomar el valor uno o cero. Los bits se agrupan en listas más largas, o *bytes*[1]. A este nivel puede incorporarse el que es quizás el criterio más básico de protección contra errores: un control de paridad.

Control de paridad

Un *byte* es una lista de ocho ceros y unos. Por ejemplo:

(0 1 0 1 0 1 0 1), (1 1 0 1 1 1 0 0).

[1] «***byte.*** Su plural es *bytes*. Por tratarse de una unidad de medida de circulación internacional, se emplea normalmente como extranjerismo crudo, con su grafía y pronunciación originarias, aunque no debe olvidarse que el equivalente español de este anglicismo es *octeto* (...)» En esta nota seguiremos el uso habitual de emplear la palabra *byte*, en vez de octeto. El párrafo que citamos está tomado de la versión electrónica del Diccionario Panhispánico de Dudas (disponible en http://buscon.rae.es/dpdl/SrvltGUIBusDPD?lema=byte, consulta: 14 de marzo de 2012). El término "bit" ha sido incorporado al léxico del idioma español, por lo que no hacemos ninguna consideración especial sobre él.

Al almacenar la información en *bytes* podemos usar la convención de solo poner datos en los primeros siete lugares. Por ejemplo:

(0 1 1 0 1 0 0 _)

reservando el último para un ***carácter de control*** que se elige de modo tal que el número total de unos en el *byte* es par. Si adoptamos esta convención para nuestro ejemplo, tenemos que poner un uno en la última posición:

(0 1 1 0 1 0 0 1).

Esta codificación de la información permite detectar algunos errores. Por ejemplo, aceptaríamos como bueno el *byte*:

(1 0 1 0 1 1 1 1)

en tanto que advertiríamos que la información almacenada en:

(0 1 0 0 1 0 0 1)

ha sufrido algún tipo de corrupción. Todavía más, esta modesta codificación ya nos permite recuperar un dígito perdido. Si leemos el *byte*:

(0 1 1 0 **¿?** 0 0 1),

en el que hemos representado con **¿?** un carácter que accidentalmente se ha borrado, sabemos cómo completarlo. En el quinto lugar debe aparecer un uno para satisfacer el control de paridad. Se trata entonces de:

(0 1 1 0 1 0 0 1).

Aritmética módulo 2

Realizar un control de paridad implica una aritmética muy sencilla: solo hay que sumar los unos, y ver si el resultado final es par o impar. Lo que es equivalente a examinar el resto que arroja la suma al hacer la división entera entre dos, y ver si es igual a cero o a uno. Esta aritmética, en la que solo los restos de dividir entre dos nos interesan, se conoce con el nombre de ***aritmética módulo 2***, y apenas requiere los dos símbolos 0 y 1 para poder implementarse.

Es en realidad una aritmética conocida en la escuela. Está contenida en las reglas

Par más par, par,
par más impar, impar,
impar más impar, par.

Par por par, par,
par por impar, par,
impar por impar, impar.

Si identificamos par con cero, e impar con uno, los restos respectivos de dividir números pares e impares entre dos, esta aritmética se expresa en términos de los símbolos 0 y 1 a través de las siguientes reglas para la suma y el producto[2]:

$$0 + 0 = 0,$$
$$0 + 1 = 1,$$
$$1 + 1 = 0.$$

$$0 \times 0 = 0,$$
$$0 \times 1 = 0,$$
$$1 \times 1 = 1.$$

Son casi las reglas usuales, con la excepción de que ahora uno más uno es igual a cero. Es una aritmética adecuada para trabajar algebraicamente con dos símbolos, cero y uno, que se adapta bien al procesamiento de la información digital. Es posible incluso que en este momento nuestra civilización esté haciendo cada segundo más operaciones en las que uno más uno es igual a cero, que operaciones en las que uno más uno es igual a dos.

Sobre este punto puede ser interesante transcribir dos párrafos de Richard Hamming (1980b): *«en un libro que he escrito recientemente [Hamming, 1980a], los enteros se emplean como etiquetas, y los números reales son usados para las probabilidades; pero aparte de esto, toda la aritmética y el álgebra que aparece en el libro, y hay mucho de ambas, sigue la regla de que:*

1 + 1 = 0.»

[2] Para definir completamente la aritmética falta especificar que 1 + 0 = 1, y que 1 x 0 = 0. O declarar que las operaciones de suma y producto son conmutativas. No es habitual hacerlo en los años escolares, una época en la que damos por cierto que *"el orden de los factores no altera el producto"*. Afirmación falsa en muchas estructuras algebraicas no conmutativas.

En este texto, el autor, uno de los pioneros en el campo de las matemáticas de la detección y corrección automática de errores, se preocupa por entender por qué la Matemática es tan útil en dominios muy diversos. Como parte de su lista de explicaciones propone: *«seleccionamos la matemática para adaptarse a la situación, y simplemente no es cierto que la misma matemática funcione en cualquier lado»*[3].

