El sistema binario.
El juego del Nim y otras aplicaciones.

R. J. Miatello - M. I. Viggiani Rocha

Es un hecho familiar que si n es un número natural, n puede ser expresado en forma única como suma de potencias de 2, $n = \sum_{i=0}^{r} a_i 2^i$, donde $a_i = 0$ ó $a_i = 1, \forall i$.

En efecto, si r = máx $\{m \in \mathbf{N} \cup \{0\} \; : \; 2^m \leq n\}$, entonces $0 \leq n - 2^r < n$. Por hipótesis inductiva, $n - 2^r = \sum_{i=0}^{t} a_i 2^i$ con $a_i \in \{0, 1\}$ determinados unívocamente por $n - 2^r$, luego por n, y necesariamente $t < r$, por la elección de r.

En el sistema de numeración binaria o diádica se representa al número n por medio de los dígitos $a_r\, a_{r-1} ... a_2\, a_1\, a_0$ que aparecen en la expansión en base 2 de n. Por ejemplo, $7 = 2^2+2+1$, $9 = 2^3+1$ y $37 = 2^5+2^2+1$, se representan respectivamente por $111, 1001$ y 100101. Este sistema ofrece la ventaja de requerir para la representación de un número dado, sólo el uso de 2 dígitos. En una computadora, cada dígito binario a_i está representado por un circuito, y el valor de a_i es igual a 1 ó 0 según haya paso, o no, de corriente por el mismo. Este sistema era conocido por los antiguos matemáticos chinos y por tribus primitivas, pero fue el gran matemático alemán Gottfried W. Leibnitz (1646-1716) quien lo desarrolló en detalle por primera vez.

El objeto de la presente nota es exponer aplicaciones del sistema binario a diversos juegos, entre otros los siguientes: estrategia para el juego del Nim, diversas adivinanzas numéricas, ciertas curvas especiales, y la llamada la torre de Brahma.

Esta nota puede considerarse como una continuación de [MV] que trata de cuestiones de divisibilidad de números combinatorios.

1. Estrategia ganadora para el juego del Nim.

El juego del Nim se puede describir como sigue. Dadas m filas con $n_1, n_2 \ldots n_m$ fósforos cada una, dos jugadores retiran, por turno, tantos fósforos como deseen y por lo menos uno, todos ellos de la misma fila. Pierde el jugador que retira el último fósforo. El nombre de Nim fue dado en 1901 por Charles L. Bouton, profesor de Matemática de la Universidad de Harvard, quien fue el primero en hacer un análisis completo del mismo ("nim" en inglés antiguo significa "robar o llevarse").

Según veremos, existe una estrategia ganadora de este juego basada en la expansión binaria de los números en cuestión.

La versión más conocida del juego es con 4 filas con 1 , 3 , 5 , y 7 fósforos respectivamente.

I	1	→	1
III	3	→	11
IIIII	5	→	101
IIIIIII	7	→	111

Observamos que si se suman por separado las columnas de las expresiones binarias anteriores se obtiene la terna (224).

La estrategia ganadora se basa en las siguientes observaciones

(a) Al retirar fósforos de una fila, se altera la paridad en al menos una de las cifras en la terna (224).

(b) En caso en que alguna de las cifras de la terna de sumas sea impar, existe siempre al menos un modo de restablecer la paridad en cada una ellas, retirando fósforos de una sola fila.

La estrategia ganadora para el segundo jugador, consiste, de acuerdo a (b), en restablecer la paridad en la terna de sumas, con las siguientes excepciones. Si sólo quedan fósforos en una fila, deberá retirar todos los fósforos excepto uno. En el caso en que queden fósforos en sólo 2 filas, y en una de ellas sólo haya 1 fósforo, deberá (obviamente) retirar todos los fósforos de la fila restante. Esta estrategia le asegura la victoria. En resumen, si las sumas de todas las cifras son pares (resp. alguna es impar) quien comienza el juego pierde (resp. gana) si el adversario juega sin cometer errores.

