

# Revista de Educación Matemática

## Consejo Editorial

### *Editor Ejecutivo*

Leandro Cagliero, FAMAF, Universidad Nacional de Córdoba - CONICET, Argentina

### *Editores Asociados*

Juan Carlos Pedraza, Universidad de Buenos Aires, Argentina

Mónica Villarreal, FAMAF, Universidad Nacional de Córdoba - CONICET, Argentina

### *Comité Editorial*

Abraham Arcavi, Weizmann Institute of Science, Israel

Carlos D'Andrea, Universitat de Barcelona, España

Cristina Esteley, FAMAF, Universidad Nacional de Córdoba, Argentina

José Nicolás Gerez Cuevas, FAMAF, Universidad Nacional de Córdoba, Argentina

Susana Paula Graça Carreira, Universidade do Algarve, Portugal

Patricio Herbst, Universidad de Michigan, Estados Unidos

Teresa Krick, Universidad de Buenos Aires - CONICET, Argentina

Ricardo Podestá, FAMAF, Universidad Nacional de Córdoba - CONICET, Argentina

Nélia Maria Pontes Amado, Universidade do Algarve, Portugal

Juan Pablo Rossetti, FAMAF, Universidad Nacional de Córdoba - CONICET, Argentina

Gabriel Rubén Soto, Fac. de Ingeniería, U. Nacional de la Patagonia San Juan Bosco, Argentina

Jhony Alexander Villa-Ochoa, Universidad de Antioquia, Colombia

Registro Nacional de la Propiedad Intelectual N° 168024

ISSN 0326-8780 (versión impresa)

ISSN 1852-2890 (en línea)

Página web: <https://revistas.unc.edu.ar/index.php/REM/index>

Correo electrónico: [revm@famaf.unc.edu.ar](mailto:revm@famaf.unc.edu.ar)

# Revista de Educación Matemática

Volumen 37, N° 2 – 2022

---

## ÍNDICE

---

---

### ARTÍCULOS

- **CRIPTOGRAFÍA, LITERATURA Y EDUCACIÓN INTEGRAL: “VIAJE AL CENTRO DE LA TIERRA” DE JULIO VERNE**  
*Vicente Jara-Vera y Carmen Sánchez-Ávila* ..... 3
- **EN BUSCA DE LA FELICIDAD**  
*Roberto Ben, Agustín Besteiro, Antonio Cafure, Darío Devia y Diego Rial* ... 30

---

### SECCIONES FIJAS

- **¿Sabías que...?**  
*por L. Cagliero y R. Podestá* ..... 27
- **Sección de Problemas**  
*por J.P. Rossetti* ..... 46

---

También encontrarás al final las *¡Crucigramas Matemáticos!*



---

# CRIPTOGRAFÍA, LITERATURA Y EDUCACIÓN INTEGRAL: “VIAJE AL CENTRO DE LA TIERRA” DE JULIO VERNE

Vicente Jara-Vera y Carmen Sánchez-Ávila

---

**RESUMEN.** Ofrecemos en este artículo un ejemplo de las posibilidades de la Criptografía, como rama de la Matemática Aplicada, para abarcar de manera grata y fructífera numerosas cuestiones imprescindibles de la Educación. Y cuando decimos Educación queremos resaltar su semántica más amplia y extensa, tan necesaria y tan añorada muchas veces hoy en día, sin perder la necesaria precisión de la especialización, agrupando en este estudio cuestiones relativas a áreas como la Matemática, la Seguridad de las Comunicaciones, la Literatura, la Lingüística, o las Lenguas Clásicas. Nos hemos apoyado para tal efecto en una famosa obra literaria del genial escritor francés Julio G. Verne, “Viaje al centro de la Tierra”. A partir únicamente del enigmático mensaje que aparece al inicio de la novela ofrecemos detalladamente y por medios criptoanalíticos la solución, mostrando paso a paso los diversos acercamientos para resolver de manera general un texto desconocido. Finalmente, este ejemplo nos sirve para detallar algunos elementos fundamentales del Álgebra y de la Teoría de la Comunicación que son propios de la Criptología.

*Palabras clave:* Criptoanálisis, Criptografía, Educación, Literatura.

**ABSTRACT.** We offer in this paper an example of the possibilities of Cryptography, as a branch of Applied Mathematics, to cover pleasantly and fruitfully many essential questions of Education. And when we say Education we want to highlight its broader and more extensive semantics, so necessary and so longed for many times today, without losing the necessary precision of specialization, grouping in this study issues related to areas such as Mathematics, Communications Security, Literature, Linguistics, or Classical Languages. For this purpose, we have relied on a famous literary work by the great French writer Jules G. Verne, “Journey to the Center of the Earth”. Based solely on the enigmatic message that appears at the beginning of the novel we offer the solution in detail and by cryptanalytic means, showing step by step the various approaches to generally resolve an unknown text. Finally, this example helps us to detail some fundamental elements of Algebra and Communication Theory that are typical of Cryptology.

*Keywords:* Cryptanalysis, Cryptography, Education, Literature

## §1. Introducción

*Toda novela es un testimonio cifrado (Vargas-Llosa, 1971).*

Sin negar la afirmación mencionada por el premiado con el Nobel de Literatura, vamos a circunscribirnos mucho más, en concreto, a algunas novelas muy significativas donde el cifrado es mucho más patente. Nuestra intención es llamar la atención sobre esas obras, las cuales suelen quedar ubicadas en aquellos momentos de la vida donde los niños y jóvenes atisban la adultez, con la pretensión de rescatarlas también, sin olvidar aquellos, para una edad más madura y reflexiva. La justificación está en que los tonos y coloridos que proyectan ofrecen a este lector más reflexivo aspectos inéditos que con casi total seguridad pasó por alto en aquella época. Además, en las tareas educativas y docentes pueden utilizarse muy acertadamente, sirviendo de textos motivadores y ofreciendo una gran transversalidad, abarcando desde ellas multitud de disciplinas, no solo la Literatura o la Lingüística, o las Lenguas Clásicas, sino también la Matemática, la Criptología y la Teoría de la Seguridad y las Comunicaciones.

Han sido muchos los literatos que se sintieron atraídos por la Criptografía, o al menos, la usaron como elemento de provecho, por aquello del misterio que lleva aparejado, para algunas de sus novelas (Kahn, 1996). Sin ser exhaustivos, podemos indicar algunos de ellos.

Así, el británico William Makepeace Thackeray (1811-1863), quien en su novela "The History of Henry Esmond" (1852) menciona un cifrado de transposición con rejilla de Cardano: una permutación de las letras del texto, desordenándolas según una serie de agujeros dispuestos de manera confusa en una plantilla.

Otro es el irlandés Bram Stoker (1847-1912), quien en "The Mystery of the Sea" (1902) muestra un complicado sistema de cifrado y esteganografía con el sistema de Francis Bacon, sustitución múltiple biliteral, obligándose a ofrecer al lector varios apéndices explicativos.

Mencionemos al inglés Henry Rider Haggard (1856-1925), el cual en "Colonel Quaritch, V.C.: A Tale of Country Life" (1888) ofrecerá un cifrado con letras nulas, escondiendo así el texto de interés.

El escritor estadounidense Robert William Chambers (1865-1933) escribirá "The Tracer of Lost Persons" (1906), donde aparecerá un cifrado de sustitución sencillo de signos a números, que serán luego los ordinales de las letras alfabéticas del mensaje oculto.

No podía faltar en este breve listado la inglesa Agatha Christie (1890-1976), quien en "The Four Suspects" (1932) diferentes nombres de dalias generan un mensaje secreto.

Sin embargo, de entre todos los autores, los que más resaltan son sin duda alguna Poe, Verne y Doyle.

De la pluma del estadounidense Edgar Allan Poe (1809-1849) salió el famoso relato "The Gold-Bug" (1843), donde encontramos un sencillo cifrado de sustitución monográfica monoalfabeto: es decir, donde cada letra del texto en claro es sustituida por otro signo y siempre por el mismo otro signo (Poe, 1843).

De entre los grandes novelistas en lengua francesa hemos de citar a Jules Gabriel Verne (1828-1905), conocido en los países iberoamericanos como Julio Verne, quien se servirá en cuatro de sus novelas de la Criptografía. En la famosa "Voyage au centre de la Terre" (Verne, 1864) encontramos un mensaje cifrado que esconde el lugar por el cual se puede acceder al centro del planeta Tierra. En la segunda novela, "Les enfants du Capitaine Grant" (Verne, 1868), los hijos de un capitán de navío lanzan una petición de socorro al mar en una botella que será posteriormente tragada por un tiburón martillo. La verdad es que aquí no estamos ante un mensaje cifrado, sino simplemente muy deteriorado, con un mismo texto de auxilio en inglés, alemán y francés, que a trozos, de uno y otro idioma, permiten recomponerlo en gran parte. Unos años más tarde escribirá Verne "La Jangada" (Verne, 1881), situada en el Amazonas, donde un texto cifrado de sustitución polialfabética (ahora no siempre la misma letra es sustituida por el mismo símbolo) es pieza fundamental para prevenir un matrimonio no deseado y conseguir una exoneración de delitos acaecidos en el pasado. La cuarta novela es "Mathias Sandorf" (Verne, 1885), donde un mensaje cifrado interceptado lleva a impedir una revuelta revolucionaria.

No podía faltar Sherlock Holmes en este tipo de enigmas, y así, el escocés Arthur Conan Doyle (1859-1930) lo situó enfrentándose a varios de estos textos cifrados. En su novela "The 'Gloria Scott'" (Doyle, 1893) encontramos un mensaje cifrado (y esteganográfico) escondido en un texto mayor con inserción de palabras nulas, pues para leer el correcto hay que tomar las terceras palabras del mensaje. El segundo caso es el más famoso, "The Dancing Men" (Doyle, 1905), donde aparece un cifrado de sustitución por figuritas humanas en diversas posiciones de brazos y manos y en ocasiones con o sin banderines. Finalmente, en el relato "The Valley of Fear" (Doyle, 1915) el famoso detective consigue acertar en la suposición del libro de código usado por su némesis Moriarty, solucionando un cifrado extremadamente complejo.

En este artículo nos centraremos en la primera novela mencionada de Julio Verne, "Viaje al centro de la Tierra", por recoger los cifrados de sustitución (al menos monoalfabético) y de transposición, que son componentes fundamentales de los métodos criptológicos (Jara-Vera y Sánchez-Ávila, 2021). Esperemos sirva para apetecer zambullirse en el resto de relatos aquí mencionados.

## §2. El cifrado de "Viaje al centro de la Tierra"

En la muy conocida novela que nos ocupa, casi al inicio de la misma, durante la conversación del profesor Otto Lidenbrock, especialista en mineralogía, con su

sobrino acerca de un preciado libro del escritor islandés del siglo XII-XIII Snorri Sturluson, recién adquirido en una vieja librería, se desprende de su interior un pergamino con un extraño mensaje (Fig. 1). Este, sin ninguna pista más, será el objeto de nuestra investigación. Vamos a intentar resolverlo de la manera más difícil, es decir, sin tener en cuenta ninguno de los aspectos relativos al libro en el cual estaba escondido o su autor, es decir, intentaremos el descifrado basándonos en el solo texto.

### 2.1. Criptoanálisis.



FIGURA 1. Mensaje original de la novela (Verne, 1864).

Este extraño mensaje parece consistir en un conjunto amplio de signos fácilmente separables. Analizando la lista de elementos y entendiendo que es un texto manuscrito donde los elementos no tienen que ser exactamente iguales, podemos contar un total de 136 signos que podemos agrupar por su aparente similitud en diversos conjuntos (Fig. 2).



FIGURA 2. Agrupación inicial de signos por su similitud.

Una mirada más precisa sobre la lista de elementos nos lleva a fijarnos en el parecido entre algunos de ellos. En concreto, los de la (Fig. 3).



FIGURA 3. Algunos aparentes parecidos entre signos.

Los pares son similares a los impares respectivamente, pero con un cierto marcado en las partes finales de los trazos tal y como se haría con las letras mayúsculas en las lenguas provenientes del latín.

Y es también remarcable que haya algunos signos, los menos comunes, que son como tildes, comas o puntos, como si fueran signos de puntuación, como apreciamos en la parte final del listado de la (Fig. 2). Hemos de ver qué significado pueden tener. Porque aún no podemos afirmar que sea un texto cifrado, por ahora no sabemos nada del mismo, o casi nada. Decir que curiosamente, dentro de la historia de la Criptografía, al menos en la Criptografía clásica, han sido habitualmente signos que no han solido cifrarse, los signos de puntuación, dándose por supuesto en la lectura del texto descifrado, que podía irlos colocando por el contexto.

Al repasar la lista de frecuencias (Fig. 2) apreciamos que la cantidad de signos diferentes es pequeña. Incluso si consideramos signos diferentes los indicados previamente (Fig. 3) y no pensamos en signos de puntuación insertos, tendríamos un total de 25, que coincide muy bien con una estructura lingüística vocálico-consonántica, y no con una estructura silábica, que precisaría de varias veces más de signos, ni estructuras intermedias entre ambas. Este es el primero de los análisis que tenemos que realizar, ver la estructura de la lengua subyacente.

En el caso más restrictivo de no contar como distintos los cuatro signos de la (Fig. 3) ni tampoco los dos finales del listado de la (Fig. 2) tendríamos un total de 19 elementos, lo que es algo menos de lo esperado en una lengua vocálico-consonántica, si bien el texto bajo estudio (Fig. 1) no es muy largo y podemos esperar que no todos los signos, por ejemplo, de un alfabeto amplio, como {a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z}, se hayan utilizado.

Otro aspecto que salta a la vista es la curiosa exposición de elementos, agrupados en lo que parecen ser tres columnas distintas y separables. Atendiendo a la cantidad de unidades o elementos que aparece en cada línea de cada columna tenemos un recuento altamente regular (Fig. 4).

7	7	7
7	7	7
7	7	7
7	6	6
6	6	6
6	6	6
6	6	6

FIGURA 4. Disposición estructural de los signos del mensaje.

A partir de este momento vamos a intentar suponer la lengua en la cual está escrito el texto. Un primer grupo de lenguas en las que podemos pensar es el gran Filo Indoeuropeo, o en los Filos Urálico, Caucásico y Altaico. Con esto completaríamos todo el arco de Europa y el Asia Occidental.

Existe un invariante muy usado en Criptografía, el denominado Índice de Coincidencia, el cual nos permite acotar la posible lengua base del mensaje, ya que nos



da la frecuencia relativa de encontrar en dos textos el mismo carácter en la misma posición (Friedman, 1987; Bauer, 2007), un dato que se mantiene con gran regularidad en los lenguajes a pesar del paso del tiempo (Jara-Vera y Sánchez-Ávila, 2019), estando definido como

$$I_c = \frac{\sum_{i=1}^m q_i(q_i - 1)}{Q(Q - 1)},$$

donde  $Q$  es el número de elementos de la secuencia literal,  $q_i$  las respectivas apariciones de cada grafema en la secuencia literal y  $m$  la cantidad de elementos alfabéticos. La expresión evalúa la probabilidad de elegir dos caracteres iguales de forma aleatoria, de ahí el producto  $(\frac{q_i}{Q})(\frac{q_i-1}{Q-1})$ , que proviene del cálculo de las combinaciones  $C_{q_i,2} = \frac{1}{2}q_i(q_i - 1)$  dividido entre  $\frac{1}{2}Q(Q - 1)$ , agrupadas en un sumatorio sobre cada uno de los caracteres o elementos alfabéticos.

El índice  $I_c$  mide la variación de la frecuencia de aparición de los caracteres en un texto, y como hemos dicho, suele estar muy acotado para cada lenguaje. Además, y es lo que a nosotros nos interesará, este valor se mantiene aun cuando el texto haya sido cifrado por transposición o sustitución monoalfabética, e incluso permite comprobar si el mensaje ha sido cifrado usando un modo polialfabético, pues en este último caso ofrece un valor cercano a cero.