Las matemáticas involucradas en la detección y corrección automática de errores tienen un nivel de dificultad que va desde la aritmética más elemental, como la que acabamos de exponer, hasta la existencia de una activa área de investigación en la que confluyen científicos con diferentes formaciones, fundamentalmente matemáticos e ingenieros. A continuación mostramos un ejemplo que requiere ideas algo más elaboradas, pero todavía manejables a nivel escolar.

ISBN (*International Statistical Book Number*)

La gran mayoría de los libros que consultamos, leemos, disfrutamos, amamos, detestamos o simplemente guardamos en nuestras bibliotecas están identificados con un número asignado a través de un Sistema Internacional de Numeración de Libros, llamado ISBN (sigla de *International Statistical Book Number*). ISBN es un sistema estandarizado, de alcance mundial, que permite asignar a cada publicación un número único[4]. Su desarrollo y difusión son relativamente recientes, mucho más modernos que los libros a los que se aplica. A mediados de los años sesenta comenzó a percibirse la necesidad de poseer un sistema eficiente de identificación de los libros, que asignara a cada publicación una etiqueta breve y fácil de manejar. En 1970 culminó el proceso de definición de un estándar con la aparición del ISBN: un número de identificación de nueve dígitos[5].

Como cualquier otra porción de información, un registro de ISBN puede estropearse, perderse, adulterarse, etc., al transmitirlo o almacenarlo. Por esa razón, el ISBN, al igual que

los números que identifican a los productos en el supermercado o los números de cédula de identidad, incorporó a su diseño un dígito de control. Hasta 2007 se utilizó un sistema al que es usual referirse como ISBN10, en que cada libro quedaba identificado por un número de diez dígitos, de los cuales los nueve primeros portan la información, y el décimo es un carácter de control.

Aunque no es nuestro principal objetivo describir esta parte del sistema ISBN10, digamos que los nueve dígitos que almacenan la información están divididos en tres campos. El primero corresponde al país, área geográfica o área lingüística, que participa en el sistema ISBN. El segundo identifica al editor dentro del grupo que corresponde al primer bloque, y el tercero a la publicación. Por ejemplo, para el primer campo, el número correspondiente a Uruguay es 9974. El de Estados Unidos es el 0, y el de España el 84.

Como todos los ISBN10 tienen que codificar la información en nueve dígitos, a las áreas con mayor producción les corresponden dígitos más cortos. También, dentro de una misma área, los editores de mayor envergadura se identifican por números más chicos. De este modo, quienes producen más libros pueden reservarse más dígitos para identificarlos. Los distintos campos se separan con un guion, y hay además algunas reglas de prefijo para evitar la confusión entre campos en caso de que el guion no esté. No desarrollaremos este párrafo, pero la información al respecto puede encontrarse, por ejemplo, en los manuales disponibles en el sitio referido en nota al pie Nº 5.

[3] La traducción fue hecha por los autores de este artículo.

[4] Aunque en este artículo nos referiremos al ISBN fundamentalmente como a un sistema de identificación de libros, se utiliza también para publicaciones en otros soportes (videos educativos, publicaciones multimedia, etc.).

[5] Más información al respecto puede encontrarse en línea: http://www.isbn-international.org/esp/index.html

La receta para determinar la última, el dígito de control, es la siguiente: hay que multiplicar la primera cifra del número que identifica al libro por 1, la segunda por 2, la tercera por 3, la cuarta por 4, la quinta por 5, la sexta por 6, la séptima por 7, la octava por 8, la novena por 9, sumar todo, hacer la división entera entre 11 y quedarnos con el resto. Ese es el dígito de control. Veamos un ejemplo.

El libro *Mati cuatro* (Pena, Gadino y Varela, 1999) está identificado por el ISBN:

$$9974 - 618 - 14 - ¿?$$

del que solo hemos copiado los datos que corresponden a región, editor y número de publicación. Falta calcular el dígito de control. Hacemos la cuenta:

$$9x1 + 9x2 + 7x3 + 4x4 + 6x5 + 1x6 + 8x7 + 1x8 + 4x9 = 200$$

y luego la división entera entre 11:

$$200 = 18 \times 11 + 2$$

que arroja resto 2. El ISBN que estamos buscando es entonces:

$$9974 - 618 - 14 - 2.$$

Para algunos libros, por ejemplo, *Con los pájaros pintados*, de Julio Brum (2000), al hacer este cálculo, la división entre 11 arroja resto 10. En estos casos el carácter de control se representa con una X. Al texto mencionado le corresponde el ISBN 9974 – 653 – 72 – X.