Veamos un caso concreto para familiarizarnos con el método. Si un jugador comienza retirando 2 fósforos de la cuarta fila, (quedando una distribución de $1,3,5,5$), la expresión binaria en la cuarta fila pasa de 111 a 101, luego la terna de sumas es ahora (214). Se puede restablecer la paridad retirando 2 fósforos de la segunda fila, obteniéndose como terna de sumas (204), pasando así a tener una distribución de $1,1,5,5$ fósforos. Si el adversario, por ejemplo, retira ahora 1 fósforo de la tercera fila, la terna de sumas pasará a ser de (203), y puede restablecerse la paridad retirando (por ejemplo) 1 fósforo de la primera fila. En este caso queda una distribución de $0,1,4,5$ fósforos y una terna de sumas de (202). Si el adversario retira 2 fósforos de la cuarta fila tendremos ahora $0,1,4,3$ y como terna de sumas (112), luego retirando 2 fósforos de la tercera fila, pasaremos a tener $0,1,2,3$ y una terna de sumas de (022). El segundo jugador continuará aplicando la estrategia de restablecer la paridad hasta llegar a una de las situaciones excepcionales descriptas al comienzo. El lector puede familiarizarse con el método ensayando diversas posibilidades.

Para concluir la discusión sobre el Nim, pasaremos a dar un esquema de la demostración de las afirmaciones (a) y (b) en las que se basa la estrategia.

La paridad de cada una de las sumas equivale a que para cada i, hay un número par de $a_i(n_j)$'s iguales a 1, si $1 \leq j \leq r$. Al retirar fósforos de la fila k se altera el valor de (al menos) uno de los dígitos binarios del n_k, digamos el $a_h(n_k)$. Esto asegura que la h-ésima suma cambiará de paridad, como se afirma en (a).

En cuanto a (b), sea h el mayor índice tal que la h-ésima suma es impar. Entonces existe (al menos) un número, digamos n_k, que tiene el h-ésimo dígito igual a 1. Es claro que podemos extraer de la fila k el número de fósforos que sea necesario para transformar el h-ésimo dígito en 0, y asimismo modificar cada uno de los dígitos binarios $a_j(n_k)$ (todos de índice menor o igual que h) para aquellos j con la propiedad de que la j-ésima suma sea impar. Esto restablece la paridad de todas las sumas, lo que demuestra (b).

2. El Teorema de Lucas.

Sea el número combinatorio $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$. Se trata de hallar condiciones sobre n y k para que éste sea impar. El matemático francés Edouard Lucas dio una respuesta elegante a esta pregunta basada en los desarrollos binarios de los números n y k. El teorema probado por Lucas es el siguiente:

Teorema. Sean $n = \sum_{i=0}^{r} a_i 2^i, k = \sum_{i=0}^{s} b_i 2^i$. Entonces $\binom{n}{k}$ es impar si y sólo si $a_i \geq b_i$, $\forall i$.

En realidad el resultado de Lucas permite decidir sobre la divisibilidad de $\binom{n}{k}$ por un primo p arbitrario. Para una discusión detallada de este resultado referimos a [MV].

3. Descubriendo un número.

3.1. Consideremos el problema de adivinar un número, haciendo el mínimo número de preguntas, donde cada pregunta sólo puede ser respondida por "sí" o "no".

De una manera intuitiva resulta claro que las preguntas deben elegirse de modo tal que cada una de ellas, cualquiera sea la respuesta, excluya el máximo posible de los números en cuestión. Por ejemplo, si se tratara de determinar un número de teléfono x de 5 cifras y se preguntara "si el número elegido es 12145", ésta sería una pregunta muy poco eficiente pues si se no se acertara el número, para la segunda pregunta quedarán 99999 números posibles. Una estrategia mejor es buscar determinar cada una de las 5 cifras decimales de x, para lo cual bastan $5.5 = 25$ preguntas (verificar). Sin embargo, la estrategia óptima consiste en buscar que en cada paso, cada pregunta divida al conjunto remanente en 2 partes iguales, o con diferencia de 1, si el total es impar. En el caso anterior dado que $2^{16} \leq 10^6 \leq 2^{17} = 131.072$, se tiene que $0 \leq x = \sum_{i=0}^{16} a_i(x) 2^i < 10^6$. Un modo de hallar x es preguntar sucesivamente, "si a_i es igual a 0", para $i = 0, 1, \ldots, 16$, por lo cual bastarán 17 preguntas para tener la certeza de determinar x. En el caso de un número x arbitrario, si $0 \leq x < N$, donde $2^{n-1} \leq N < 2^n$, y $x = \sum_{i=0}^{n-1} a_i(x)2^i$, n preguntas bastarán y resulta intuitivamente claro que éste es el número mínimo posible.