Para nuestro texto cifrado el valor del I.C. sin considerar los valores mayúscula es de 0,071203777, mientras que en el caso de tenerlos en cuenta es de 0,072287763. Estos valores nos llevan a pensar en que no se han aplicado cifrados polialfabéticos, y en todo caso solo permutaciones o sustituciones monoalfabéticas. Sin embargo, los valores obtenidos son muy comunes en multitud de lenguas, incluso de diversos Filos lingüísticos diferentes (Jara-Vera, 2016), por lo que prescindiremos de este invariante y buscaremos otros modos de atacar nuestro texto.

A pesar de lo poco que sabemos hasta ahora de nuestro mensaje secreto, es claro no obstante, que los signos gráficos del mensaje nos obligan a considerar las runas como un lenguaje que quizás resuelva el significado de lo que tenemos delante, o cuanto menos, ayuden en algo. La grafía es de alfabeto rúnico, si bien esta denominación, más que única, corresponde a un conjunto de alfabetos diversos más o menos similares que sirvieron de base para escribir lenguas germánicas durante la Edad Antigua y Media, siendo desplazadas poco a poco por las formas latinas a partir del siglo VIII. Las inscripciones más antiguas se remontan a la mitad del siglo II, habiendo persistido su uso hasta el siglo XX en algunas zonas rurales de Suecia. Tratando la diversidad de subfamilias, hemos de citar el futhark antiguo, que se desarrolló desde el siglo II hasta el IX. Entre tanto, en el siglo V surgió la variante anglosajona o futhorc, presente hasta el siglo XII. También, entre el siglo IX y el XII se desarrolló el futhark escandinavo, del que se derivarían las formas danesas, las sueco-noruegas, las islandesas, las de Hälsingland, las marcomanas, las medievales y las dalecarlianas (Arntz, 2007).

Sin entrar en los detalles de las variantes y considerando las más cercanas en su trazado a las de nuestro texto, hemos de quedarnos con seis posibilidades (Fig. 5). Recogemos cada uno de los signos del mensaje que estamos analizando y damos la transliteración entre corchete y el sonido fonético IFA correspondiente en los casos en que existe igualdad. En los que no existe igualdad damos la runa más cercana con sus opciones transliterada y fonética.

	futhark antiguo	futhorc anglosajón	futhark escandinavo	runas marcomanas	runas medievales	runas dalecarlianas
✚	X: [g], /g/ t: [n], /n/	X: [g], /g/ t: [n], /n/	[a], /a(:)/	[n], /n/	[æ], /ɛ/, /æ/	[a], /a(:)/
ᚠ		[k], /k/	[r], /r/, /r/		[y], /y/	[o], /o/
ᚡ					[t], /t/, /d/	[t], /t/, [e], /e/, [n], /n/
ᚢ	[t], /t/	[t], /t/	[t], [d] /t/, /d/	[t], /t/	[t], /t/, /d/	[y], /y/
ᚣ		[s], /s/	[s], /s/	[s], /s/	[s], /s/	[s], /s/, [c]
ᚤ		[k], /k/			[n], /n/	[n], /n/
ᚥ	[i], /i(:)/	[i], /i(:)/	[i], /i(:)/	[i], /i(:)/	[i], /i/, /j/, /e/	[s], /s/, [i], /i/
ᚦ			[k], /k/, [g], /g/	[ch]	[k], /k/, [g], /g/	[k], /k/, [y], /y/
ᚧ	[u], /u(:)/	[u], /u(:)/	[u], [o], /u(:)/, /v(:)/, /z(:)/, /w/	[r], /r/, [u], /u/	[u], /u/, /w/, /v/	[u], /u/
ᚨ	[l], /l/	[l], /l/	[l], /l/	[l], /l/	[l], /l/	[l], /l/
ᚩ						[b], /b/
ᚪ	[z], /z/	[z], /z/	[m], /m/	[y], /y/	[m], /m/	[m], /m/
ᚫ	ƿ: [f], /f/	ƿ: [f], /f/	ƿ: [f], /f/, [v], /v/	ƿ: [f], /f/	ƿ: [f], /f/, [v], /v/	[f], /f/
ᚬ	[a], /a(:)/	[æ], /æ(:)/	[a], /ä/, [o], /o(:)/	[a], /a(:)/		[f], /f/
ᚭ	[b], /b/	[b], /b/	[b], /b/, [p], /p/	[b], /b/	[b], /b/	[b], /b/
ᚮ			ƿ: [k], /k/, [g], /g/		ƿ: [k], /k/, [g], /g/	[k], /k/, [y], /y/
ᚯ						
ᚰ		/h/: [io], /jo/	/h/: [h], /h/	[k], /k/	/h/: [h], /h/	[m], /m/ /h/: [h], /h/, [ä]
ᚱ						
ᚲ				[s], /s/		
ᚳ						
ᚴ				[i], /i(:)/		
ᚵ						

FIGURA 5. Tabla de correspondencias de los elementos del mensaje con distintas subfamilias de runas.

A la vista de la (Fig. 5) no podemos decantarnos por una variante lingüística con claridad. Incluso la variante dalecarliana, que es la que más correspondencias tiene



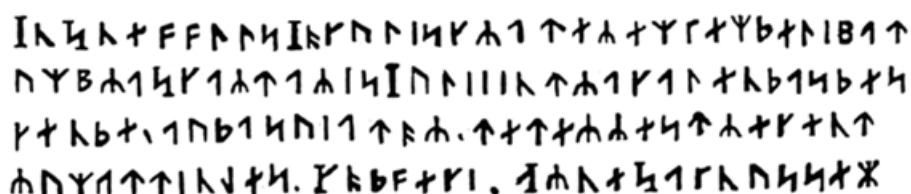


FIGURA 7. Más que posible recolocación del texto.

Volviendo a aplicar la transliteración con las diferentes posibilidades (Fig. 5) con esta nueva estructura no parece obtenerse ningún sentido dentro de las lenguas que les corresponderían, en especial las lenguas de la Familia Germánica, Subfamilia Septentrional, del Filo Indoeuropeo, como el islandés, danés, noruego, sueco o elfdaliano (o dalecarliano).

Con estos resultados podemos decir que nuestro texto ha sido sometido tanto a un cifrado de sustitución utilizando signos de aspecto rúnico, y además a un cifrado de transposición, con la colocación elemento a elemento en los distintos bloques y columnas junto con la lectura inversa. Queda por ver ahora la correspondencia de cada signo, de cada runa o pseudo-runa, con alguna determinada letra del lenguaje original del texto, que aún desconocemos.

De ahí que un siguiente cometido sea el análisis de frecuencias de los signos presentes, el cual suele ofrecer numerosas indicaciones de la lengua originaria, pues es un dato suficientemente ligado a cada lengua y mantenido diacrónicamente (Jara-Vera y Sánchez-Ávila, 2019). Calcularemos las dos opciones siguientes (Fig. 8), ambas sin tener en cuenta los signos que parecen ser puntos y comas, que tampoco son demasiados para alterar mucho los porcentajes: a) sin considerar los cuatro signos que parecen ser versiones mayúsculas; b) considerándolos y asimilándolos a sus posibles versiones minúsculas.

Los datos obtenidos son muy corrientes en multitud de lenguas, pudiendo inicialmente ceñirnos al ámbito Indoeuropeo o tal vez del Urálico, como Filos más probables, y más extraordinariamente, podríamos pensar en lenguas de los Filos Altaico o Caucásico. Por lo tanto, podemos suponer un cifrado de sustitución donde cada signo de las runas y pseudo-runas han sido tomados como reemplazos de un signo de un alfabeto, posiblemente un alfabeto latino.

Considerando los primeros 7 signos más habituales del texto, que suponen alrededor de algo más de la mitad del total del mismo, un 59,56 %, vamos a hacer las sustituciones con un conjunto amplio de lenguas, como son las siguientes: español, portugués, italiano, francés, inglés, alemán, holandés, danés, sueco, noruego, islandés, finés, húngaro, polaco, griego, latín y esperanto (Jara-Vera, 2016; ETA, 2021).

Al considerar los signos más habituales en las diversas lenguas que estamos considerando como hipótesis, la más repetida es una vocal, ya sea una “e” (ej.

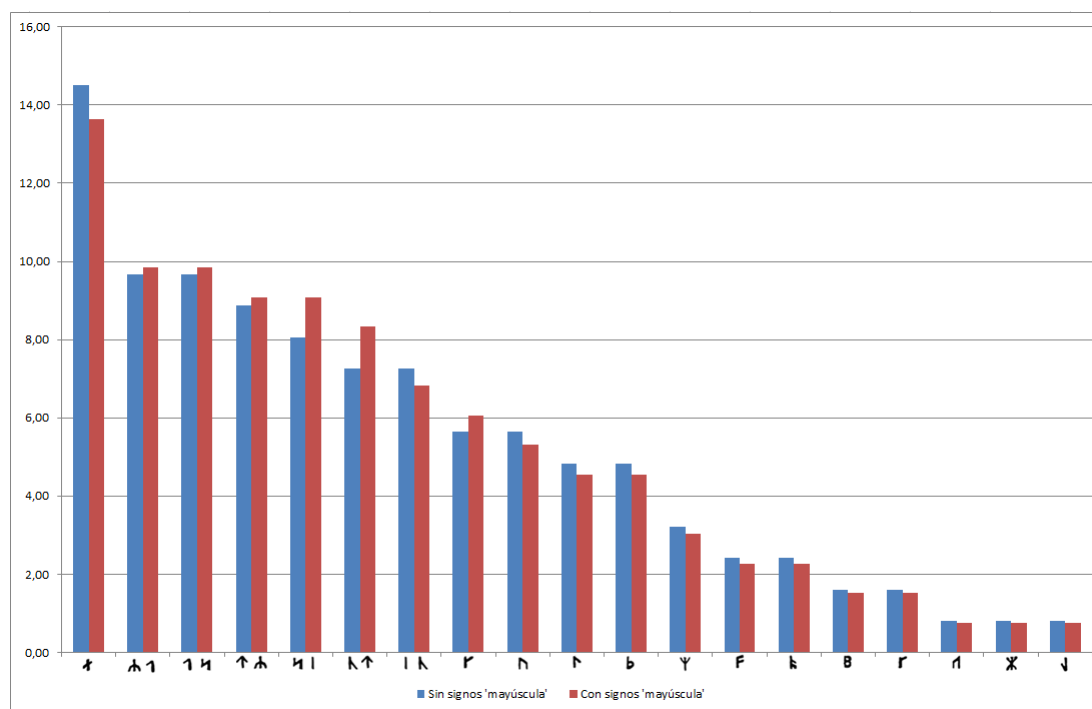


FIGURA 8. Frecuencias de los signos.

español), una “a” (ej. griego) o una “i” (ej. polaco). Viendo la (Fig. 5), este dato nos hace pensar como una posibilidad quizás elegida por el criptógrafo el darle al signo más repetido algunas de las opciones del futhark escandinavo, medieval o dalecarliano, lo que vendría a ser una letra como la “a” o la “e”, si bien podría haber tomado otra elección. También es habitual en las lenguas consideradas que el segundo signo más repetido o bien sea una vocal (ej. español) o bien “t” (ej. inglés), “n” (ej. danés), “s” (ej. francés), “r” (ej. noruego), lo que nos hace pensar, si es que hubiera tenido en cuenta valores transliterados, en el futhark escandinavo, el medieval o el dalecarliano. De igual forma, para la tercera letra más repetida podemos también quedarnos con letras que tenemos en la (Fig. 5), como son “e”, “t”, “n”, que encontramos en esas posiciones en varias lenguas, como el esperanto, húngaro o sueco, respectivamente.

Con este procedimiento podemos pensar en la hipótesis de la transliteración de los diversos signos, y con ello, considerando los siete más habituales, probaremos las siguientes opciones:

$$(a/e) - (r/y/o) - (e/t/n) - (t/d/y) - (s) - (k/n) - (i/j/s)$$

Por otro lado, debido a la presencia de la letra “a” en las lenguas que estamos considerando en los primeros lugares por su elevada frecuencia, también consideraremos en todos los lugares su posible existencia como opción posible.

Al realizar las diversas sustituciones hay en concreto una que parece ofrecer una cierta presencia de significado: e-r-a-t-s-n-i. Y que en gran parte parece acercarse a la (Fig. 5). La recogemos en la (Fig. 9).

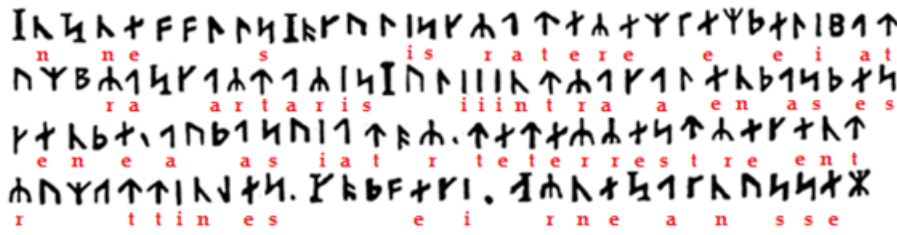


FIGURA 9. Primera aproximación a la solución, con 7 letras (minúsculas).

En la 3ª fila podemos suponer la palabra “terrestre”, que tenemos en el español. Si añadimos tres de los signos que suponemos ser formas mayúsculas, y les damos los posibles valores de sus formas minúsculas consideradas, “a”, “s”, “i”, tendríamos:

*InSne - - - - sI - - - - is - ratere - - e - - e - i - at*  
*- - - raS - artarisI - - iintra - a - en - as - es*  
*- en - e - a - - as - iat - r - teterrestre - ent*  
*r - - - ttin - es - - - - e - i - ArneSa - n - sse -*

No obstante, la posibilidad de la escritura en español se desvanece por la presencia de otras formas ajenas que podemos ver. Pero parece ser acertada la suposición de considerar la transliteración de los signos. Incluso podemos añadir alguno más del conjunto de las runas de la (Fig. 5) que sea el mismo en todas las variantes y que no sea una opción posible para varios signos, como es el caso de la “l”:

*InSne - - llsI - - - lis - ratere - - e - - eli - at*  
*- - - raS - artarisI - liintra - alen - as - es*  
*- en - e - a - - as - iat - r - teterrestre - ent*  
*r - - - ttin - es - - - - e - i - ArneSa - n - sse -*

El texto parece ir cobrando sentido, si bien no es sencillo, apareciendo también secuencias extrañas como “iii”. Aún está pendiente conocer la lengua origen del texto, mientras que la posibilidad de que fuera español ha desaparecido. Por otro lado, la última línea, tras lo que parece realmente un punto, parece mencionar, al suponer una mayúscula inicial, *Arne Sa...*, lo cual nos lleva a pensar en una firma final, un nombre y un apellido, o un título, siendo *Arne* un nombre masculino habitual escandinavo, coherente además con el uso de las runas.

Todo lo anterior parece confirmar los signos en mayúscula y el uso de puntos y comas. Lo cual, por otro lado, no es una buena práctica porque facilita la labor al criptoanalista que desee conocer el texto de manera no autorizada. Con ello, si vamos a la primera línea en el inicio, tendríamos el comienzo *In Sne...* lo

que nos acerca a lenguas como el inglés, pero que descartamos por la aparición de la expresión *terrestre*, llevándonos a pensar en el latín, que sí tiene la forma “terrestris/terrestre”, y además la preposición “in”.

Veamos a continuación las frecuencias de la lengua latina. Para ello tomaremos en consideración el análisis de diversas obras, en concreto diez, a saber, una sátira de Juvenal, fragmentos de la “Vulgata” del evangelio de san Lucas, también de “Confesiones” de san Agustín, poemas de Venancio Fortunato, de “Etimologías” de san Isidoro, del “Carmina Burana”, de himnos de Pedro Abelardo, de un sermón de san Antonio de Padua, así como algunos textos de la “Summa de Teología” de santo Tomás de Aquino, junto a algunos versos de Petrarca (Jara-Vera, 2016), lo cual nos da un abanico de obras en prosa y en verso desde el siglo I hasta el XIV (Fig. 10).