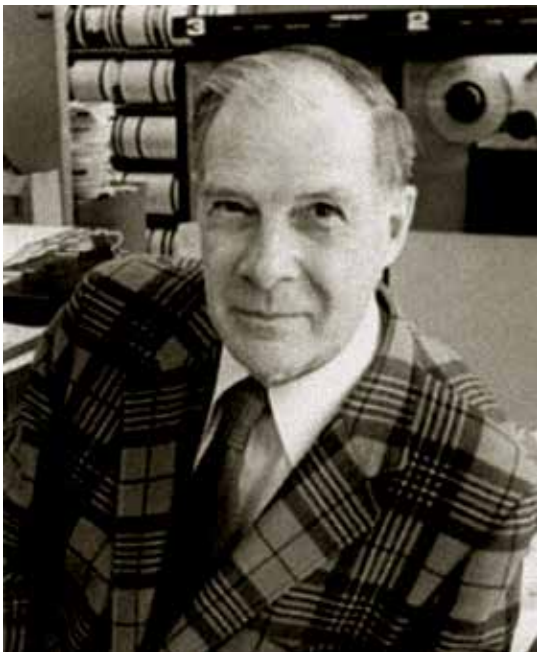
La aritmética en la que solo conservamos los restos de la división entera entre 11 se conoce con el nombre de ***aritmética módulo 11***. En general, dado cualquier número entero *n* se puede construir una aritmética módulo *n*, siguiendo la regla de dividir entre *n* y solo conservar el resto de la división entera. Por ejemplo, calcular empleando una ***aritmética módulo 10*** es equivalente a solo conservar, de los números, la cifra de las unidades. Esta aritmética se emplea en algunos dígitos de control. En particular, en el nuevo ISBN13, un estándar de identificación que se está usando en todos los libros impresos a partir de enero de 2007, y que seguramente será el mayoritario en nuestras bibliotecas dentro de poco tiempo.

Una ventaja de la aritmética módulo 10 es que los restos de dividir entre 10 se reducen a las cifras habituales, por lo que no hace falta incorporar ningún carácter extra, como ocurre en el ISBN estándar que a veces requiere una X. Esta aritmética es la que emplean el dígito de control de la cédula de identidad y el sistema EAN13 de identificación de productos, según el cual se asigna a todos los productos que encontramos en almacenes y supermercados un número de identificación que aparece representado por medio de un código de barras impreso en el exterior del envase. Desde el punto de vista del cálculo de los dígitos de control, EAN13 e ISBN13 son idénticos. Para cerrar este párrafo, digamos que aunque la aritmética módulo 10 es más simple de manejar cuando los números se representan en base 10, tal como hace nuestra civilización con casi todos los registros

numéricos que los humanos leemos, las propiedades de un dígito de control basado en una aritmética módulo 11 son mejores que las de uno que emplea aritmética módulo 10. Escapa al alcance de esta nota explicar la razón, pero digamos que el dígito de control del ISBN10 permite detectar muchos de los posibles errores al almacenar o digitar este número, como son el cambio de cualquier dígito por otro, o la transposición de dos dígitos cualesquiera. Como vimos antes con los controles de paridad, también hace posible recuperar cualquier dígito perdido, aunque rara vez se utiliza de esta manera. Algunas de estas capacidades de detección de errores, o corrección de borraduras, no se alcanzan por los dígitos de control de EAN13 o la cédula de identidad uruguaya. El lector interesado puede consultar Fernández y Gil (2001). Una descripción literaria de la aritmética módulo cualquier número entero *n* y otras alternativas a la aritmética usual -que también tienen interés matemático y significados relevantes- puede encontrarse en el capítulo 13 del libro *Matemáticamente tenemos chance* (Gil, 2011), reproducido en el Nº 109 de la Revista *QUEHACER EDUCATIVO*.

Un paso más: corrigiendo

En su fundamental artículo de 1950, "Error detecting and error correcting codes", Richard Hamming (1915-1998) analiza el problema de cómo conseguir que una computadora pueda corregir los inevitables errores que se producen en el procesamiento de un gran volumen de datos. En este trabajo, de agradable lectura, Hamming relata *«en algunas situaciones la verificación automática no es suficiente... las máquinas trabajaban sin atención durante las noches y fines de semana, sin embargo, los errores implicaban que los cálculos se detuvieran, aunque las máquinas pudieran dedicarse a otros problemas. El presente se orienta hacia la velocidad en computadores digitales cuyos elementos básicos son algo más confiables por operación que los relays. Sin embargo, la incidencia de fallos aislados, aún cuando sean detectados, podría interferir seriamente con el uso normal de estas máquinas»*. La posibilidad de detectar automáticamente errores ya era conocida en esa época, y se usaba para detener los cálculos cuando aparecían errores. Continúa

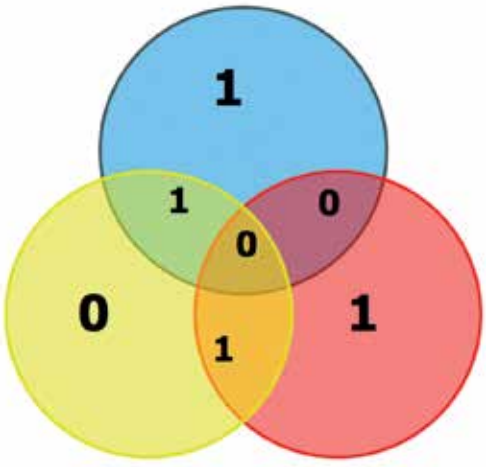


Hamming, *«parece entonces deseable examinar el próximo paso más allá de la detección de errores, la corrección de errores»*[6].