De hecho, cualquier serie de preguntas tal que cada una de ellas divide al conjunto remanente en dos partes (aproximadamente) iguales es válida. Por ejemplo, la primer pregunta podría ser si " x es par" . Si la respuesta fuera positiva, la segunda podría ser si "x es múltiplo de 4", etc.

Según nos fuera observado por Diego Vaggione, un modo de demostrar rigurosamente que la estrategia anterior es la óptima posible, consiste en asociar a cada estrategia de búsqueda un árbol binario cuyos nodos correspondan a las distintas preguntas y cuyas hojas correspondan a los estados finales, es decir a cada uno de los distintos números a obtener. Para un razonamiento de este tipo (aplicado al problema de la moneda falsa) referimos a [B].

3.2. Una aplicación de la aritmética binaria esta implícita en el siguiente juego de números. Consideremos las siguientes tarjetas:

TARJETA	A
16	24
17	25
18	26
19	27
20	28
21	29
22	30
23	31

TARJETA	B
8	24
9	25
10	26
11	27
12	28
13	29
14	30
15	31

TARJETA	C
4	20
5	21
6	22
7	23
12	28
13	29
14	30
15	31

TARJETA	D
2	18
3	19
6	22
7	23
10	26
11	27
14	30
15	31

TARJETA	E
1	17
3	19
5	21
7	23
9	25
11	27
13	29
15	31

A un estudiante se le muestran estas tarjetas y se le pide que indique aquellas que tengan su edad impresa. Supongamos que éste responde que su edad está impresa en las tarjetas A y E. El dueño de las tarjetas suma los números que aparecen en la parte superior izquierda de estas dos tarjetas y dice: "Usted tiene 17 años de edad"

Observemos que los números que aparecen en la parte superior izquierda de cada tarjeta representan las potencias de 2 desde n = 0 hasta n = 4, y usando la representación binaria de los números entre 1 y 31 notamos que en la tarjeta A aparecen todos los números (entre 1 y 31) que poseen $a_4 = 1$; en la tarjeta B los que poseen $a_3 = 1$; en la C, los con $a_2 = 1$; en la D, los con $a_1 = 1$ y en la E, los con $a_0 = 1$. Por lo tanto identificando las tarjetas donde aparece el requerido número se conocerá inmediatamente su desarrollo binario y, en consecuencia, el número a determinar.

4. La cadena de plata.

Un buscador de plata no disponía de dinero para pagar el alquiler de una semana de hospedaje. Tenía en cambio una cadena de plata pura de 7 eslabones, por lo tanto hizo un arreglo con la casera para pagar por medio de la cadena, a razón de un eslabón por día. Al finalizar la semana dispondría del dinero necesario para abonar su deuda y recuperaría la cadena de plata.