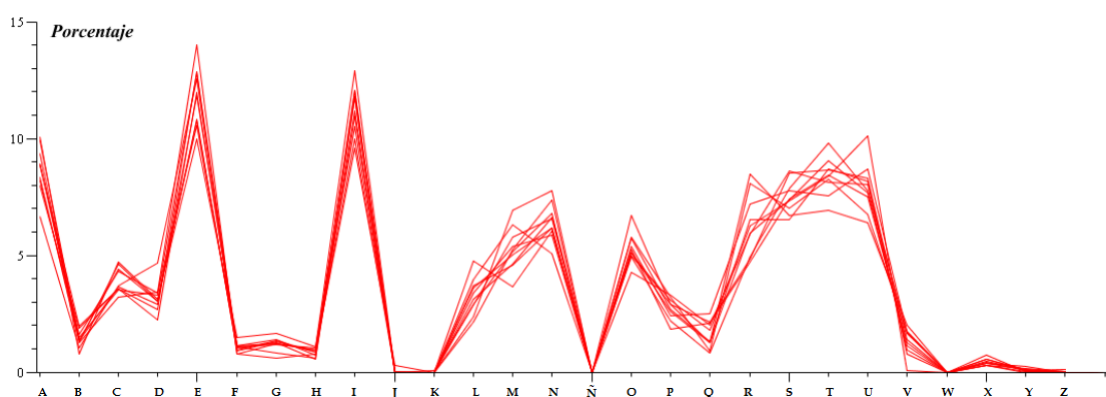


FIGURA 10. Frecuencias de las letras en la lengua latina.

La solución última dada para el mensaje cifrado, a pesar de que el texto no sea muy extenso, arroja una cierta coherencia con las frecuencias latinas. Así, hemos colocado numerosas letras de entre las más frecuentes: *e-a-s-r-i-t-n-\*-l\**, con una presencia de 18-13-13-12-12-11-9-8-7-6-6.

Echamos en falta, viendo las frecuencias latinas, la necesidad de localizar los valores “m”, “u”, “o” en nuestro texto, siendo valores con esperada presencia. Podemos suponer que se encuentran en los lugares que hemos marcado con asteriscos en la secuencia previa, y que corresponden a los signos rúnicos pendientes (Fig. 11).

ʀ    ʀ    ʀ

FIGURA 11. Tres signos a los que buscar su significado.

Considerando la (Fig. 11), la suposición de que el signo situado a la izquierda sea una “m” no parece tener sentido al sustituirse, generándose expresiones absurdas,

como "lismratere". Lo mismo si suponemos los valores "u" y "o". Tampoco parece que el signo de la derecha encaje con ninguna de las opciones "m", "u", "o", mirando por ejemplo, la secuencia "alen\*as\*es". Para el signo central encontramos que el valor "u" ofrece altas posibilidades, quedándonos el siguiente texto, (Fig. 12), que mostramos con los signos originales.

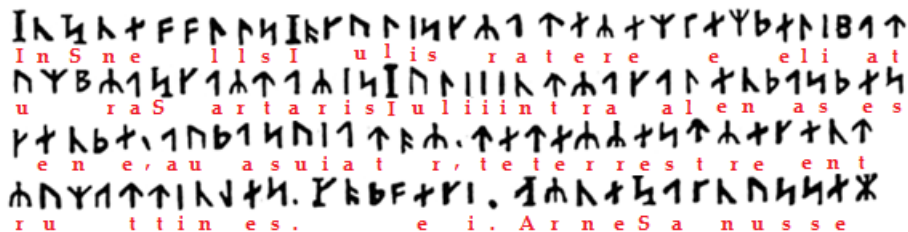


FIGURA 12. Solución parcial con 9 letras.

Centrémonos ahora en el signo situado a la izquierda de la (Fig. 11), con 7+1 apariciones (minúsculas+mayúscula) en el texto. Mirando las frecuencias de la lengua latina, y eliminando las opciones colocadas y las que hemos descartado para él, podemos pensar en "p" y en "c". Es claro al hacer algunas sustituciones que el valor que ofrece varios sentidos en el texto es "c". Además, esto es coherente con la (Fig. 5), donde una de las opciones era el valor "k". El texto queda de esta forma:

*InSne - - llsI - culiscratere - - e - - eli - at  
 u - - raScartarisIuliiintracalen - as - es  
 cen - e, au - asuiat - r, teterrestrecent  
 ru - - ttin - es. C - - - eci. ArneSa - nusse -*

Para el signo situado en la derecha (Fig. 11), la letra más inmediata viendo la (Fig. 5) de runas y pseudo-runas es la "b", pero no obtenemos un sentido claro con esta asignación. También parece que no corresponde a un valor vocálico, sino consonántico. Viendo las letras que nos quedan pendientes y su no escasa frecuencia parece encajar con "d", llegando al mensaje mostrado en (Fig. 13).

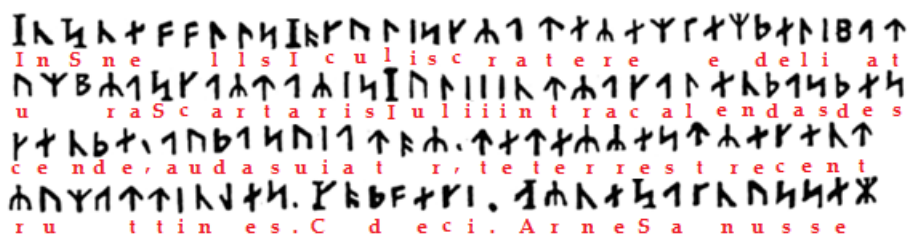


FIGURA 13. Solución parcial con 11 letras.

Ya es fácil darse cuenta por el sentido que tenemos las palabras "descende, audas viator", lo que nos indica que en ocasiones el valor "u" hace las veces de "u" o de



“v”, lo cual es propio del latín, además de resolver el valor para el tercero de los signos de la (Fig. 14) al que le asignamos la “o”, por otro lado coherente con la variedad futhark escandinava.



FIGURA 14. Cinco signos a los que buscar su significado.

Además, tenemos en el lenguaje latino algunas letras que deberían de aparecer (Fig. 10): en especial “m” y “p”, con porcentajes no del todo escasos, en torno al 5%-3%; con en torno al 1% podemos esperar los valores “b”, “f”, “g”, “h”, “q”. Viendo además la (Fig. 5) podemos hacer las suposiciones siguientes para la (Fig. 14): pensar en “m” para el primero o el quinto de los signos; “f” para el segundo; “p” para el cuarto. Al ir sustituyendo podemos comprobar que son adecuadas las suposiciones excepto para el caso de “p”, que no parece ser correcto. Por otro lado, para la “m” es llamativo que corresponda bien para ambos signos, el primero y el quinto. Otra opción, y por el doblado de signo, arriba y abajo, frente al primero, es suponer que el quinto corresponda al valor “mm”. El texto quedaría así:

*InSneffllsIoculiscraterem - emdeli - at  
um - raScartarisIuliiintracalendasdes  
cende, audasuiator, teterrestrecent  
rum - ttin - es. Codfeci. ArneSa - nussem*

En este momento podemos intentar para el cuarto de los signos de la (Fig. 14) el que la (Fig. 5) ofrecía también, el valor “b”, lo cual parecer ser correcto.



FIGURA 15. Dos signos parecidos.

Hay dos signos parecidos, uno de los cuales ya resuelto (Fig. 15), el de la derecha, con valor “c”. Para el otro, el de la izquierda, intentando las opciones “k”, “g”, “y”, presentes en la lista de la (Fig. 5), vemos que parece ser el valor “k”, cercano al valor “c”, dado al otro signo tan parecido a él, por lo que fonéticamente tienen una gran semejanza. No obstante, mirando el mensaje, todo es algo más confuso y no tan sencillo, pues el signo de la derecha en ocasiones obliga a “c”, como en “craterem”, pero en otras a “qu”, como parece sugerir su forma mayúscula en “Cod feci”, debiendo ser en latín “Quod feci”. Esto hace que el signo a la izquierda de la (Fig. 15), que tenemos en dos ocasiones en el texto, en una sea “k”, para “Saknussem”, más propio de las lenguas escandinavas, y en otra sea “qu”, para “quem”.

Así, llegamos al texto siguiente, que permite entender el llamativo "iii", y donde podemos ver que hay un error con la preposición "te" en "...te terrestre", debiendo decir "et terrestre":

*In Snefflls Ioculis craterem quem delibat  
umbra Scartaris Iulii intra calendas des  
cende, audas viator, te [=et] terrestre cent  
rum - ttin - es. Quod feci. Arne Saknussem*

¿A qué corresponden los dos extraños signos de la (Fig. 16), pseudo-runas pendientes, que en la (Fig. 5) no concuerdan con runas reales existentes? ¿Acaso con alguno de los valores no utilizados como "g", "h", "p", "x", "y", "z"? No parece ser el caso para el primero de ellos, que parece pedir una vocal, si bien para el segundo podemos pensar en la forma latina "-ttinges", y por lo tanto en una "g", forma verbal que tenemos en "atingo, attigi, attactum", que significa "alcanzar, tocar ligeramente", y nos da la vocal "a" para el primero.



FIGURA 16. Últimos signos pseudo-runas.

Indicar además que la palabra latina "audas" corresponde más concretamente a "audax", habiéndose así sustituido tanto la "s" como la "x" por el mismo signo, lo cual es un caso extraño en Criptografía, por llevar a dificultades de recuperar el texto original, si bien solo se ha usado en esta ocasión y con letras cercanas fonéticamente. De esta forma, el texto queda tal y como recoge la (Fig. 17).

*I n S n e f f l l s I o c u l i s c r a t e r e m q u e m d e l i b a t  
u m b r a S c a r t a r i s I u l i i i n t r a c a l e n d a s d e s  
c e n d e , a u d a s / x u / v i a t o r , t e t e r r e s t r e c e n t  
r u m a t t i n g e s . Q u o d f e c i . A r n e S a k n u s s e m m*

FIGURA 17. Solución del mensaje.

Sin entrar en detalles de traducción, podemos reconocer la forma vocativa de "audax viator" con la coma precedente, el verbo al final, "descende", en presente de imperativo, necesitando de un acusativo, que encontramos en "craterem", el cual lleva una oración subordinada relativa con el mismo caso en "quem", la cual tiene un verbo en presente de indicativo ligado al complemento temporal "Iuliis intra calendas", donde "intra" adquiere un significado de "antes de", en lugar del habitual "dentro de", por la razón de referirse a una medida de tiempo, las calendas

o primer día de mes; además, tenemos el complemento de lugar con la preposición “in” para “Snefflls Iouculis”; seguida de una coma tenemos una oración unida por la conjunción copulativa “et” y un verbo en futuro imperfecto de indicativo, “attinges”. Finalizando el texto tenemos en “Quod feci. Arne Saknussem” un falso relativo, debido a la presencia del punto, que separa ambas sentencias y rompe la subordinación; así “quod” adquiere el sentido de pronombre anafórico “is/ea/id”, y se refiere a la frase precedente, y el verbo es un pretérito perfecto de indicativo en 1ª persona del singular. De esta forma el mensaje,

*In Snefflls Ioculis craterem quem delibat umbra Scartaris Iulii  
intra calendas descende, audas[=x] viator, te [=et] terrestre centrum attinges.  
Quod feci. Arne Saknussem*

tendría como traducción ajustada desde el latín al español:

*Audaz viajero, descende el cráter que la sombra del Scartaris roza  
antes del 1 de julio en el Snefflls Ioculis, y alcanzarás el centro de la tierra.  
Lo cual he hecho. Arne Saknussem*

En la novela las cosas son más sencillas: primeramente se toma algunas licencias suponiendo que es rúnico islandés y con ello el sabio profesor Lidenbrock copia de manera directa las letras latinas. Por otro lado, revisando el antiguo libro donde estaba el pergamino encuentra en un margen escrito el nombre “Arne Saknussem” con los mismos símbolos rúnicos. Junto a ello, de manera inmediata supone que el texto está escrito en latín, por ser la lengua culta por antonomasia. A partir de aquí, de forma sencilla acabarán, tanto él como su sobrino, ordenándolo y leyéndolo de manera inversa (Fig. 18).

*In Sneffels Yoculis craterem kem delibat  
umbra Scartaris Iulii intra calendas descende,  
audas viator, et terrestre centrum attinges.  
Kod feci. Arne Saknussem.*

*Descends dans le cratère du Yocul de  
Sneffels que l'ombre du Scartaris vient  
caresser avant les calendes de Juillet,  
voyageur audacieux, et tu parviendras  
au centre de la Terre. Ce que j'ai fait.  
Arne Saknussem.*

FIGURA 18. Solución al texto en latín y francés (publicación original de la novela (Verne, 1864)).

Como podemos ver al comparar la solución obtenida con la dada por Verne (Fig. 18) hay algunos errores y diferencias, pues en lugar de “Snefflls” aparece

"Sneffles", cambiando una "l" por una "e". También el cambio de "I" por "Y" desde "Ioculis" a "Yoculis", si bien comprensible por la similitud fonética. También el error ya mencionado de "te" por "et". Junto a ello, mencionar la inexistencia de la palabra "Ioculis", que proviene de una voz islandesa, "Jökull", con significado de "glaciar", y que suele formar parte sufixa de muchos picos de la región, y que Verne traduce como "ventisquero" (Lexilogos, 2021). Así, el nombre en islandés es "Snæfellsjökull", que es verdaderamente un volcán islandés. Indicar que "Scartaris" no es un pico o monte existente, sino que parece una invención de Verne. No obstante, Arne Saknussemm está basado en el del erudito islandés Árne Magnússon (1663-1730) (Margot, 1980).

**2.2. Algunas formalizaciones.** Demos algunas definiciones algo más formales de los tipos de cifrados que acabamos de criptoanalizar.

Sea  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  un criptosistema, formado por el conjunto de textos en claro  $\mathcal{P}$ , textos cifrados  $\mathcal{C}$ , espacio de claves  $\mathcal{K}$ , así como las operaciones de cifrado  $\mathcal{E}$  y descifrado  $\mathcal{D}$ .

En general  $\mathcal{P} = \mathcal{C}$ , habiendo previamente un alfabeto, más o menos amplio,

$$L = \{A, B, C, \dots, Z, a, b, \dots, z, 0, \dots, 9, \dots\},$$

incluso con algunos signos de puntuación o no, con cardinal  $\#L = m$ , capaz de constituir los diferentes elementos de  $\mathcal{P}$  y  $\mathcal{C}$ . En nuestro caso

$$L_1 = \{A, B, \dots, G, I, K, \dots, N, O, \dots, U, V, X, Z, a, b, \dots, g, i, k, \dots, n, o, \dots, u, v, x, z, \dots\},$$

con  $\#L_1 = 46$ , suponiendo un alfabeto latino de 22 letras, además del punto y la coma.

Para el caso de las runas hemos encontrado una asignación para las letras como la que mostramos en la (Fig. 19). No sabemos si hay más casos como el de la forma doble "mm". Suponiendo que no, y echando en falta las asignaciones "p" y "z", que suponemos que existan, tendríamos 21 signos para las minúsculas, con otros tantos para las mayúsculas, y al menos dos valores más para la coma y el punto, resultando así un cardinal, si no hay más elementos, de  $\#L_2 = 44$ .

En los cifrados simétricos tanto la operación de cifrado  $e$  como de descifrado  $d$  hacen uso de una misma clave  $k$ . En los cifrados asimétricos no son iguales dichas claves si bien están relacionadas matemáticamente entre sí. Con ello, de manera general tendríamos:

$$e_k : \mathcal{P} \rightarrow \mathcal{C},$$

$$d_k' : \mathcal{C} \rightarrow \mathcal{P},$$

a	ᚦ ᚧ	g	ᚩ	n	ᚲ	t	ᚱ
b	ᚷ	i	ᚪ	o	ᚫ	u	ᚱ
c	ᚦ	k	ᚦ	p	ᚇ?	v	ᚱ
d	ᚷ	l	ᚦ	q[u]	ᚦ ᚷ (mayúsc.)	x	ᚱ
e	ᚦ	m	ᚷ	r	ᚱ	z	ᚇ?
f	ᚷ	mm	ᚷ	s	ᚱ		

FIGURA 19. Asignación de las runas y pseudo-runas (solo minúsculas, con una excepción).

de tal forma que

$$d_{k'}(e_k(x)) = x, \forall x \in \mathcal{P}, k, k' \in \mathcal{K}, e \in \mathcal{E}, d \in \mathcal{D}.$$

2.2.1. *Cifrados de sustitución y de permutación.* Vayamos, dicho lo anterior, a formalizar los cifrados que hemos encontrado en nuestro texto. Hemos tenido tanto un cifrado de sustitución, donde las letras latinas eran sustituidas por runas o pseudo-runas, y dos cifrados de permutación o transposición, donde las letras eran cambiadas de lugar o de posición, por un lado, escribiendo el texto original al revés, de atrás hacia adelante, y por otro lado, colocando en la estructura tabulada de tres columnas y siete filas (Fig. 4) una letra tras otra en cada posición. Podemos intercambiarlos entre sí, procediendo primero con la sustitución y luego con las permutaciones o al revés. Quizás lo más cómodo en el procedimiento sea empezar con la transposición que construye el texto en sentido inverso, seguir con la que lo coloca en la estructura de columnas y filas, y finalmente hacer la sustitución de las letras por signos rúnicos.