En el mismo artículo citado, Hamming propone una familia de códigos, que ilustramos a través de un ejemplo, por medio de una representación gráfica introducida por Robert McEliece. El código que mostraremos es conocido como código de Hamming [7,4,3]. Codifica una "palabra" de cuatro bits, como:

(1 0 1 0)

con siete bits, y permite corregir un error.

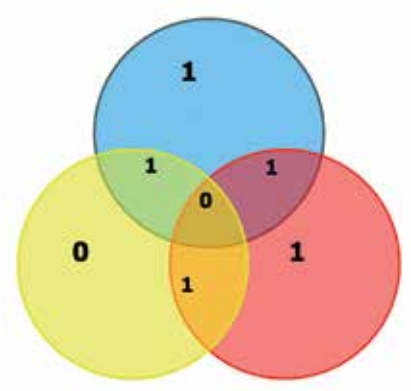


[6] La traducción fue hecha por los autores de este artículo.

Distribuyamos los cuatro símbolos 1, 0, 1, 0 como aparecen en color negro y números pequeños en el esquema, y luego agreguemos controles de paridad en cada uno de los círculos, de modo que todos contengan un número par de unos. En el azul y en el rojo habrá que colocar un uno, y un cero en el amarillo. Estos dígitos de control, representados en el esquema con un tipo de letra de mayor tamaño, completan una palabra de siete bits:

(**1 0** 1 **1** 0 1 0)

formada por los cuatro dígitos originales, que interpretaremos como la información que queremos almacenar o transmitir, y los tres dígitos de control de paridad, que hemos intercalado en negrita[7].



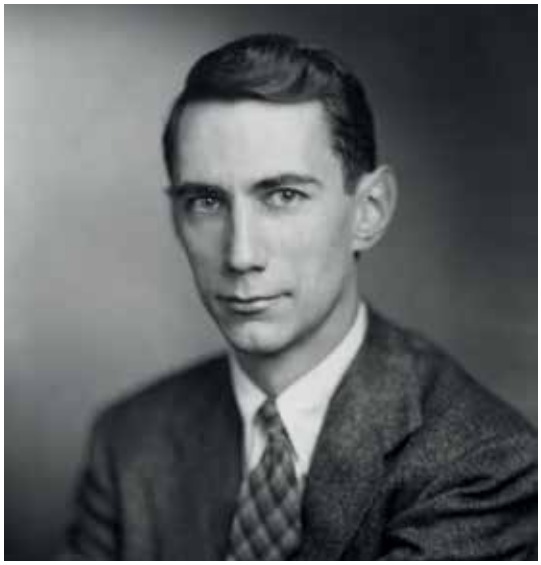
Este esquema permite corregir un error: si uno de los siete dígitos se cambia por un valor equivocado, tal como hemos hecho en la figura pequeña, no solo detectaremos que hubo un error. Tenemos además suficiente información para ubicarlo y corregir el "bit dañado".

Al examinar el círculo azul del nuevo esquema encontramos que su control de paridad falla, igual que ocurre con el rojo. Pero el del amarillo se satisface. Por lo tanto tenemos que cambiar lo que está en la intersección del disco rojo y del azul, pero no en el amarillo. De esta manera corregimos el uno equivocado, y recuperamos la palabra que habíamos codificado en nuestro primer diagrama.

[7] El lugar en que los hemos intercalado es irrelevante para nuestra discusión, pero respeta la disposición original propuesta por Hamming. Ver, por ejemplo, el artículo original (Hamming, 1950).

El lector interesado puede jugar con los diagramas, y encontrará que siempre es posible corregir correctamente cualquier patrón que contenga exactamente un error. También se pueden borrar dos números cualesquiera del esquema de círculos, y encontrar la información perdida imponiendo la condición de que en cada uno de los tres círculos coloreados debe satisfacerse un control de paridad. Si se introducen dos errores, ya no se puede recuperar correctamente la palabra original, pero el interés de este esquema de codificación subsiste, porque en la práctica es mucho más improbable cometer dos errores que cometer uno solo.

Shannon y la teoría de la información



La frase que cierra el último párrafo ilustra un hecho central de toda la teoría y la práctica de la corrección automática de errores: solo podemos disminuir la probabilidad de cometer errores, pero nunca podremos estar seguros de que evitaremos todos los errores. Por ejemplo, si un fragmento de información correcta es sustituido completamente por otro también correcto, no lo notaremos, pero la probabilidad de que esto suceda como puro fruto del azar es muy baja. La fiabilidad de los procesos de comunicación depende entonces de un análisis estadístico, cuyos fundamentos fueron establecidos por Claude E. Shannon en el artículo "A Mathematical Theory of Communication", publicado en 1948. Una obra que ha tenido una influencia impactante en nuestra vida cotidiana: la sociedad

de la información y las telecomunicaciones en la que vivimos descansa en buena parte sobre esta teoría, que sentó las bases necesarias para hacer posible la comunicación digital. Los procesos de protección contra errores y de compresión de la información encuentran en ella un marco natural.