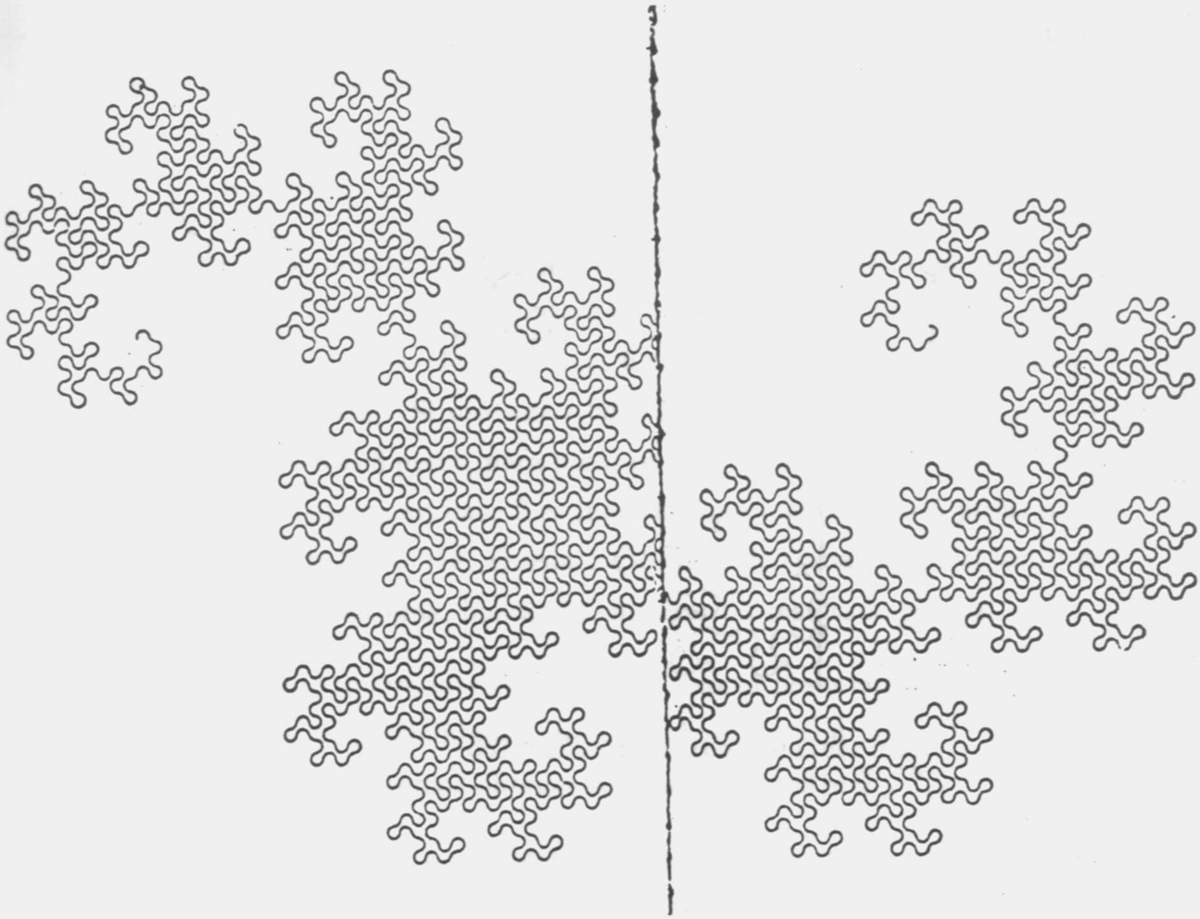
Luego de pensar un momento percibió que no era necesario hacer más que 2 cortes en la cadena para pagar su alquiler. En efecto, separando el primer eslabón del segundo y el tercero del cuarto, quedaron 3 trozos con 1, 2 y 4 eslabones respectivamente.

Luego, el primer día entregó el pedazo con 1 eslabón, el segundo día el de 2 eslabones y la casera le devolvió el de 1 eslabón, el tercer día entregó el de 1 eslabón nuevamente. El cuarto día dió el de 4 eslabones y recibió a cambio los pedazos de 1 y 2 eslabones, y así continuó dando y recibiendo los distintos pedazos hasta completar la cadena el séptimo día.

Este procedimiento es una aplicación directa de la expansión binaria, como es fácil de verificar.

5. La curva dragón.

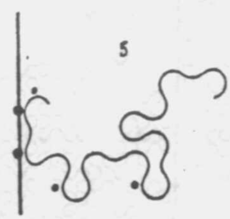
La descripción de una curva dragón cualquiera, puede hacerse con auxilio de una sucesión de dígitos binarios, en la cual los 1's denotan giros hacia la izquierda y los 0's giros hacia la derecha, trazándola desde la cola hacia la cabeza.



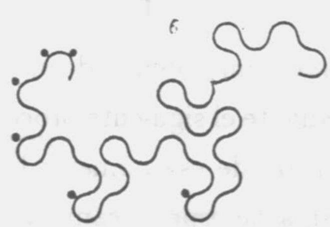
La fórmula correspondiente a un orden dado se deduce de la del orden inmediatamente anterior mediante el siguiente proceso recursivo: se añade un 1, cambiando la cifra central de ese número; lo que es equivalente a añadir un 1 y copiar, en forma de espejo, cambiando 0 por 1 y 1 por 0. Esto último se traduce en que cada curva dragón está formada por 2 copias de dragones de orden inmediatamente inferior, unidas cabeza a cabeza. Si se interpreta cada 1 (resp. 0) como un giro a la derecha (resp. izquierda) las mismas fórmulas generan imágenes en sentido contrario.

A continuación vemos las curvas dragón de órdenes 1 a 6. Los puntos negros corresponden a los 1 's centrales en los sucesivos órdenes de la curva (desde el 1 hasta el propio orden). Se observan que estos puntos caen sobre un espiral logarítmica.