De manera general la transposición no es sino una permutación algebraica, que podemos expresar del modo conocido:

$$(2.1) \quad e_{\pi}(x_1, x_2, \dots, x_n) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}),$$

para el caso de un mensaje de longitud  $n$ , siendo la función una biyección, y que en el caso de aplicarse monográficamente sobre un texto de longitud  $n$  la podemos expresar como

$$\mathcal{P}_n^{(1)} \leftrightarrow \mathcal{C}_n^{(1)},$$

donde para nuestro ejemplo  $\mathcal{P} = \mathcal{C}$  y el alfabeto es  $L_1$ .

En el caso de la permutación consistente en escribir el texto en sentido inverso,  $\pi_1$ , tendríamos que (2.1) debe de cumplir que  $\forall i \in \{1, 2, \dots, n\}$ :

$$\pi_1(i) : n + 1 - i,$$

es decir,

$$e_{\pi_1}(x_1, x_2, \dots, x_n) = (x_n, x_{n-1}, \dots, x_1),$$

donde  $n = 136$ ,  $\mathcal{P} = \mathcal{C}$  y el alfabeto es  $L_1$ .

Para el segundo cifrado de transposición, que coloca el actual texto en la estructura de columnas y filas (Fig. 4), transposición más compleja de formalizar, podemos expresarla, haciendo una lectura de arriba hacia abajo, y de izquierda a derecha, donde la ecuación (2.1) se expresa para todo  $i \in \{1, 2, \dots, n\}$ , con  $n = 136$ , como

$$\pi_2(i) : \left( \left\lfloor \frac{i+71}{71} \right\rfloor \pmod{2} \right) \left\lfloor \frac{i+6}{7} \right\rfloor + \left\lfloor \frac{i}{71} \right\rfloor \left\lfloor \frac{i-5}{6} \right\rfloor + 21 \left( i - \left( \left\lfloor \frac{i+71}{71} \right\rfloor \pmod{2} \right) (7 \left\lfloor \frac{i-1}{7} \right\rfloor + 1) + \left\lfloor \frac{i}{71} \right\rfloor (6 \left\lfloor \frac{i-71}{6} \right\rfloor + 71) \right),$$

quedando expresado en algunos pocos términos de la siguiente forma:

$$e_{\pi_2}(x_1, x_2, x_3, \dots, x_8, x_9, \dots, x_{135}, x_{136}) = (x_1, x_{22}, x_{43}, \dots, x_2, x_{23}, \dots, x_{105}, x_{126}),$$

así como gráficamente en todos sus valores en la (Fig. 20).

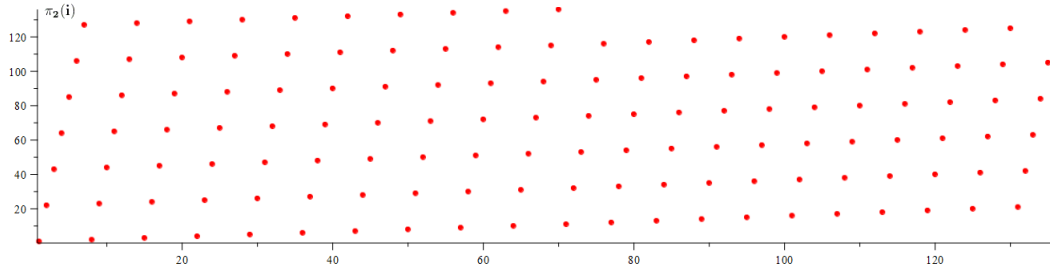


FIGURA 20. Función  $\pi_2(i)$ .

Sus funciones inversas de descifrado son respectivamente  $d_{\pi_1^{-1}}$  y  $d_{\pi_2^{-1}}$ , donde  $\pi_1^{-1}(i) = \pi_1(i)$  y

$$\pi_2^{-1}(i) : \left\lfloor \frac{i+20}{21} \right\rfloor + 6 \left( (i-1) \pmod{21} - 10 \right) \left\lfloor \frac{(i-1) \pmod{21} + 1}{12} \right\rfloor + 7 \left( 11 \left\lfloor \frac{(i-1) \pmod{21} + 1}{12} \right\rfloor + \left( (i-1) \pmod{21} + 1 \right) \left( \left\lfloor \frac{((i-1) \pmod{21}) + 13}{12} \right\rfloor \pmod{2} - 1 \right) \right),$$

con

$$d_{\pi_1^{-1}}(x_1, x_2, \dots, x_n) = (x_n, x_{n-1}, \dots, x_1)$$

$$d_{\pi_2^{-1}}(x_1, x_2, x_3, \dots, x_8, x_9, \dots, x_{135}, x_{136}) = (x_1, x_8, x_{15}, \dots, x_{50}, x_{57}, \dots, x_{63}, x_{70}),$$

siendo la representación gráfica de valores para esta última transposición la mostrada en la (Fig. 21).

En cuanto a la sustitución tendríamos

$$\sigma : \mathcal{P}_n^{(1,2)} \rightarrow \mathcal{C}_n^{(1)},$$

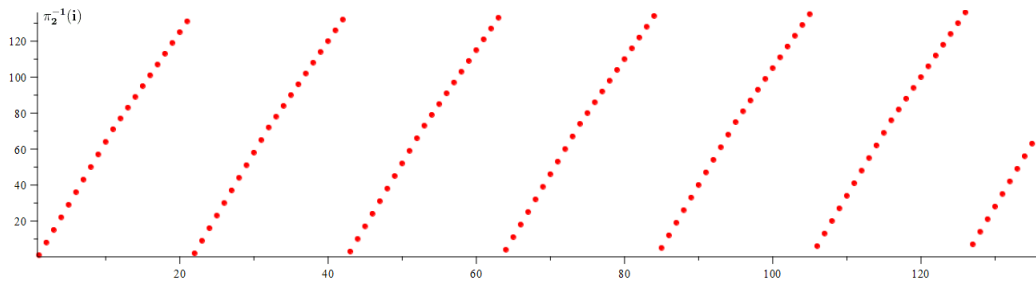


FIGURA 21. Función  $\pi_2^{-1}(i)$ .

donde  $\mathcal{P} \neq \mathcal{C}$ , al ser el conjunto de sustitución  $\mathcal{C}$  el de runas y pseudo-runas, con su alfabeto  $L_2$ , diferente al inicial de letras de grafía latina,  $L_1$ .

Tal y como vimos en nuestro criptoanálisis nuestro texto no ha sido una biyección ni tampoco ha sido incluso una función (Fig. 19). En la mayoría de las ocasiones, es verdad que un elemento del conjunto origen ha sido sustituido siempre por un elemento, el mismo, del conjunto destino; pero en otras, ha habido más de una opción, como en el caso de “a”; o bien en otros casos, dos elementos diferentes como “s” y “x” han tenido la misma imagen; e igualmente a “k” (monograma) y a “qu” (bigrama) se les ha asignado la misma imagen. Y como hemos acabado de mencionar, no solo con una asignación monográfica, sino en ocasiones poligráfica: tomándose del conjunto origen uno, o más raramente dos elementos, pero solo uno siempre del conjunto destino, como ocurre con el caso “mm” o el antes mencionado “qu”. Todo lo dicho lleva a que nuestra relación no sea una función, permitiendo la Criptografía relaciones y asignaciones altamente elaboradas, en muchos casos muy complejas para dificultar el ataque criptoanalítico, dejando ciertas ambigüedades que pudieran darse en las asignaciones a la posterior resolución con apoyo de las redundancias del lenguaje y el conjunto finito de las palabras posibles de la lengua.

Con todas las funciones de cifrado y descifrado definidas, tendríamos las composiciones

$$P_1 \xrightarrow{e_{\pi_1}} P_1 \xrightarrow{e_{\pi_2}} P_1 \xrightarrow{e_{\sigma}} C_2$$

$$C_2 \xrightarrow{d_{\sigma^{-1}}} P_1 \xrightarrow{d_{\pi_2^{-1}}} P_1 \xrightarrow{d_{\pi_1^{-1}}} P_1$$

donde los subíndices de los conjuntos indican los alfabetos a los que pertenecen,  $L_1$  o  $L_2$ .

Otro aspecto que queremos resaltar es la escasa longitud del texto, incluso con presencia de palabras ajenas a la lengua en la que está escrito, el latín, como “Snefflls”, “Ioculis”, “Scartaris” o “Arne Saknussem”, que llevan a variar las frecuencias esperadas de las letras del idioma, dificultando un ataque de frecuencias.

Hay una pregunta que antes de finalizar deberíamos responder. Se trata de saber si nuestra solución es la correcta, si es única o hay alguna otra más que pueda obtenerse del texto cifrado original. Para atender a este asunto se define la Distancia de Unicidad,

$$D_U = \frac{H(\mathcal{K})}{D},$$

cociente entre la Entropía del espacio de claves y la Redundancia del lenguaje. Esta última,  $D = R - r$ , es la diferencia entre el Ratio Absoluta del lenguaje y la Ratio Real (Guerrero, 2009; Shannon, 1950, 1951).

Considerando que en ambas transposiciones operamos sobre  $L_1$  y que en la sustitución es también éste nuestro lenguaje del conjunto origen, tendríamos un total de 46 valores, si consideramos distintos los signos mayúscula y minúscula junto a los signos de puntuación. Con ello y a partir de la definición de  $R = \log_2(\#L)$ , obtendríamos  $R = 5,523$ . En lenguajes como las lenguas romances tenemos una Ratio Real en el rango  $1,2 \leq r \leq 1,5$ . Así los valores obtenidos para la Redundancia estarían en el rango  $4,323 \leq D \leq 4,023$ , que podemos ponderar como  $D = 4,173$ .

Calculemos ahora la entropía del espacio de claves. Tengamos en cuenta que la composición de los dos cifrados de transposición es otro cifrado de transposición. El cálculo consistirá en toda las permutaciones posibles, es decir,

$$\log_2 \left( \frac{136!}{18!12!12!11!10!9!9!7!7!6!6!4!3!3!2!2!1!1!1!3!1!3!1!2!2!} \right),$$

y la Distancia de Unicidad final es de 123,626 caracteres.

Para el caso de un cifrado de sustitución monográfica monoalfabeto  $H(\mathcal{K})$  viene dado como  $\log_2(\#L_1!)$ , resultando un valor de 45,964. No obstante, nuestro cifrado de sustitución tenía en un par de ocasiones bigramas con "mm" o "qu", o una doble asignación para la "a", o la misma para la "s" y la "x", o la "k", la "c" y la "qu". No parece que haya más, pues son las que podríamos esperar por los parecidos fonéticos, por lo que podríamos aumentar el anterior valor ligeramente, sin entrar en más afinados cálculos, pongamos por caso,  $\log_2((\#L_1 + 5)!) = 52,691$ . Todo ello sin necesidad de suponer más parejas ni otras posibilidades de relaciones entre conjunto origen y destino.

Considerando finalmente la suma de ambas distancias de unicidad, las de transposición y de sustitución, tendríamos un valor total de 176,317 caracteres. Como nuestro texto tiene 136 signos, un valor menor que el obtenido de unos 176 o 177 caracteres, no tenemos unicidad. Podría por lo tanto haber otra transposición distinta a las obtenidas (conjuntamente) y otra sustitución que desde el texto cifrado diera un mensaje con sentido. No obstante, la coherencia de la sustitución encontrada con las runas diversas, así como las dos transposiciones, una inversa y otra según la colocación ordenada y secuencial en la tabla por el patrón percibido, parece



indicar claramente que la solución encontrada sí es la correcta y la que generó el mensaje.

Para finalizar, y más en un artículo orientado al ámbito docente y educativo, mencionar la necesidad de un cierto conocimiento, a veces profundo y no solo somero, de la lengua origen del texto mensaje, en este caso el latín, lengua clásica por antonomasia, para poder ir adivinando las palabras que puedan ir apareciendo en sílabas y pequeños fragmentos. Cuánto más en casos como este donde hay varias opciones para un mismo signo, e incluso errores (tal vez intencionados para complicar el descifrado) en la generación del texto.

### §3. Comentarios finales

No hemos querido decir apenas nada más del argumento de esta novela, ni del resto que hemos mencionado al inicio, todas ellas muy recomendables y entretenidas, al tiempo que permiten apreciar el interés por los mensajes secretos en multitud de autores de aventuras y misterio, llevando al lector a participar de la intriga intentando descifrarlos por su cuenta, lo que aquí hemos expuesto de forma detallada para la novela "Viaje al centro de la Tierra".

Leamos, o incluso releamos, algunas de estas obras tras haber dejado la adolescencia ya hace tiempo pero esta vez con ojos más agudos e interés científico-humanístico, para indagar con perspicacia, como ocurre con Julio Verne, la amplia variedad de conocimientos en diversas disciplinas que salpican sus obras, desde la matemática, pasando por las diversas ingenierías, a la geografía, la botánica, o la lingüística.

En lo que a nuestra especialidad se refiere, la Matemática Aplicada en Criptografía, creemos que puede ser muy sugerente iniciar a los más jóvenes en esta disciplina con este tipo de ejemplos, no tan ingenuos ni sencillos, sino incluso arduos, y potencialmente muy motivadores y efectivos para introducir diversidad de conceptos y métodos de esta área en los procesos educativos, al tiempo que se les ofrece un marco intelectual integral amplio en muchas otras materias del conocimiento.

### Contribuciones

Conceptualización: VJV. Metodología: VJV. Investigación: VJV. Supervisión: VJV, CSA. Validación: VJV, CSA. Escribió el artículo: VJV.

### Bibliografía

- Arntz, H. (2007). *Handbuch der Runenkunde*. Leipzig, Deutschland: Lempertz.  
Bauer, F. L. (2007). *Decrypted Secrets: Methods and Maxims of Cryptology*. Berlin, Deutschland: Springer.

- Doyle, A. C. (1893). *The Memoirs of Sherlock Holmes*. London, England: George Newnes.
- Doyle, A. C. (1905). *The Dancing Men*. London, England: George Newnes.
- Doyle, A. C. (1915). *The Valley of Fear*. New York, United States of America: George H. Doran Company.
- ETA. (2021). *LetterFrequency.org*. Descargado de <http://letterfrequency.org/letter-frequency-by-language/>
- Friedman, W. F. (1987). *The Index of Coincidence and its Applications in Cryptanalysis*. Laguna Hills (CA), United States of America: Aegean Park Press.
- Guerrero, F. G. (2009). A New Look at the Classical Entropy of Written English. *Transactions on Information Theory*, 1–15.
- Jara-Vera, V. (2016). *Contexto, Criptoanálisis y propuesta de solución de la inscripción de la talla (original) de la Virgen de Candelaria de Tenerife (Canarias, España)* (Tesis Doctoral no publicada). ETSIT, Universidad Politécnica de Madrid, Madrid, España.
- Jara-Vera, V., y Sánchez-Ávila, C. (2019). Graphemic-phonetic Diachronic Linguistic Invariance of the Frequency and of the Index of Coincidence as Cryptanalytic Tools. *Plos One*, 14(3), 1–31.
- Jara-Vera, V., y Sánchez-Ávila, C. (2021). Some Notes on a Formal Algebraic Structure of Cryptology. *Mathematics*, 9(2183), 1–28. Descargado de <https://doi.org/10.3390/math9182183>
- Kahn, D. (1996). *The Code-breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York, United States of America: Scribner.
- Lexilogos. (2021). *Icelandic Dictionary*. Descargado de [https://www.lexilogos.com/english/icelandic\\_dictionary.htm](https://www.lexilogos.com/english/icelandic_dictionary.htm)
- Margot, J. M. (1980). Comment se Documentait Jules Verne. *Bulletin de l'Association Bibliothécaires Genevoise*, 4, 5–12.
- Poe, E. A. (1843). The Gold-Bug. *Dollar Newspaper*, 28 de junio, 1–4.
- Shannon, C. E. (1950). The Redundancy of English. *Cybernetics*, 248–272.
- Shannon, C. E. (1951). Prediction and Entropy of Printed English. *Bell System Technical Journal*, 30(50), 47–51.
- Vargas-Llosa, M. (1971). *García Márquez: historia de un deicidio*. Barcelona, España: Seix Barral.
- Verne, J. (1864). *Voyage au Centre de la Terre*. Paris: France: Pierre-Jules Hetzel.
- Verne, J. (1868). *Les Enfants du Capitaine Grant*. Paris: France: Pierre-Jules Hetzel.
- Verne, J. (1881). *La Jangada*. Paris: France: Pierre-Jules Hetzel.
- Verne, J. (1885). *Mathias Sandorf*. Paris: France: Pierre-Jules Hetzel.