Luego de los trabajos de Hamming y Shannon de fines de los años cuarenta, el progreso en esta área se fue acelerando. En 1960 aparecieron los códigos de Reed-Solomon (1960), que permiten trabajar a nivel de los *bytes* y no de los bits individuales. Se adaptan mucho mejor que los códigos de Hamming a muchas situaciones reales, en que los errores suelen aparecer en forma de rachas que afectan varios bits consecutivos. Un hecho notable es que están basados en el álgebra introducida por el francés Évariste Galois (1811-1832). Un álgebra que permitió resolver problemas provenientes de la antigüedad clásica, como demostrar la imposibilidad de la cuadratura del círculo o la trisección del ángulo con regla y compás; también cerrar el problema de decidir cuándo se pueden hallar las raíces de un polinomio cualquiera por una fórmula similar a la que desde el liceo conocemos para los polinomios de segundo grado, una cuestión candente en los tiempos en que Galois vivió. En un giro imprevisible en esos años, partes de su teoría terminaron ocupando un lugar importante en nuestra tecnología de comunicaciones.

A pesar de morir antes de cumplir los veintiún años, las contribuciones de Galois hacen que lo consideremos uno de los matemáticos más destacados que la humanidad ha producido. La historia de su vida no es menos apasionante que la Matemática que nos ha dejado. Al respecto ver, por ejemplo, Corbalán (2000). La introducción histórica de Stewart (2004) también es recomendable.

Para tener procedimientos de comunicación prácticos no basta con codificar bien, también hay que decodificar bien y rápido. A fines de los años sesenta se desarrollaron los primeros algoritmos eficientes para decodificar códigos de Reed-Solomon. Este hecho, junto a las mayores exigencias de fidelidad originadas por los progresos en la compresión de la información, hizo que en los años setenta los códigos de Reed-Solomon pasaran a formar parte de los estándares de comunicaciones adoptados por la NASA para sus misiones espaciales. En los ochenta fueron integrados a las especificaciones de los discos compactos. Desde entonces, los códigos correctores de errores, la aritmética módulo 2, el álgebra de Galois, están ahí, trabajando todo el tiempo para nosotros, cada vez que escuchamos música o miramos una película almacenada en un DVD.

Todo esto, ¿tiene un lugar en la escuela?

Las matemáticas que el procesamiento y la trasmisión de la información utilizan son muy ricas y variadas. Esto está fuera de toda duda y se refleja en miles de libros de texto y artículos. Por ejemplo, una búsqueda de documentos que contuvieran referencias a *"information theory"*, realizada en la base de datos *Zentralblatt* durante la redacción de este artículo, arrojó casi 3000 títulos. *Zentralblatt* es una base de consulta para investigadores, especializada en publicaciones de Matemática. El mismo experimento, hecho sobre la mucho menos especializada internet a través de una ventana del buscador *Google*, devuelve más de dos millones de páginas. En esta nota pretendemos mostrar que parte de todo este rico mundo podría merecer un lugar en las aulas escolares y de formación docente, y que además es interesante y estimulante referir a él. Ilustraremos esta idea con ejemplos provenientes del área de los dígitos de control y los códigos correctores de errores.

Las primeras actividades que se pueden proponer a un nivel muy lúdico, solo requieren sumar e identificar la cifra de las unidades de un número natural. Las codificaciones según los estándares EAN13 e ISBN13 son aplicaciones realistas, que pueden trabajarse sobre la base de estas mismas ideas y la multiplicación por tres. A partir de aquí se extiende un continuo de posibilidades, con un nivel de dificultad que va creciendo hasta alcanzar problemas abiertos, cuestiones de investigación en la frontera misma del conocimiento.

Por otra parte, el estudio de los dígitos de control y los códigos correctores de errores permite integrar en forma natural temas de aritmética, geometría, combinatoria, probabilidad, estadística y álgebra lineal, al tiempo que promueve la búsqueda de algoritmos para ejecutar en forma eficiente algunas tareas. Creemos posible entonces proponer actividades adecuadas a los distintos niveles educativos, desde la escuela al bachillerato, que permitan:

- Mostrar que el conocimiento científico, en particular el matemático, es el resultado de una obra humana inacabada, que continúa haciéndose hoy en día. También que nuestra sociedad participa activamente de esta tarea.
- Presentar situaciones en las que se opera con objetos usuales siguiendo reglas diferentes, para ir generando la idea de que la Matemática toma diversas formas para adaptarse a distintas situaciones.
- Proponer actividades para poner en juego competencias y contenidos tradicionales que la escuela asume y que es pertinente conservar.
- Favorecer la construcción de algoritmos y de algoritmos eficientes, para realizar algunas tareas simples.

El último punto de esta selección de objetivos hace a este tema especialmente apropiado para explotar el potencial del proyecto CEIBAL, porque se tendrá la posibilidad de visualizar ejemplos en la pantalla de una computadora, implementar en una computadora algunos algoritmos, modificar algoritmos preexistentes, realizar simulaciones, etc.

2. Actividades en el aula

En el resto de este trabajo presentamos el esbozo de algunas propuestas de trabajo en el aula, y un avance de los resultados surgidos de su puesta en práctica con alumnos de sexto grado.

Actividad 1 - "El matemágico"

En esta actividad se presenta a los alumnos una caja conteniendo las 10 000 posibles listas de cinco números de una cifra cuya suma es un múltiplo de diez.

Objetivo: identificar una regularidad en un conjunto de datos.

Consigna: en esta caja hay muchísimas listas de números de una sola cifra. Cada equipo sacará dos listas y las copiará en una hoja. Al copiar una de ellas, el equipo debe cambiar una cifra por otra que elija, sin que ningún otro equipo se entere. La otra lista la deben copiar sin realizar ningún cambio. Cada equipo nos mostrará sus listas y descubriremos cuál es la lista que ha sido modificada.

Se pretende que los alumnos busquen una posible explicación a la "magia".

Nuestra hipótesis inicial era que podía resultar difícil el reconocimiento de la regularidad, por lo que previmos algunas intervenciones posibles. El docente puede proponer sumar los números de cada lista y observar alguna regularidad.

Listas fieles	Listas modificadas
5 - 7 - 8 - 9 - 1	1 - 7 - 6 - 9 - 1
1 - 2 - 3 - 5 - 9	5 - 3 - 8 - 2 - 1
4 - 6 - 2 - 5 - 3	1 - 7 - 1 - 4 - 5

Los alumnos deben sacar una "regla" para discutir colectivamente. Todas las listas cumplen una misma propiedad: al sumar los números de la lista el resultado termina en cero. Previamente pensamos que era posible que los niños intentaran probar con otros números el cumplimiento de la regla.

Los alumnos inmediatamente comenzaron a buscar la regularidad y la identifican de la siguiente manera:

–"Da justo 20, 30, 40..., pero la que cambia, no."
– "En realidad tiene que dar un número terminado en cero."
– "¡Son múltiplos de 10!"

De esta manera se llega a la regla: la suma de todos los números de una lista es un número múltiplo de 10.

Aquí se da una interesante discusión sobre qué múltiplos de 10.

B: –Sí, son múltiplos de 10.
R: –Pero no todos, porque 100 no te puede dar.
B: –Claro, porque no llegas.
A: –Sí, puede ser 10, 20 o 30.
R: –Te puede dar 40; si pones 9, 9, 9, 9, 4 da 40.
A: –Pero vos repetiste el 9.
R: –Y pongo 8, 9, 7, 7, 9 y también me da 40.
B: –Pero sin repetir ninguno, solo podes llegar a 30.

Posteriormente es necesario ver de qué manera "el mago" utiliza esta regla. Para ello se proponen las siguientes actividades.

Actividad 2

Objetivo: identificar las condicionantes de la regla ya construida.

Consigna: ahora ustedes sacarán otras listas y deberán modificarlas alterando una única posición. ¿Se cumple la regla que descubrieron anteriormente?

Con esta actividad se pretende que verifiquen que, en esta situación, nunca se obtiene una lista con la propiedad de que la suma de sus cifras termina en cero. En este caso se apunta a que los alumnos puedan dar una explicación a la regla que construyen.

Inmediatamente concluyen que **es necesario cambiar más de un número para que la primera regla se cumpla**. Afirman que con uno no se puede, que hay que cambiar **dos números**.

Estas dos actividades aportan elementos para la detección de errores, puesto que, en caso de no cumplirse la regla, ya se sabe que hay un número erróneo.

Se presenta la posibilidad de promover la comparación entre las dos actividades y sintetizar las reglas elaboradas hasta el momento. Se puede ir armando un "yo ya sé" provisorio que incluya estas reglas.

Actividad 3

Objetivo: poner en juego la regla explicitada bajo ciertas condiciones.

Consigna: ustedes deberán completar listas de la bolsa del mago. Por ejemplo, los primeros cuatro números de una lista son: 1, 8, 7 y 7, ¿cuál es el quinto número?
En la lista del mago 1, 2, 1, **X**, 3 alguien tachó el cuarto número y solo se ve una **X**. ¿Qué número está debajo de la **X**? ¿Y en 6, 5, **X**, 9, 9?

La variante de esta actividad es que la suma de los 5 números está condicionada por 4 dígitos ya dados.

Esta actividad es fácilmente resuelta y se debe discutir si existe más de una posibilidad de completar esas listas, argumentando la respuesta.

Actividad 4

En las actividades anteriores, los alumnos construyen reglas que describen las características de las listas; han probado cambiar números de las listas sustituyéndolos por otros, extrayendo posteriormente nuevas conclusiones. En esta actividad, en la que se hacen nuevos "movimientos" de números, se pretende poner en juego la propiedad conmutativa de la suma. Como en oportunidades anteriores, se promueve la explicación, por parte de los alumnos, de las conclusiones que extraen.

Objetivo: activar la propiedad conmutativa de la adición.

Consigna: si en vez de cambiar un número por otro, intercambiamos entre sí dos números de la lista, ¿el mago puede descubrir el engaño? ¿Y si entreveramos toda la lista, copiando los números en cualquier orden?

Actividad 5

Objetivo: explorar los límites de la regla.