VICENTE JARA-VERA

*Dpto. de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones.*

*ETS de Ingenieros de Telecomunicación.*

*Universidad Politécnica de Madrid (España)*

(✉) [vicente.jara@upm.es](mailto:vicente.jara@upm.es)

CARMEN SÁNCHEZ-ÁVILA

*Dpto. de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones.*

*ETS de Ingenieros de Telecomunicación.*

*Universidad Politécnica de Madrid (España)*

(✉) [carmen.sanchez.avila@upm.es](mailto:carmen.sanchez.avila@upm.es)

---

Recibido: 7 de agosto de 2021.

Aceptado: 17 de julio de 2022.

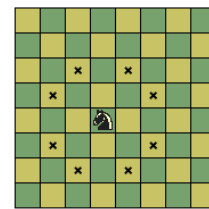
Publicado en línea: 6 de setiembre de 2022.

---

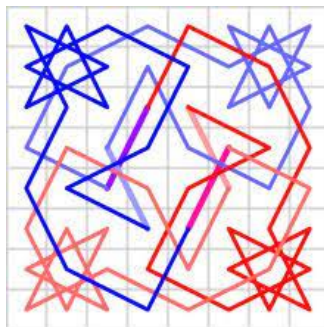
se puede ir de un número racional cualquiera a otro con saltos de un caballo de ajedrez?

Pues es posible, pero primero tenemos que precisar qué entendemos por ¡movidas de caballo entre números!

Como casi todos saben, el ajedrez es un juego de estrategia que se juega en un tablero de  $8 \times 8$  casillas. Una de sus piezas es el *caballo* que tiene un curioso movimiento en forma de L y que además puede saltar a piezas propias y rivales. Más precisamente, para moverse, el caballo avanza dos casillas horizontales (resp. verticales) en cualquier dirección y luego, desde esta casilla, una casilla vertical (resp. horizontal) en cualquier dirección, sin importar si las casillas por las que pasaría están ocupadas por otras piezas o no. A continuación mostramos los 8 posibles movimientos de un caballo ubicado en el centro del tablero. No usaremos en lo que sigue la capacidad de saltar, sólo su movimiento en forma de L.

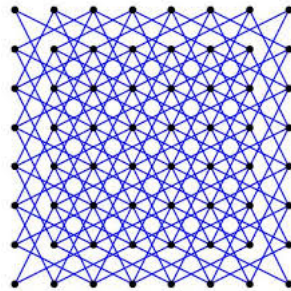


Hay un antiguo y famoso problema ajedrecístico, conocido como la *ruta del caballo*. En éste, se trata de recorrer todas las casillas del tablero con un único caballo pasando por cada una de ellas una sola vez y comenzando desde cualquier casilla. Una variante es que la ruta sea cerrada, es decir comenzar y terminar en la misma casilla. Existen un total de 19.591.828.170.979.904 rutas de caballo (abiertas o cerradas) en un tablero de ajedrez. En la siguiente figura mostramos una ruta cerrada y simétrica.



Matemáticamente, pensamos al tablero como un grafo de 64 vértices (las casillas) donde los vértices se conectan entre dos casillas si existe una movida de caballo entre ellos (ver siguiente figura). El problema de la ruta del caballo es

entonces equivalente a encontrar caminatas Hamiltonianas del grafo (circuitos Hamiltonianos si la ruta es cerrada).



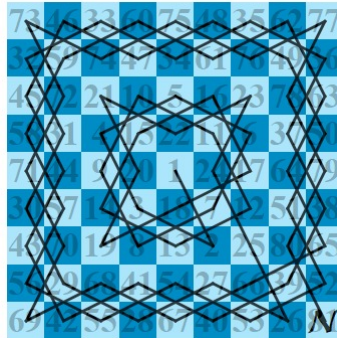
Bueno, pero volvamos a los números racionales, ¿qué tienen que ver con los tableros de ajedrez? Sabemos que los números racionales son infinitos de la forma  $\frac{m}{n}$  con  $m$  y  $n$  enteros y  $n \neq 0$ . Entonces la idea es que vamos a pensar en el plano como un “tablero de ajedrez infinito”, donde cada casilla represente un número racional. En efecto, podemos pensar en un tablero infinito donde cada casilla es un cuadradito de lado 1 centrado en los puntos de coordenadas enteras. De esta manera, la casilla cuyo centro corresponde al punto  $(m, n) \in \mathbb{Z} \times \mathbb{Z}$  tiene asociado el número racional  $\frac{m}{n}$ , si  $n$  no es 0. Cada número racional con sus dos coordenadas no nulas aparece 2 veces en el tablero:  $(m, n)$  y  $(-m, -n)$  representan a  $\frac{m}{n}$  y  $(-m, n)$  y  $(m, -n)$  representan a  $-\frac{m}{n}$ . Las casillas correspondiente al eje  $x$  representan todas al 0 y convenimos en asignar el número 0 también a las casillas que corresponden al eje  $y$ . De esta manera podemos decir que hay un salto de caballo entre los números racionales  $\frac{m_1}{n_1}$  y  $\frac{m_2}{n_2}$  si existe un salto de caballo entre alguna de las casillas  $(\pm m_1, \pm n_1)$  y  $(\pm m_2, \pm n_2)$  que los representan en el tablero infinito. Matemáticamente,  $(m_1, n_1)$  está a salto de caballo de  $(m_2, n_2)$  si y sólo si  $(m_2, n_2)$  es alguno de los siguiente 8 puntos

$$(m_1 + 2, n_1 \pm 1), \quad (m_1 - 2, n_1 \pm 1), \quad (m_1 \pm 1, n_1 + 2), \quad (m_1 \pm 1, n_1 - 2).$$

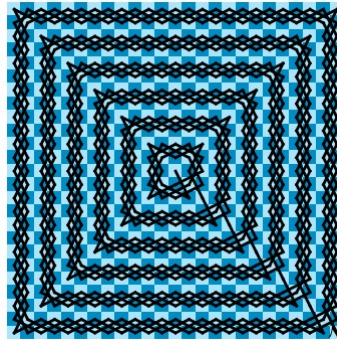
Ahora que tenemos identificados los puntos de  $\mathbb{Q}$  con un tablero de ajedrez infinito, nos preguntamos si hay una ruta de caballo que vaya de un punto racional cualquiera a otro punto racional cualquiera.

Allen Schwenk probó en 1991 (*Which rectangular chessboards have a knight's tour?* Mathematics Magazine 64:5, 325–332) que existen rutas cerradas de caballo en un tablero  $n \times m$  con  $n \leq m$  si y sólo si (a)  $n$  y  $m$  no son ambos impares y (b)  $n \geq 5$  ó  $n = 3$  y  $m \geq 10$ . Sin embargo nos interesan las rutas abiertas. Es sabido que para todo tablero  $n \times n$  con  $n$  impar mayor que 5 existe una ruta de caballo abierta. En efecto, en 2005 Shun-Shii Lin y Chung-Liang Wei probaron (*Optimal algorithms for constructing knight's tours on arbitrary  $n \times m$  chessboards*, Discrete Applied Mathematics 146:33, 219–232) que existe una ruta de caballo abierta en un tablero  $n \times m$ , con  $n \leq m$ , si y sólo si (a)  $n = 3$  y  $m = 4$  o  $m \geq 7$  o bien (b)  $n \geq 4$  y  $m \geq 5$ . De hecho, el procedimiento es repetido de tableros más chicos a tableros más grandes. A continuación mostramos una ruta en un tablero  $9 \times 9$

donde si nos concentramos en tablero  $5 \times 5$  del centro vemos además una ruta de caballo en un tablero  $5 \times 5$  (aunque no en el tablero  $7 \times 7$ ).



La siguiente es una ruta de caballo  $25 \times 25$  que incluye rutas de caballo para todos los tableros  $n \times n$  con  $n$  impar de la forma  $4k + 1$  menor que 25.



Es claro que este procedimiento sirve para cualquier tablero  $4k + 1 \times 4k + 1$  y por lo tanto, dados dos racionales  $q_1 = \frac{m_1}{n_1}$  y  $q_2 = \frac{m_2}{n_2}$ , primero los ubicamos en un tablero  $4k + 1 \times 4k + 1$  (el menor posible) y luego los unimos siguiendo la ruta que sabemos que existe (y que puede ser inductivamente construida por el procedimiento que ya mencionamos arriba). Luego, ¿existen saltos de caballos que unen cualquier par de números racionales!

La primera referencia a una ruta de caballo se remonta al siglo IX d.C. En el libro de poesía en sánscrito escrito por **Rudrata**, menciona poemas escritos a partir de rutas de caballo. En un libro escrito por **Bhat Nilakantha**, que data de entre los años 1600 a 1700, describe 3 rutas de caballo, que no sólo son cerradas sino que son simétricas. Uno de los primeros matemáticos en ocuparse del tema fue, cuando no, **Leonhard Euler**, quien en 1759 presentó varias rutas de caballo simétricas. En 1823, **H. C. von Warnsdorff** introdujo un procedimiento heurístico para producir rutas de caballo en el 85% de las veces en tableros menores que  $50 \times 50$  y un 50% en tableros menores que  $100 \times 100$ . La regla de Warnsdorff dice: 'iniciar en cualquier casilla e ir siempre a una casilla que tenga la menor cantidad de casillas vecinas (a tiro de salto de caballo) no visitadas.

---

## EN BUSCA DE LA FELICIDAD

Roberto Ben, Agustín Besteiro, Antonio Cafure, Darío Devia y Diego Rial

---

RESUMEN. Acaso los números naturales sean los seres vivos más básicos, las células primigenias de ese entramado vital, fértil, complejo e inabarcable que es la actividad matemática. Están sujetos a diversas leyes de evolución que nosotros mismos podemos definir, de acuerdo a nuestro completo antojo, tantas como nuestra imaginación permita. Quizás, si somos afortunados, podremos predecir cómo es la evolución bajo cada ley que impongamos, cómo es la transformación de ese estado inicial. Quizás, si somos afortunados, podremos encontrar la felicidad.

*Palabras clave:* Números felices, Sucesiones, Evolución.

ABSTRACT. Perhaps natural numbers are the most basic living beings, the original cells of that vital, fertile, complex and unbounded network that is mathematical activity. They are subject to various laws of evolution that we ourselves can define, according to our complete whim, as many as our imagination allows. Perhaps, if we are lucky, we will be able to predict what evolution is like under each law that we impose. Perhaps, if we are lucky, we can find happiness.

*Keywords:* Happy Numbers, Sequences, Evolution.

### §1. Introducción

Un número natural  $N$  suele *representarse* como una tira  $N = a_n a_{n-1} \cdots a_0$  de cifras entre 0 y 9. La condición es que  $a_n$ , la cifra más a la izquierda, sea distinta de 0 (así se explica el rechazo a ser un cero a la izquierda). Esta *representación* es una forma abreviada de indicar lo siguiente:

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0.$$

A partir de *esta* forma de representar los naturales, definimos una función que a cada natural  $N$  le asigna la suma de los cuadrados de sus cifras:

$$S_2 : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ a_n a_{n-1} \cdots a_0 & \longmapsto & a_n^2 + a_{n-1}^2 + \cdots + a_0^2 \end{array}$$

Es fácil calcular algunos ejemplos como

$$\begin{aligned} S_2(25) &= 2^2 + 5^2 = 29, \\ S_2(2437) &= 2^2 + 4^2 + 3^2 + 7^2 = 78, \\ S_2(111111) &= 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 = 6. \end{aligned}$$

Sin embargo, no es tan fácil calcular  $S_2(293^{341} - 14 \cdot 45)$ . Para hacerlo, necesitamos conocer las cifras decimales o, lo que es lo mismo, la representación en base 10 de  $293^{341} - 14 \cdot 45$ .

A primera vista, una función como  $S_2$  podría parecernos una curiosidad. No está mal ya que en numerosas oportunidades lo que comienza siendo una curiosidad se revela luego como una suerte de caja de Pandora inversa cuyo contenido nos permite, si estamos dispuestos, modificar nuestra mirada sobre el mundo matemático. Quizás haya un poco de exageración en nuestras afirmaciones pero estamos en la introducción del artículo y necesitamos despertar el interés del lector: ¿será posible que  $S_2$  pueda ser algo parecido a una caja de sorpresas?

Como escribimos en el resumen, los números naturales pueden considerarse como las células básicas del entramado matemático y, en consecuencia, están sujetos a diversas leyes de evolución. Una de estas leyes puede definirse iterando  $S_2$ . Estamos ante la magnífica ocasión de observar cómo se manifiesta la naturaleza matemática en todo su esplendor, cómo evolucionan los números naturales bajo la dinámica que induce  $S_2$ . Esta acción hace surgir la noción de *número feliz*, una noción poco conocida aunque fácil de entender y, aquí el interés de este artículo, con un potencial enorme tanto para la enseñanza como para la investigación. Esta es la gran sorpresa que los lectores van a llevarse. Los invitamos a acompañarnos en este recorrido, en esta suerte de relato matemático que, esperamos, pueda darles un rato de felicidad.

## §2. Salir de la melancolía

Es claro que  $S_2$  es una función un tanto atípica. No es usual encontrar en los textos y prácticas universitarias funciones de este tipo, que apelen a cierta forma de representar objetos matemáticos. Sí encontramos una serie de preguntas y problemas casi inevitables sobre las funciones típicas que forman parte de toda colección de ejercicios que se precie de tal. Por supuesto, pueden formularse en este contexto. La función  $S_2$ , ¿es inyectiva?, ¿es suryectiva?, ¿es creciente?, ¿tiene puntos fijos? (no, esta última no es una pregunta típica), ¿cómo se grafica?

**2.1. Inyectividad y suryectividad.** No hay que dar demasiadas vueltas para concluir que  $S_2$  no es una función inyectiva. Toma el mismo valor en números diferentes. Por ejemplo,

$$S_2(188) = S_2(818) = S_2(881) = S_2(1880) = S_2(188000) = 129.$$



Más aún, la ecuación  $S_2(N) = 129$  tiene muchas, infinitas soluciones.

Caracterizar la imagen de  $S_2$  nos permite decidir si es o no suryectiva. Es evidente que los números cuadrados de 1 y 2 cifras decimales, y que 129 pertenecen a la imagen. Veamos qué ocurre con 43 (¿por qué 43?, ¿por qué no 43?). Nuestra tarea consiste en determinar si la ecuación  $S_2(N) = 43$  tiene alguna solución. Si acaso la ecuación tuviera alguna solución cuya representación en base 10 es  $N = a_n \cdots a_1 a_0$ , tendríamos que  $S_2(N) = a_n^2 + \cdots + a_1^2 + a_0^2 = 43$ . Es sencillo encontrar *una* solución. Alcanza con elegir el número  $N$  cuyas 43 cifras decimales son todas iguales a 1. Es decir, el número cuyo desarrollo decimal es  $N = \sum_{i=0}^{42} 1 \cdot 10^i$ . Habiendo encontrado una solución, podemos exhibir una colección infinita de soluciones.