Consigna: ustedes tomarán una lista de la urna y la modificarán cambiando exactamente dos números, para producir una nueva lista que pueda estar en la bolsa y engañar de esta manera al mago.

La propuesta exige poner en juego la primera regla (resultado de la suma terminado en cero) y modificar dos números para que la misma se cumpla. Si bien está condicionado por los dígitos dados, exige decidir por dos de ellos y modificarlos llevando el control de la suma. En esta ocasión se pueden discutir las diferentes soluciones halladas. También es posible relacionar con otra de las actividades anteriores en la que los cambios debían respetar la regla.

Es interesante ver algunos intercambios de opiniones entre los alumnos.

S: –Con esta lista 5 - 9 - 4 - 7 - 5 podés cambiar el 4 y el 5 por el 3 y el 6.
N: –O podes cambiar por 2 y 7, o también por 1 y 9.
C: –Y nada más. Después tenés que elegir otros dos números para cambiar.

Actividad 6

Objetivo: poner en juego la regla sin ninguna restricción.

Consigna: ahora ustedes inventarán dos listas diferentes para la caja del mago.

En esta ocasión se agrega la dificultad de tener que llevar un control sobre los números que se van seleccionando y el resultado de la suma de los mismos. Una vez armadas las listas, se intercambian las producciones para que cada equipo valide las listas realizadas por otros equipos.

A esta altura de la secuencia, muchos alumnos al realizar las sumas no tomaban los dos dígitos resultantes, sino que quedaban solamente con la última cifra, hecho este que les simplificaba las sumas siguientes.

Actividad 7

Objetivo: reflexionar sobre los procesos seguidos para la creación de listas.

Consigna: en las actividades anteriores ustedes tuvieron que fabricar algunas listas del mago. Ahora tendrán que escribir una serie de instrucciones o "recetas" para enseñar a otros niños la "magia" que ustedes descubrieron.

Primera "receta"

¿Cómo hacer cuando nos entreguen los cuatro primeros números de la lista del mago y se debe encontrar el quinto?

- Escribir y comprobar que las instrucciones están bien dadas.
- Pasar la "receta" a otro equipo para que la pruebe.

Esta actividad apunta a que los alumnos expliciten reglas que se pusieron en juego. La primera parte se realiza en duplas y se intercambian posteriormente las recetas con otra pareja. Luego de comprobada la receta recibida, se integra un equipo con los 4 alumnos y acuerdan la redacción de una única receta.

A partir de esta actividad se elabora la regla de "hacer sumas fáciles", que son las reglas de la aritmética módulo 10. En clase, esta expresión, más técnica, no fue utilizada.

$$5 + 7 + 8 + 9 + 6 = 35$$

La última cifra no es cero, por lo tanto sabemos que no está en la lista. La forma "fácil de hacer la suma" se expresa de la siguiente forma:

$$5 + 7 = 12$$

me quedo solamente con la última cifra, un dos. Continuamos con la suma:

$$2 + 8 = 10$$

de la que conservamos solamente la última cifra, que ahora es un cero. Continuamos:

$$0 + 9 = 9$$

que no requiere ningún paso adicional, porque ya es un número de una sola cifra. Luego:

$$9 + 6 = 15$$

que tiene un cinco como última cifra.

Esta nueva regla aportó elementos para la comprensión del funcionamiento de los números de identificación de los productos según el estándar EAN13, que requiere un volumen de cálculo mayor, y en el que la simplificación de trabajar todo el tiempo módulo 10 es notoria.

La actividad posterior con estos códigos de barra permitió la utilización de algoritmos puestos en juego en la secuencia "del mago".

Algunas reflexiones

El siglo XX fue muy rico en avances de la ciencia, en particular de la Matemática, en direcciones muy diversas. ¿De qué manera debe reflejarse este hecho en la Matemática que se enseña en la escuela? La escuela seguramente deberá mantener en sus programas los grandes ejes temáticos de número, operaciones, geometría y mediciones, que hoy atraviesan su currículo. Son temas tradicionales, bien establecidos, que conservan su vigencia aunque en algunos casos provienen de la antigüedad clásica: son antiguos, pero no obsoletos.

Sin embargo, los avances del siglo XX muchas veces significan cambios en la aproximación a viejos conceptos, o la introducción de ideas simples con consecuencias profundas. Es falsa la creencia de que las matemáticas contemporáneas son necesariamente más complejas que las antiguas, y que a nivel del sistema educativo solamente pueden tener lugar a niveles de posgrado, pero son poco importantes para la formación de docentes, mucho menos aún para el currículo del bachillerato o la enseñanza media, y completamente irrelevantes para el nivel escolar. En muchos casos, la diferencia entre tenerlas presentes o no, tiene más que ver con la orientación general del sistema que con la profundidad de los conocimientos que se pretenden compartir y comunicar.