Este caso particular bien describe lo que ocurre en el caso general y es lo que nos permite confirmar que  $S_2$  es una función suryectiva. Para cada natural  $M$ , el número  $N$  cuya representación decimal es  $\sum_{i=0}^{M-1} 1 \cdot 10^i$  tiene a  $M$  como imagen:

$$S_2(N) = \sum_{i=0}^{M-1} 1^2 = M.$$

**2.2. El crecimiento de  $S_2(N)$ , máximos y mínimos.** Estudiar el crecimiento y decrecimiento de una función es un tópico que no puede faltar en una práctica de las primeras matemáticas universitarias.

En nuestro caso, este ejercicio ya estaría resuelto:  $S_2$  no es creciente ni decreciente ya que no es una función inyectiva. Podemos entonces estudiar la existencia de subconjuntos de los números naturales en los cuales tenga alguna de estas características. Por ejemplo,  $S_2$  es creciente en el intervalo natural  $\llbracket 450, 459 \rrbracket$ . Sin embargo  $S_2(460) = 4^2 + 6^2$  es menor que  $S_2(459) = 4^2 + 5^2 + 9^2$ . En realidad, esta situación se observa en intervalos de 10 números consecutivos de la forma  $\llbracket (N-1) \cdot 10, (N-1) \cdot 10 + 9 \rrbracket$ . Estos intervalos son *maximales*: constituyen el subconjunto de números naturales consecutivos más grande posible sobre el cual  $S_2$  es creciente.

Hay cambios más abruptos entre las imágenes de números consecutivos. La mayor distancia entre las imágenes se da al pasar del mayor número de  $n$  cifras al menor número de  $n+1$  cifras:

$$S_2\left(\sum_{i=0}^{n-1} 9 \cdot 10^i\right) = S_2(10^n - 1) = 81n \quad \text{y} \quad S_2(10^n) = 1.$$

Si restringimos nuestra atención al intervalo natural  $\llbracket 1, 10^n - 1 \rrbracket$ , el conjunto de números naturales de a lo sumo  $n$  cifras, encontramos que 1 y  $10^n - 1$  son el mínimo y el máximo absoluto de  $S_2$ . Esto significa que para todo  $N$  en  $\llbracket 1, 10^n - 1 \rrbracket$  es válida

la desigualdad

$$1 \leq S_2(N) \leq 81n.$$

Aquí surge una idea con potencial. Consideremos el conjunto de todos los naturales de  $n$  cifras. Se puede representar como el intervalo natural  $\llbracket 10^{n-1}, 10^n - 1 \rrbracket$ . Si  $n$  es mayor o igual que 4, entonces  $10^{n-1} > 81n$ . Esta situación implica que la imagen por  $S_2$  de cualquier número  $N$  de ese intervalo es menor que  $N$ . En otras palabras, la imagen de cualquier número que tenga por lo menos 4 cifras decimales es menor que el propio número. Con un poco más de cuidado es posible optimizar la cantidad de cifras de los naturales para los cuáles es válido que  $S_2(N)$  es menor que  $N$ .

**Proposición 2.1.** *Si  $N$  es un número natural que tiene 3 o más cifras, entonces  $S_2(N) < N$ .*

*Demostración.* Si  $N$  tiene por lo menos tres cifras, entonces  $N$  es un número mayor o igual que  $10^2$ . Si lo expresamos en la forma  $N = a_n 10^n + \dots + a_1 10 + a_0$ , asumimos que  $n$  es mayor o igual que 2 y que, por supuesto,  $a_n$  es distinto de 0. Vamos a probar que  $N - S_2(N)$  es una cantidad positiva. Tenemos que

$$\begin{aligned} N - S_2(N) &= a_n 10^n + \dots + a_1 10 + a_0 - a_n^2 - \dots - a_1^2 - a_0^2 \\ &= a_n(10^n - a_n) + a_{n-1}(10^{n-1} - a_{n-1}) + \dots + a_1(10 - a_1) + a_0(1 - a_0) \\ &\geq 99 - 72 = 27 \end{aligned}$$

La última desigualdad se justifica teniendo en cuenta que el menor valor que puede tomar  $a_n$  es 1, el mayor valor que puede tomar  $a_0$  es 9 y que los términos que involucran a  $a_{n-1}, \dots, a_1$  son mayores o iguales que 0.  $\square$

La Proposición 2.1 muestra algo más. Nos informa que, en caso de tenerlos, los posibles puntos fijos de  $S_2$  son números de una o dos cifras. Quizás sea conveniente recordar que un número  $a$  es un *punto fijo* de una función  $f$  si  $f(a) = a$ . No es difícil demostrar que 1 es el único punto fijo de  $S_2$ . En el peor de los casos, lo hacemos recorriendo uno a uno los números de 1 a 99; o sea, una demostración de fuerza bruta. Aunque también podemos proceder de forma más elegante. Si un número de 2 cifras  $a_1 10 + a_0$  fuera un punto fijo de  $S_2$ , entonces tendríamos que  $a_1^2 + a_0^2 = a_1 10 + a_0$  y, luego, que  $a_1(a_1 - 10) = a_0(1 - a_0)$ . Como consecuencia de la simetría del miembro izquierdo y la paridad del derecho, es suficiente mostrar que para  $a_1 = 2$  y  $a_1 = 4$  la ecuación no tiene soluciones.

**2.3. El gráfico de  $S_2(N)$ .** Muchas de las actividades, de los problemas que involucran funciones en las primeras materias universitarias concluyen cuando utilizamos la información obtenida para confeccionar un gráfico aproximado. Para no ser menos, concluimos con dos gráficos aproximados de  $S_2$ .

Las Figuras 1 y 2 nos permiten apreciar el gráfico de  $S_2$  definida sobre los intervalos naturales  $\llbracket 1, 100 \rrbracket$  y  $\llbracket 1, 5000000 \rrbracket$ , respectivamente. Observamos algunas de las características ya mencionadas como la no inyectividad, el crecimiento en intervalos de 10 números consecutivos, los saltos abruptos en las imágenes de  $S_2(10^n - 1)$  y  $S_2(10^n)$ .

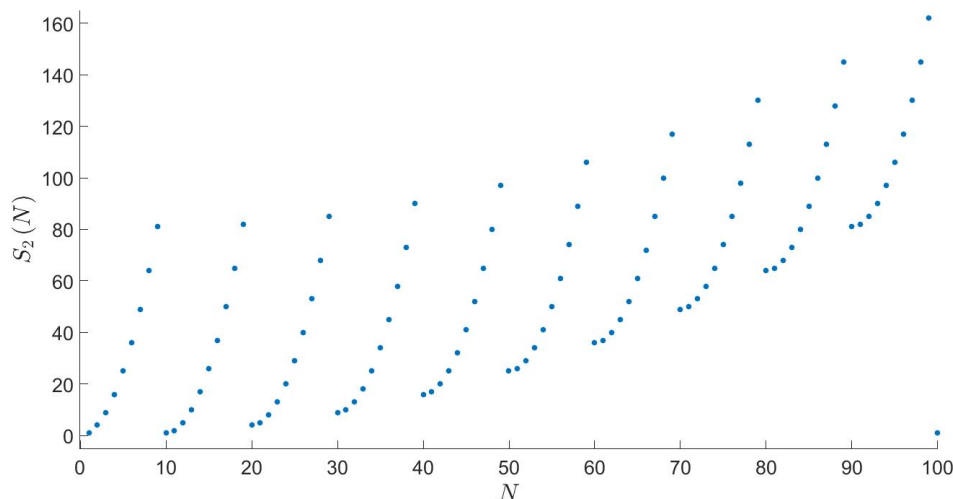


FIGURA 1. El gráfico de  $S_2$  definida en  $\llbracket 1, 100 \rrbracket$ .

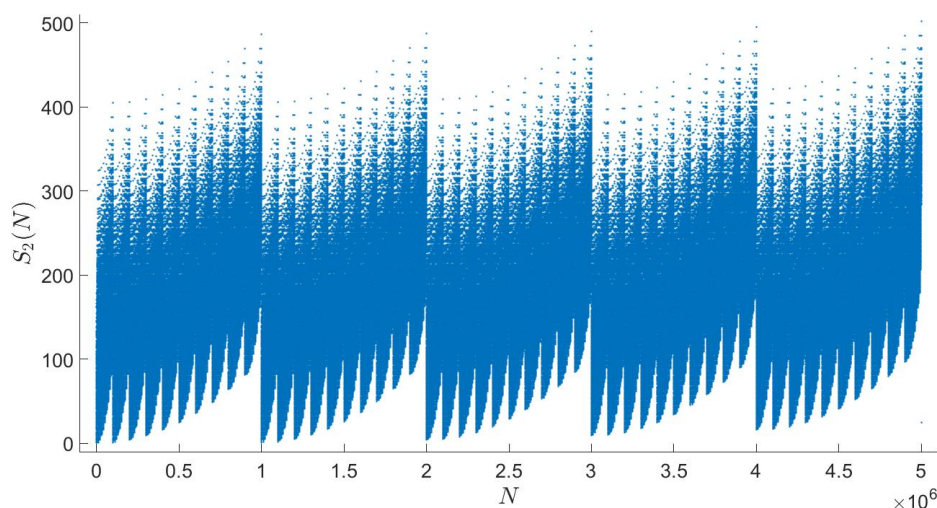


FIGURA 2. El gráfico de  $S_2$  definida en  $\llbracket 1, 5000000 \rrbracket$ .

### §3. Divididos por la felicidad

Una de las sensaciones más inquietantes de nuestra existencia es la imposibilidad de predecir el futuro. Es difícil no sucumbir a la tentación de planificar nuestras

acciones y tener completo control sobre sus consecuencias. Lamentablemente, o mejor, nos corregimos, afortunadamente, son pocas las situaciones en las que es posible avizorar lo que nos espera.

También es cierto que, nuestra experiencia da cuenta de eso, insistiendo, persistiendo en una acción vamos ajustando nuestra visión del mundo actual y el venidero. Mediante sucesivas aproximaciones podemos imaginar que hay algún futuro al que irremediamente vamos a llegar más allá de la dinámica de nuestras acciones. Esta idea tan presente en la vida cotidiana es también una de las ideas más fecundas de la matemática: insistir, repetir, reiterar un proceso y estudiar si esta dinámica de la insistencia nos conduce a algún lugar, si nos determina un futuro posible, una forma de evolucionar.

¿Qué ocurre si estudiamos cómo es la evolución de cada número natural bajo la acción, bajo la dinámica que sugiere la función  $S_2$ ? Por ejemplo, partimos de 1112 o de 41 y estudiamos las sucesiones de números naturales cuyos términos se obtienen iterando  $S_2$ :

$$\begin{aligned} 1112 &\rightarrow S_2(1112) \rightarrow S_2(S_2(1112)) \rightarrow S_2(S_2(S_2(1112))) \rightarrow \dots \\ 41 &\rightarrow S_2(41) \rightarrow S_2(S_2(41)) \rightarrow S_2(S_2(S_2(41))) \rightarrow \dots \end{aligned}$$

Podemos imaginar que estas sucesiones describen la evolución de estos números a lo largo del *tiempo*. Cada uno de sus términos es un estadio en la evolución. En el caso de 1112 y 41 observamos la siguiente evolución:

- $1112 \rightarrow 7 \rightarrow 49 \rightarrow 97 \rightarrow 130 \rightarrow 10 \rightarrow 1 \rightarrow 1 \rightarrow 1 \rightarrow \dots$
- $41 \rightarrow 17 \rightarrow 50 \rightarrow 25 \rightarrow 29 \rightarrow 85 \rightarrow 89 \rightarrow 145 \rightarrow 42 \rightarrow 20 \rightarrow 4 \rightarrow 16 \rightarrow 37 \rightarrow 58 \rightarrow 89 \rightarrow \dots$

Estamos frente a dos comportamientos diferentes, frente a dos escenarios que dan lugar a dos posibles tipos de sucesiones de números naturales.

- En el caso de 1112, nos encontramos con una sucesión que atraviesa siete estadios diferentes durante su evolución hasta que al tomar el valor 1, adopta su forma definitiva, constante a lo largo del tiempo. Esta sucesión es un ejemplo de lo que denominamos *sucesión convergente de números naturales*.

Se impone la siguiente pregunta: ¿cuántos tipos diferentes de sucesiones convergentes quedan determinados por la dinámica inducida por  $S_2$ ? Responder esta pregunta es equivalente a responder cuántos puntos fijos tiene  $S_2$ . Como 1 es el único punto fijo, la dinámica definida por  $S_2$  da lugar a un solo tipo de sucesión convergente: las que convergen a 1.

- En el caso de 41, su evolución atraviesa catorce estadios diferentes hasta alcanzar por segunda vez el 89. A partir de allí entra en un ciclo que se repite por toda la eternidad:

$$89 \rightarrow 145 \rightarrow 42 \rightarrow 20 \rightarrow 4 \rightarrow 16 \rightarrow 37 \rightarrow 58 \rightarrow 89.$$

Esta sucesión es un ejemplo de lo que denominamos *sucesión periódica*. Entra en escena además la noción de *órbita periódica*. En este caso, la sucesión tiene una órbita periódica de longitud 8. En particular, cabe señalar que la noción de sucesión periódica incluye la de sucesión convergente de números naturales. Las sucesiones convergentes son aquellas que tienen una órbita periódica de longitud 1.

La pregunta que se impone en esta situación es la siguiente: ¿cuántas sucesiones periódicas diferentes surgen con esta dinámica? Por el momento, no es claro cómo responder esta inquietud.

La ambición por conocer, por entender, es el motor. Nos moviliza el deseo por anticipar el futuro que le espera a la población de números naturales. Hasta aquí encontramos dos posibles futuros. Si dejamos que la dinámica inducida por  $S_2$  actúe libremente, que la naturaleza matemática se tome su tiempo y haga su trabajo, ¿será posible atisbar el futuro?, ¿con qué nos vamos a encontrar?

El conjunto de números naturales que generan una sucesión convergente, la única posible, es muy particular, se distingue del conjunto de los otros naturales. Suele suceder en matemática que al encontrar una particularidad, una característica especial, algo que nos llama la atención de un objeto matemático, nos interesa darle entidad. La manera de visibilizar esa singularidad es darle un nombre.

**Definición 3.1.** *Un número natural  $N$  es feliz si su evolución bajo la dinámica inducida por  $S_2$  es 1.*

En otras palabras, los números felices son aquellos que bajo la dinámica inducida por  $S_2$  dan lugar a una sucesión convergente; es decir, tienen una órbita periódica de longitud 1.

De acuerdo a esta definición, el mundo de los números naturales queda dividido en dos subconjuntos: el de los números felices (1, 7, 10, 49, 97, 130, 1112) y el de los números que no lo son (2, 4, 16, 17, 20, 25, 29, 37, 41, 42, 50, 58, 85, 89, 145). En realidad, como multiplicar un número por una potencia de 10 no cambia su naturaleza feliz o no feliz, deducimos que hay una cantidad infinita tanto de números felices como de números no felices. La existencia de infinitos números felices nos da la posibilidad de referirnos a la *sucesión de números felices* y, por qué no considerarla, a la *sucesión de números no felices*. Si de sucesiones de números naturales se trata, tenemos la obligación de visitar [The On-Line Encyclopedia of Integer Sequences](#) (OEIS).

OEIS es una iniciativa que comenzó en 1964 como una tarea llevada a cabo por un solo hombre: Neil Sloane. Es una base de datos de todas las sucesiones de números naturales que tengan algún interés para los matemáticos. Desde hace muchos años, se transformó en un trabajo colectivo, que se nutre de los aportes de diversas personas, quienes colaboran proporcionando nuevas sucesiones o

brindando nueva información para sucesiones ya registradas. Cada entrada de la enciclopedia provee información sobre bibliografía, actualizaciones, relaciones con otras sucesiones, etc.

La sucesión de números felices ha sido registrada como la entrada [A007770](#) de OEIS. Sus diez primeros términos son 1, 7, 10, 13, 19, 23, 28, 31, 32, 44. La sucesión de números no felices se encuentra como la entrada [A031177](#) y sus primeros diez términos son 2, 3, 4, 5, 6, 8, 9, 11, 12, 14.

La división de los números naturales en estas dos clases tiene consecuencias. Los que son felices saben que, aun cuando lleve mucho tiempo, una vez que alcancen la felicidad, la disfrutarán por toda la eternidad. ¿Qué ocurre con los números que no pertenecen a esta clase, con los que no son felices?, ¿qué futuro les espera? La respuesta está en el viento que nos trae el que denominamos *Teorema de la Felicidad*.

**Teorema 3.2.** *Hay solo dos futuros posibles:*

1. *La felicidad eterna.*
2. *La condena a oscilar por toda la eternidad en el ciclo de la infelicidad que muestra la Figura 3:*

$$4 \rightarrow 16 \rightarrow 37 \rightarrow 58 \rightarrow 89 \rightarrow 145 \rightarrow 42 \rightarrow 20 \rightarrow 4.$$

*Demostración.* La Proposición 2.1 proporciona la clave de la demostración. Supongamos que  $N = N_0$  es un número que tiene al menos 3 cifras. Escribimos  $N_{k+1} = S_2(N_k)$ . Mientras  $N_k$  tenga 3 o más cifras tenemos que  $N_{k+1} < N_k$ . Es decir, en algún estadio de su evolución, la evolución de  $N_0$  pertenece a la población de naturales de 1 o 2 cifras.

Esta situación es maravillosa. El futuro de los números naturales se reduce al estudio de la evolución de los naturales de 1 o 2 cifras. No menos maravilloso es el modo en que Ross Honsberger ([Honsberger, 1998](#)) en su *Ingenuity in Mathematics* termina la demostración:

*The writer knows of no way of showing that the assertion holds for  $0 < N < 100$  except by direct enumeration.*

□

**Una digresión.** ¿Por qué alguien, alguna vez, decidió llamarlos números felices?, ¿por qué la elección del adjetivo feliz? Podríamos haberlos llamado *números generosos* o *números revolucionarios*, o haber elegido cualquier otro adjetivo para acompañar a *número*. Esa elección no habría modificado la dinámica de la evolución. En consecuencia, se trata de elegir algún término cuyo sentido cotidiano, usual, describa de forma más o menos aproximada el sentido de la noción matemática con la que estamos trabajando. ¿Por qué entonces los llamamos números felices?, ¿cómo se vincula nuestra idea de felicidad con el hecho de que un número evolucione a 1 bajo la dinámica inducida por  $S_2$ ? La respuesta es sincera: no sabemos.







239, 263, 293, 313, 331, 367, 379, 383, 397, 409, 487. ¿Existen infinitos primos felices? No se conoce la respuesta a esa pregunta. Si se quiere conocer un poco más con respecto a la sucesión (finita, por ahora) de los primos felices se puede consultar la sucesión [A035497](#).

**4.3. La cantidad de números felices.** La felicidad no es un estado al que puedan aspirar todos los números naturales. ¿Cuántos de ellos pueden hacerlo?, ¿la mayoría de la población de números? Disponer de evidencia empírica siempre es saludable pues nos permite tomar decisiones. Así que para empezar a responder esas preguntas vamos a tratar de contar la cantidad de números felices en el intervalo  $\llbracket 1, N \rrbracket$  como para tener una idea de la *densidad* del conjunto de números felices en el conjunto de los números naturales.

La sucesión [A068571](#) presenta la cantidad de números felices en el intervalo  $\llbracket 1, 10^n \rrbracket$ . Sus primeros términos son 3, 20, 143, 1442, 14377, 143071, 1418854, 14255667, 145674808, 1492609148. Si miramos la lista de 20 términos que ofrece OEIS, observamos que la proporción de números felices en el intervalo  $\llbracket 1, 10^n \rrbracket$  oscila entre las cantidades 0,118226055080025491 cuando  $n = 18$  y 0,15091199357 cuando  $n = 15$ .

Vamos a considerar la densidad de números felices como una función del intervalo  $\llbracket 1, N \rrbracket$ . A continuación, presentamos dos gráficos que aportan alguna información al respecto.

La Figura 4 representa la densidad en  $\llbracket 1, N \rrbracket$ , considerando valores de  $N$  entre 1 y  $7 \cdot 10^6$ . Observamos que la densidad tiene una suerte de comportamiento asintótico.

Reescalando adecuadamente, la Figura 5 presenta el gráfico de la densidad en  $\llbracket 1, N \rrbracket$ , considerando valores de  $N$  entre 1 y  $2,15 \cdot 10^8$ . Si bien los valores de la densidad permanecen acotados, no observamos el comportamiento asintótico sugerido por la Figura 4.

Los resultados provistos por estos gráficos no son alentadores. Nos muestran que son *muy pocos* los números felices. ¿Será posible determinar la densidad de los números felices? Justin Gilmer respondió la pregunta aunque su respuesta no hace más que confirmar nuestro desánimo. En su trabajo *On the Density of Happy Numbers* publicado en 2013 (([Gilmer, 2013](#))), mostró que, como indica la evidencia, *alrededor* de  $1/7$  de los números naturales es feliz; es decir, *grosso modo* solo uno de cada siete números es feliz.

Gilmer es capaz de calcular la densidad de números felices en intervalos  $\llbracket 1, 10^m \rrbracket$  con  $m < 8000$ . Señala que ese hipotético carácter asintótico tampoco se observa para valores muy grandes de  $N$ . Es más, encuentra que la densidad de números felices está acotada entre 0,1138 y 0,18577.

No es muy saludable que la felicidad sea para pocos.

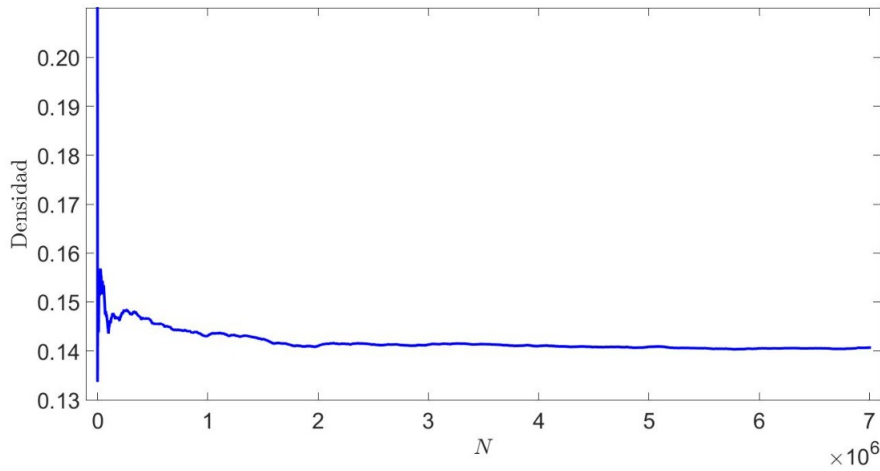


FIGURA 4. La densidad de números felices en  $\llbracket 1, 7000000 \rrbracket$

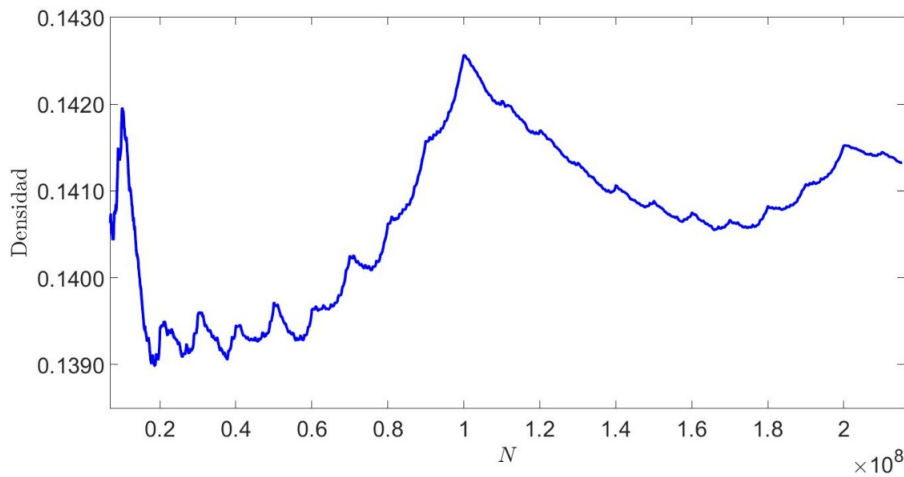


FIGURA 5. La densidad de números felices en  $\llbracket 1, 215000000 \rrbracket$

**4.4. Un trabajo de base.** La función  $S_2$  puede definirse sobre los naturales representados en cualquier base. En consecuencia, la dinámica implícita podría variar de acuerdo a cada base. Por lo tanto, la naturaleza feliz de un número podría modificarse. Por supuesto, extendiendo la Definición 3.1 a una base arbitraria.

De acuerdo a nuestra definición inicial, 2 no es un número feliz bajo el sistema decimal. Si consideramos el sistema binario, la representación de 2 es  $(10)_2$  y su imagen por  $S_2$  es

$$S_2((10)_2) = 1^2 + 0^2 = 1.$$

En el sistema binario,  $2 = (10)_2$  es un número feliz. Este simple ejemplo muestra que, como imaginábamos, la definición inicial de número feliz *no* es intrínseca: depende de la representación en base 10.

El sistema de representación decimal ya mostró sus evidentes limitaciones para asegurar la felicidad de la mayoría de los números. Solo puede garantizarle la felicidad a un séptimo de los naturales. Quizás sea el momento de cambiar el sistema de representación y considerar una base sobre la cual la felicidad de la mayoría de los números esté garantizada.

En esa búsqueda de un cambio de sistema, comenzamos con el sistema de representación binario. Es decir, nuestro mundo es el de los naturales representados en base 2. Utilizamos el símbolo  $(\mathbb{N}, 2)$  para representar ese conjunto. Si dejamos que la dinámica inducida por  $S_2 : (\mathbb{N}, 2) \rightarrow (\mathbb{N}, 2)$  actúe libremente, observamos que la evolución de cualquier  $N = (a_n a_{n-1} \cdots a_0)_2$  es  $(1)_2$ . La representación en base 2 asegura la felicidad de *todos* los números naturales.

El ejemplo binario es suficiente para darnos cuenta de que la introducción de un nuevo concepto está al alcance de la mano. Antes, extendemos una notación recientemente introducida. Indicamos por  $(\mathbb{N}, b)$  el conjunto de números naturales representados en base  $b$ . Si deseáramos ser extremadamente precisos, tendríamos que escribir algo así como  $S_{2,b}$  para indicar que la definición depende de la base utilizada. De esta manera, deberíamos escribir  $S_{2,b} : (\mathbb{N}, b) \rightarrow (\mathbb{N}, b)$ .

**Definición 4.2.** Una base  $b$  es *feliz* si todo elemento de  $(\mathbb{N}, b)$  es feliz.

La demostración del Teorema de la Felicidad (Teorema 3.2) tiene un costado muy interesante. Muestra que la fortuna de los números naturales depende de lo que ocurre con los números que tienen 1 o 2 cifras decimales. A su vez, esta reducción fue consecuencia de la Proposición 2.1. Como si nuestro texto fuera un relato policial en el cual se van sembrando las pistas, la forma de enunciarla preanunciaba algo importante: su enunciado solo alude a la cantidad de cifras del número en cuestión. Además, si bien su demostración utiliza explícitamente que la base es 10, la validez de la argumentación se puede extender a cualquier base  $b$ .

**Proposición 4.3.** Si  $N$  es un elemento de  $(\mathbb{N}, b)$  y tiene tres o más cifras, entonces  $S_{2,b}(N) < N$ .

*Demostración.* El trabajo consiste en traducir adecuadamente la demostración de la Proposición 2.1. Si  $N = (a_n a_{n-1} \cdots a_0)_b = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$  tiene tres o más cifras en base  $b$ , entonces  $n$  es mayor o igual que 2 y, por lo tanto,

$$\begin{aligned} N - S_{2,b}(N) &= a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 - a_n^2 - \cdots - a_1^2 - a_0^2 \\ &= a_n(b^n - a_n) + a_{n-1}(b^{n-1} - a_{n-1}) + \cdots + a_1(b - a_1) + a_0(1 - a_0) \\ &\geq b^2 - (b-1)(b-2) = 3b - 3 > 0 \end{aligned}$$

□

En definitiva, concluimos que para cada base  $b$ , la fortuna de los elementos de  $(\mathbb{N}, b)$  depende de lo que ocurre con los números que tienen 1 o 2 cifras.

Una de las primeras consecuencias es que 4 también es una base feliz. En efecto, como  $(1)_4$ ,  $(2)_4$  y  $(3)_4$  son felices, resulta que todo elemento de  $(\mathbb{N}, 4)$  es feliz. Hasta el momento 2 y 4 son las únicas bases felices conocidas menores que  $5 \cdot 10^8$ .

La sucesiones [A193583](#) y [A193585](#) indican el número de puntos fijos y el número de órbitas periódicas bajo la acción de  $S_{2,b}$ , respectivamente. Mirando estas entradas nos enteramos que en base 43 hay 11 puntos fijos y 6 órbitas periódicas; que en base 63 hay 7 puntos fijos y 9 órbitas periódicas, y que en base 83 hay 15 y 10, respectivamente.

La tabla que sigue, extraída de un trabajo de Helen Grundman y Elizabeth Teeple (([Grundman y Teeple, 2001](#))) detalla los puntos fijos y las órbitas periódicas para todas las bases  $b$  menores o iguales que 10.

Base	Puntos fijos y órbitas
2	1
3	1, 12, 22 2 → 11 → 2
4	1
5	1, 23, 33 4 → 31 → 20 → 4
6	1 32 → 21 → 5 → 41 → 25 → 45 → 105 → 42 → 32
7	1, 13, 34, 44, 63 2 → 4 → 22 → 11 → 2 16 → 52 → 41 → 23 → 16
8	1, 24, 64 4 → 20 → 4 5 → 31 → 12 → 5 15 → 32 → 15
9	1, 45, 55 58 → 108 → 72 → 58 82 → 75 → 82
10	1 4 → 16 → 37 → 58 → 89 → 145 → 42 → 20 → 4

Acaso sea imposible vivir en un estado permanente de felicidad; sin embargo, aquí encontramos ejemplos de que, al menos, en la población de números naturales no es algo impensado, algo imposible de lograr. Un cambio de sistema de representación abre la puerta a esa utopía.

### §5. Día de fiesta

Este artículo tiene sus orígenes en el video [Sobre la felicidad y los números](#) que Antonio Cafure subió a Matemática Sentimental, su canal de YouTube, durante la cuarentena de 2020.

Durante 2022, los autores comenzamos a discutir sobre diversos problemas que involucran la noción de número feliz y, a la vez, a poner por escrito las diferentes ideas que iban surgiendo. Como una forma de poner a prueba el interés de lo que escribíamos, a fines de julio de 2022, Antonio Cafure y Darío Devia dictaron el curso *La felicidad es un arma cargada* durante la Octava Escuela de Matemáticas de la Universidad Nacional de General Sarmiento, EMASUNGS VIII-Sabrina Victoria Vieiro.

Mientras terminábamos de escribir este artículo, notamos que la sucesión de distancias entre números felices no formaba parte de la OEIS. Tenemos el honor de presentar en sociedad nuestra sucesión, la entrada [A356412](#) de *The On-Line Encyclopedia of Integer Sequences*. Sus primeros diez términos son 6, 3, 3, 6, 4, 5, 3, 1, 12, 5.

Intentamos mostrar un posible recorrido: partiendo de una aparente curiosidad, de una iniciativa lúdica, de un contenido sencillo que bien podría formar parte de alguna currícula escolar o universitaria, seguimos asistiendo y participando de la ramificación de ese árbol tan saludable que es el conocimiento matemático. La savia del árbol matemático son los problemas, hasta aquellos que a primera vista puedan parecernos un simple entretenimiento. Así, se recrea el ciclo de la naturaleza matemática.