En particular, algunas de estas cuestiones permiten visitar con una nueva mirada otras, más clásicas, o simplemente proponer actividades que ayudan a explicar aspectos de la vida cotidiana que han aparecido gracias al avance científico y tecnológico. Los ejemplos provenientes de los códigos correctores de errores implican un contexto en el que realizar operaciones aritméticas, permiten resignificar algunas operaciones y aproximarse a ellas desde nuevos ángulos (por ejemplo, el resto de una división pasa a tener una importancia de la que carece en otros problemas), y hacen referencia a cuestiones de la vida diaria, contribuyendo a explicarlas. Dado que se trata de recuperar información perdida o aparentemente escondida, estos problemas admiten aproximaciones muy lúdicas y atractivas. De hecho, hemos presentado la primera parte de nuestras actividades como un juego de adivinación. Esta línea de trabajo ha sido

explorada por "Teatro y Matemática" (ANII, 2010), un proyecto que nuclea científicos, artistas y educadores.

Nuestra hipótesis de trabajo, que justifica la redacción de este artículo, es que los problemas relacionados con dígitos de control permiten generar un conjunto de actividades que, por su valor cultural, su capacidad de movilizar otros contenidos matemáticos, y el lugar que en la ciencia contemporánea ocupa todo lo que tiene que ver con el procesamiento de la información, justifican la inclusión del tema en el nivel escolar. Intuimos que otros temas relativos a la transmisión de información, como son la compresión de datos y la criptografía, son susceptibles de un tratamiento similar, aunque no hemos avanzado en esta dirección, ni siquiera para formular las primeras conjeturas y borradores de propuestas.

Este trabajo fue iniciado en el año 2007, en el marco de las acciones del Programa para el Mejoramiento de la Enseñanza de la Matemática en ANEP, y contamos con los aportes de los colegas que nos brindaron su estímulo y colaboración, muchos docentes y especialistas dedicaron tiempo y su experiencia a discutir con nosotros diversos aspectos de nuestro proyecto, a hacer posible la puesta en acto en un salón de clase, a aportar ejemplos, ideas, etc. Agradecemos entonces a: la

Dirección y Maestras de la Escuela Paraguay (2007, 2008) y del Colegio Latinoamericano; María del Carmen Chamorro (Universidad Complutense de Madrid); Pablo Fernández (Universidad Autónoma de Madrid); Adolfo Quirós (Universidad Autónoma de Madrid); Gadiel Seroussi (Hewlett-Packard); Jack Keil Wolf (Universidad de California en San Diego); y, por supuesto, a los niños que compartieron su entusiasmo con nosotros. Especialmente a ellos, que son los que dan algún sentido a estas páginas.

Referencias bibliográficas

ANII (2010): "Teatro y Matemática". Proyecto ANII de Popularización de la Ciencia, la Tecnología y la Innovación, desarrollado por la Facultad de Ingeniería de la Universidad de la República y Polizonteatro. En línea: http://teatroymatematica.blogspot.com

BRUM, Julio (2000): *Con los pájaros pintados*. Montevideo: Alfaguara Infantil.

CORBALÁN, Fernando (2000): *Galois. Revolución y matemáticas*. Madrid: Nivola Libros y Ediciones.

FERNÁNDEZ GALLARDO, Pablo; GIL ÁLVAREZ, Omar (2001): "Una introducción a los códigos detectores y correctores de errores". En línea: http://www.fing.edu.uy/~omargil/educmate/codyal31-71.pdf

GIL, Omar (2011): *Matemáticamente tenemos chance*. Montevideo: Ed. Fin de Siglo.

HAMMING, Richard W. (1950): "Error Detecting and Error Correcting Codes" en *The Bell System Technical Journal*, Vol. XXIX, Nº 2, páginas 147-160. En línea: http://www.lee.eng.uerj.br/~gil/redesII/hamming.pdf

HAMMING, Richard W. (1977): *Digital Filters*. Englewood Cliffs, NJ: Prentice-Hall.

HAMMING, Richard W. (1980a): *Coding and Information Theory*. Englewood Cliffs, NJ.: Prentice-Hall.

HAMMING, Richard W. (1980b): "The Unreasonable Effectiveness of Mathematics" en *American Mathematical Monthly*, Vol. 87, Nº 2, pp. 81-90. En línea: http://www.dartmouth.edu/~matc/MathDrama/reading/Hamming.html

INTERNATIONAL ISBN AGENCY. En línea: http://www.isbn-international.org/esp/index.html

PENA, Mónica; GADINO, Alfredo; VARELA, Carlos (1999): *Mati cuatro. Libro para el alumno*. Montevideo: Ed. Aula.

REED, Irving S.; SOLOMON, Gustave (1960): "Polynomial Codes over certain Finite Fields" en *Journal of the Society for Industrial and Applied Mathematics*, Vol. 8, pp. 300-304.

RODRÍGUEZ RAVA, Beatriz (2011): "Matemáticamente tenemos chance. Entrevista al autor" en Revista *QUEHACER EDUCATIVO*, Nº 109 (Octubre), pp. 22-26. Montevideo: FUM-TEP.

SHANNON, Claude E. (1948): "A Mathematical Theory of Communication" en *The Bell System Technical Journal*, Vol. XXVII, pp. 379-423 (Julio), 623-656 (Octubre).

STEWART, Ian (2004): *Galois Theory*. Nueva York: Chapman & Hall.