### Bibliografía

- El-Sedy, E., y Siksek, S. (2000). On happy numbers. *Rocky Mt. J. Math.*, 30(2), 565–570. Descargado de [math.la.asu.edu/~rmmc/rmj/VOL30-2/CONT30-2/CONT30-2.html](http://math.la.asu.edu/~rmmc/rmj/VOL30-2/CONT30-2/CONT30-2.html) doi: 10.1216/rmjm/1022009281
- Gilmer, J. (2013). On the density of happy numbers. *Integers*, 13, paper a48, 25.
- Grundman, H. G., y Teeple, E. A. (2001). Generalized happy numbers. *Fibonacci Q.*, 39(5), 462–466.
- Guy, R. (1994). *Unsolved problems in number theory*. (2nd ed. ed.). New York, NY: Springer-Verlag.
- Honsberger, R. (1998). *Ingenuity in mathematics*. (6th printing ed., Vol. 23). Washington, DC: Mathematical Association of America.
- Styer, R. (2010). Smallest examples of strings of consecutive happy numbers. *J. Integer Seq.*, 13(6), 10. (Id/No 10.6.3)

ROBERTO BEN

*Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento*

*Ciclo Básico Común, Universidad de Buenos Aires*

(✉) [rben@campus.ungs.edu.ar](mailto:rben@campus.ungs.edu.ar)

**AGUSTÍN BESTEIRO**

*Centro de Altos Estudios en Tecnología Informática, Universidad Abierta Interamericana*

(✉) [agustin.besteiro@uai.edu.ar](mailto:agustin.besteiro@uai.edu.ar)

**ANTONIO CAFURE**

*Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento*

CONICET

(✉) [acafure@campus.ungs.edu.ar](mailto:acafure@campus.ungs.edu.ar)

**DARÍO DEVIA**

*Instituto de Ciencias, Universidad Nacional de General Sarmiento*

*Ciclo Básico Común, Universidad de Buenos Aires*

(✉) [ddevia@campus.ungs.edu.ar](mailto:ddevia@campus.ungs.edu.ar)

**DIEGO RIAL**

*Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires*

CONICET

(✉) [drial@dm.uba.ar](mailto:drial@dm.uba.ar)

---

Recibido: 9 de agosto de 2022.

Aceptado: 25 de agosto de 2022.

Publicado en línea: 6 de septiembre de 2022.

---

---

# Sección de Problemas

✉ por Juan Pablo Rossetti

---

En este número, se presentan tres problemas, y por primera vez, en lugar de las *sucesiones al toque*, hay dos *crucigramas matemáticos*, en los que aparecen solo números enteros no negativos. Las soluciones se encuentran en las páginas siguientes.



**Problema 1.** *Coleccionando las figuritas del Mundial.*

Un niño tiene el álbum de figuritas del Mundial de Qatar y decide coleccionarlas para llenarlo. Sus padres quieren complacerlo, aunque se preocupan por el costo que podría tener esto, porque saben que su hijo no es de cambiar figuritas. Cada paquetito trae 5 figuritas distintas y cuesta 200 pesos.

Si suponemos que el álbum tiene  $n = 650$  figuritas. ¿cuánto costaría completarlo si le tocaran todas figuritas distintas?

Asumiendo que no hay figuritas difíciles, sino que todas salen aleatoriamente ¿cuál es la probabilidad de que en el 2do paquetito no salga ninguna repetida?

En general, si hay pegadas  $k$  figuritas en el álbum y se consigue una nueva figurita al azar, ¿cuál es la probabilidad de que no sea repetida?

Pregunta (difícil): ¿Cuál es la probabilidad de llenar el álbum con  $k$  figuritas?

Pregunta (muy difícil): ¿cuál es el *valor esperado* de lo que costaría, en promedio, completar el álbum sin cambiar figuritas?

---

**Problema 2.** *Polinomios.* Dados los monomios  $x^2y^2, x^2y^3, x^3y^2, x^3y^3, x^2y^4, x^4y^2$ , ¿existen enteros  $a_1, a_2, \dots, a_6$  tales que el polinomio  $p(x) = a_1x^2y^2 + a_2x^2y^3 + a_3x^3y^2 + a_4x^3y^3 + a_5x^2y^4 + a_6x^4y^2$  sea siempre no negativo?

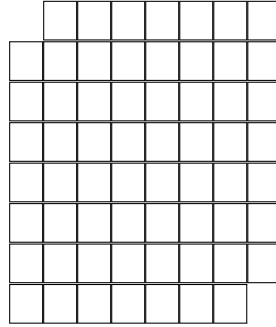
[Nota. Es muy interesante analizar el caso más general, donde no se especifican los monomios. Esto apareció como Problema nro. 4 en la CIMA (Competencia Interuniversitaria de Matemática Argentina) tomada este año el día 24 de agosto en todo el país.]

---

**Problema 3.** Cubrir un tablero con fichas de dominó.

Se tiene un tablero de  $8 \times 8$  casillas y fichas de dominó de  $2 \times 1$ , del tamaño de dos casillas del tablero. Claramente, con 32 fichas se puede cubrir bien el tablero sin superposiciones entre las fichas.

Ahora quitamos dos casillas al tablero, dos esquinas opuestas, como se muestra en la figura. ¿Se lo puede cubrir con 31 fichas?



Vale la pena pensar en el mismo problema en situaciones más generales. Si el lector no conocía el problema planteado, una ayuda para resolverlo puede ser pensar en los casos más pequeños de tableros de  $2 \times 2$  sin las dos esquinas opuestas y una sola ficha, o de  $4 \times 4$  y 7 fichas, etc.

Planteamos la misma pregunta para el tablero  $8 \times 8$ , pero ahora quitando dos casillas arbitrarias del mismo. ¿En qué casos se lo podrá cubrir bien con 31 fichas de dominó?

Pensar también el caso de un tablero de  $m \times n$  casillas, al que se le quitan dos casillas. ¿Cuándo se puede cubrir con  $\frac{m \times n}{2}$  fichas de dominó? (la pregunta tiene sentido cuando al menos uno de los dos números,  $m$  y  $n$ , es par; el caso en que ambos son impares, no se puede).

### ¡Crucigramas matemáticos!

Podés encontrar las soluciones en las páginas siguientes.

Los siguientes dos crucigramas se arman con números enteros no negativos, un dígito por casilla. En el segundo crucigrama algunas preguntas pueden requerir consultas bibliográficas o a internet. En el primero, el desafío es intentar hacerlo sin consultas a internet.



1	2			3		4	5
6			7			8	
9		10			11		
	12			13		14	
15				16	17		
		18	19				20
21	22		23			24	
	25				26		

**HORIZONTALES** 1.- Se pinta un cubo grande formado con 512 cubitos del mismo tamaño. Cantidad de cubitos pintados (en al menos una de sus caras). 3.-  $n^5$ , con  $n$  tal que el número de oro es igual a  $\frac{1+\sqrt{n}}{2}$ . 6.- Número de particiones del 8. 7.- 6to número triangular (el 1 es el primero). 8.- Cantidad de caras del icosaedro. 9.- Suma de los primeros 20 cuadrados perfectos. 11.- Menor número primo mayor que 100. 12.- Término de la sucesión de Fibonacci que se encuentra entre 2584 y 6765. 14.- Cantidad de números primos entre 50 y 100. 15.- 4to primo de Fermat, contando al 3 como el primero. 16.- Tres primeros dígitos significativos de  $\pi$ . 18.- Suma (en grados) de los ángulos interiores de un polígono de 9 lados. 21.- Cantidad de raíces de  $\cos(x) = 0$  para  $x \in [0, 100]$ . 23.- Menor número natural que tiene 12 divisores. 24.- Medida del tercer lado (número entero) de un triángulo rectángulo cuyos otros lados miden 60 y 109. 25.-

Cantidad de cuadrados (de todos los tamaños) que se forman en un tablero de ajedrez. 26.- Número de 3 dígitos cuya cifra de las unidades es 4 y que se obtiene al restar el número de 3 cifras  $abc$  por su permutado  $cba$ .

**VERTICALES** 1.- Vigésimo número natural que tiene todos sus dígitos iguales (el 1 es el primero). 2.- El 31 % de 299500. 3.- En sistema binario  $(11111)_2$  4.- En base 8  $(52776)_8$ . 5.- 10 veces la suma de los primeros 18 primos. 7.-  $n$  tal que  $n + 2$  es el producto de los primeros 4 primos. 10.-  $abab$  con  $ab$  primo y  $a = b + 6$ . 13.- MCCCLX 15.- Potencia quinta de 3 cifras. 17.- Base del sistema decimal. 19.- Área del polígono de vértices  $(27, 0)$ ,  $(19, 12)$ ,  $(2, 12)$  y  $(0, 0)$ . 20.-  $n$  tal que  $n(n+1)$  es el producto de los primeros 7 primos. 22.- Cantidad de veces que en un día las agujas del reloj forman un ángulo llano. 24.- Capicúa que es suma de 3 cubos consecutivos.

1	2	3		4	5	6	7
8				9			
10			11				
	12	13				14	
15		16			17		
18	19		20	21			22
23		24		25		26	
27					28		

**HORIZONTALES** 1.- 37mo término de la sucesión de Fibonacci, se encuentra entre 14930352 y 39088169. 8.- Primer cuadrado perfecto mayor que 1 en la sucesión de Fibonacci. 9.- Año del Nacimiento de Karl Friedrich Gauss. 10.- Cantidad de los famosos "Problemas de Hilbert". 11.- 5to primo de Fermat (3 es el 1ero). 12.- Primeros 4 dígitos significativos de  $e$ . 14.- Cantidad de triángulos distintos (no congruentes) con lados enteros entre 1 y 5. 16.- Cantidad de primos menores que 50. 17.- Cantidad de veces que se superponen las agujas del reloj en un día, sin contar las que se producen a las 12. 18.- Cantidad de aristas del Dodecaedro. 20.- Cantidad de rectángulos en un tablero de ajedrez. 23.- Menor número primo mayor que 300. 25.- Primeros 4 dígitos significativos del *número de oro*. 27.- Número de la patente del taxi que tomó Hardy cuando visitó a Ramanujan en el Hospital. 28.- Se

pinta un cubo grande formado con mil cubitos del mismo tamaño. Cantidad de cubitos que fueron pintados (en al menos una de sus caras).

**VERTICALES** 1.- Capicúa, par, cuyos dígitos suman 5. 2.- 25 % de 17728. 3.- 3er *número piramidal* (pirámide de base cuadrada). 4.- En sistema binario (110111110110)<sub>2</sub>. 5.- Cantidad de días en 5<sup>3</sup> semanas. 6.- MDCCXXXII por 10. 7.- Se le resta 2, luego se lo divide por 10 y solo le quedan siete. 11.- En base octal (14015)<sub>8</sub>. 13.- Primo gemelo del 73. 15.- Cubo perfecto y capicúa. 17.- Yuxtaposición del factorial de 4 y del menor cuadrado y cubo perfecto (simultáneamente) mayor que uno. 19.- Número del Agente Secreto más famoso 21.- Potencia cuarta perfecta, impar. 22.-  $\prod_{k=1}^4 k!$ . 24.- Medida en grados de los ángulos exteriores del pentágono regular. 26. Cantidad de pentominós (cinco cuadrados unidos por sus lados) distinguiendo la orientación.

## SOLUCIONES

**Solución 1.** Respuesta: 26 mil pesos costaría si no salen repetidas. Resulta de hacer  $650/5 = 130$ , serían los paquetitos necesarios, y luego multiplicar por 200 pesos.

Al comprar el 2do paquetito, la probabilidad de tener las 5 nuevas figuritas distintas a las anteriores viene dada por el cociente de números combinatorios:

$$\frac{\text{casos favorables}}{\text{casos totales}} = \frac{\binom{n-5}{5}}{\binom{n}{5}} = \frac{645 \cdot 644 \cdot 643 \cdot 642 \cdot 641}{650 \cdot 649 \cdot 648 \cdot 647 \cdot 646} \cong 0,962.$$

En general, si hay  $k$  figuritas pegadas, la probabilidad de que salga una nueva es  $p_{k+1} := \frac{n-k}{n}$ .

Llenar el álbum de  $n$  figuritas habiendo comprado  $k$  figuritas, es como colocar aleatoriamente  $k$  bolas en  $n$  celdas y que ninguna celda quede vacía. Esta probabilidad se calcula en la teoría:

$$\sum_{i=0}^n (-1)^i \binom{n}{i} \left(1 - \frac{i}{n}\right)^k.$$

Veamos ahora brevemente cómo se calcula el valor esperado de la cantidad de figuritas necesarias para llenar el álbum:

llamemos  $T$  y  $t_i$  a las variables aleatorias tales que  $T$  cuenta la cantidad de figuritas que tendremos que conseguir hasta completar el álbum y  $t_i$  las necesarias para obtener la  $i$ -ésima figurita nueva después de tener ya  $i - 1$  pegadas en el álbum. Entonces  $T = t_1 + \dots + t_n$ . La probabilidad de obtener una nueva figura es  $p_i := \frac{n-(i-1)}{n} = \frac{n-i+1}{n}$ . Así,  $t_i$  tiene distribución geométrica con valor esperado  $\frac{1}{p_i} = \frac{n}{n-i+1}$ . Por linealidad de la esperanza tenemos

$$\begin{aligned} E(T) &= E(t_1) + E(t_2) + \dots + E(t_n) = \frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} = \\ &= \frac{n}{n} + \frac{n}{n-1} + \dots + \frac{n}{1} = n \cdot \left(\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n}\right) = n \cdot H_n, \end{aligned}$$

donde  $H_n$  es la suma parcial hasta  $n$  de la serie armónica, que se puede aproximar bien usando el logaritmo natural; con lo que queda

$$E(T) = n \cdot H_n \cong n \ln n + 0,577 \cdot n$$

En nuestro caso, para  $n = 650$ , da cercano a 7. Es decir, si no se cambian figuritas, habrá que comprar aproximadamente  $7 \times 650 = 4550$  figuritas; es decir, 910

paquetitos, que en pesos se traduce a un gasto de 182 mil pesos. La conclusión infaltable es que hay que salir a cambiar las figuritas repetidas.

**Solución 2.** Respuesta: Sí, existen. Por ejemplo, tomando  $a_1 = 25$ ,  $a_2 = a_3 = -10$ ,  $a_4 = 2$ ,  $a_5 = 1$ ,  $a_6 = 4$ , resulta que  $p(x) = (xy^2 - 5xy + 2x^2y)^2$ , por lo tanto es siempre no negativo.

**Solución 3.** Respuesta: No se puede. La solución al problema es iluminadora, muestra muy bien un aspecto del poder de los invariantes en la matemática.

Pensar el tablero  $8 \times 8$  como de ajedrez, con las casillas blancas y negras. Notar que cada ficha de dominó que se ponga en el tablero, siempre va a cubrir una casilla blanca y una negra. El tablero original tiene 32 casillas de cada color, pero cuando se le quitan dos esquinas opuestas queda con 32 casillas de un color y 30 del otro. Por lo tanto, es imposible cubrirlo con 31 fichas de dominó.

Lo mismo sucede en general, en un tablero  $n \times m$ . Se lo colorea como al del ajedrez, por ser  $m$  o  $n$  pares. Entonces no se lo puede cubrir si se han quitado dos casillas de un mismo color. Ahora, si se se quitan dos casillas de distinto color, se puede ver, que siempre se lo puede cubrir bien, para  $m, n > 1$ . Una demostración se puede hacer con un razonamiento de tipo inductivo.

### Soluciones de los Crucigramas Matemáticos

2	9	6	■	3	1	2	5
2	2	■	2	1	■	2	0
2	8	7	0	■	1	0	1
■	4	1	8	1	■	1	0
2	5	7	■	3	1	4	■
4	■	1	2	6	0	■	7
3	2	■	6	0	■	9	1
■	2	0	4	■	5	9	4

2	4	1	5	7	8	1	7
1	4	4	■	1	7	7	7
2	3	■	6	5	5	3	7
■	2	7	1	8	■	2	2
1	■	1	5	■	2	0	■
3	0	■	7	8	4	■	2
3	0	7	■	1	6	1	8
1	7	2	9	■	4	8	8

Viene de páginas anteriores.