1 110 1101100 110110011100100



1101100111001001110110001100100



110110011100100111011000110010011101100111001000110110001100100

6. Balanzas y Pesas.

Como consecuencia directa de la existencia de expansión binaria para un número natural arbitrario, se tiene que usando una balanza de dos platillos y disponiendo de 5 pesas de 1 , 2, 4, 8 y 16 gramos respectivamente, se puede pesar cualquier objeto de hasta 31 gramos (colocando pesas en un único platillo). Más generalmente , dadas n pesas de 2^jg, con $0 \leq j < n$ se puede pesar cualquier objeto de hasta $2^n - 1$g.

Comparativamente notemos que si usamos pesas de valor una potencia de 3 (esto es la base de la expansión es 3) serán necesarias 2 pesas de 1g, 2 pesas de 3g y 2 pesas de 9g, esto es 6 pesas, para poder pesar cualquier objeto de hasta 26g. Si usáramos base 5 harían falta 4 pesas de 1g y 4 pesas de 5g, esto es 8 pesas, para pesar objetos de hasta $24 = 5^2 - 1$g. Esto indica que el sistema en base 2 es más eficiente pues bastan 5 pesas para pesar objetos de hasta 31g. Queda como tema de trabajo para el lector el reflexionar sobre el tema, buscando enunciar un resultado general.

Una variante interesante es el permitir colocar pesas en ambos platillos, lo que amplía las posibilidades. Resulta claro que con pesas de $1, 2$ y 4g respectivamente podremos obtener sólo los pesos entre 0 y 7g.

Veamos que el uso de la base 3 es más efectivo para este problema. Por ejemplo, con pesas de 1, 3, 9 y 27 gramos se puede pesar cualquier objeto de hasta 40 gramos, como lo muestra la siguiente tabla:

	1er. Platillo	2do. Platillo
Objeto	$A_3A_2A_1A_0$	$A_3A_2A_1A_0$
1	0 0 0 0	0 0 0 1
2	0 0 0 1	0 0 1 0
3	0 0 0 0	0 0 1 0
4	0 0 0 0	0 0 1 1
5	0 0 1 1	0 1 0 0
6	0 0 1 0	0 1 0 0
7	0 0 1 0	0 1 0 1
8	0 0 0 1	0 1 0 0
9	0 0 0 0	0 1 0 0
10	0 0 0 0	0 1 0 1
11	0 0 0 1	0 1 1 0
12	0 0 0 0	0 1 1 0
13	0 0 0 0	0 1 1 1
14	0 1 1 1	1 0 0 0
15	0 1 1 0	1 0 0 0
16	0 1 1 0	1 0 0 1
17	0 1 0 1	1 0 0 0
18	0 1 0 0	1 0 0 0
19	0 1 0 0	1 0 0 1
20	0 1 0 1	1 0 1 0

	1er. Platillo	2do. Platillo
Objeto	$A_3A_2A_1A_0$	$A_3A_2A_1A_0$
21	0 1 0 0	1 0 1 0
22	0 1 0 0	1 0 1 1
23	0 0 1 1	1 0 0 0
24	0 0 1 0	1 0 0 0
25	0 0 1 0	1 0 0 1
26	0 0 0 1	1 0 0 0
27	0 0 0 0	1 0 0 0
28	0 0 0 0	1 0 0 1
29	0 0 0 1	1 0 1 0
30	0 0 0 0	1 0 1 0
31	0 0 0 0	1 0 1 1
32	0 0 1 1	1 1 0 0
33	0 0 1 0	1 1 0 0
34	0 0 1 0	1 1 0 1
35	0 0 0 1	1 1 0 0
36	0 0 0 0	1 1 0 0
37	0 0 0 0	1 1 0 1
38	0 0 0 1	1 1 1 0
39	0 0 0 0	1 1 1 0
40	0 0 0 0	1 1 1 1

Queda como ejercicio generalizar este ejemplo y enunciar un resultado general.

7. Simbología dactilar.

Casi todos los manuales de aritmética de los períodos medieval y renacentista daban cuenta de métodos de simbología dactilar en base 10. En 1966 Froderik Pohl, sugiere un método en base 2, en el cual se empieza con los puños cerrados y los dorsos de las manos vueltos hacia arriba. Un dedo extendido es 1 y un dedo recogido es 0. Así pues para contar desde 1 a 1023 se comienza extendiendo el dedo meñique de la mano derecha. Para indicar el 2 se encoge el meñique y se extiende el anular y así se continúa hasta $1023 = 1111111111$ que se logra con los 10 dedos extendidos.

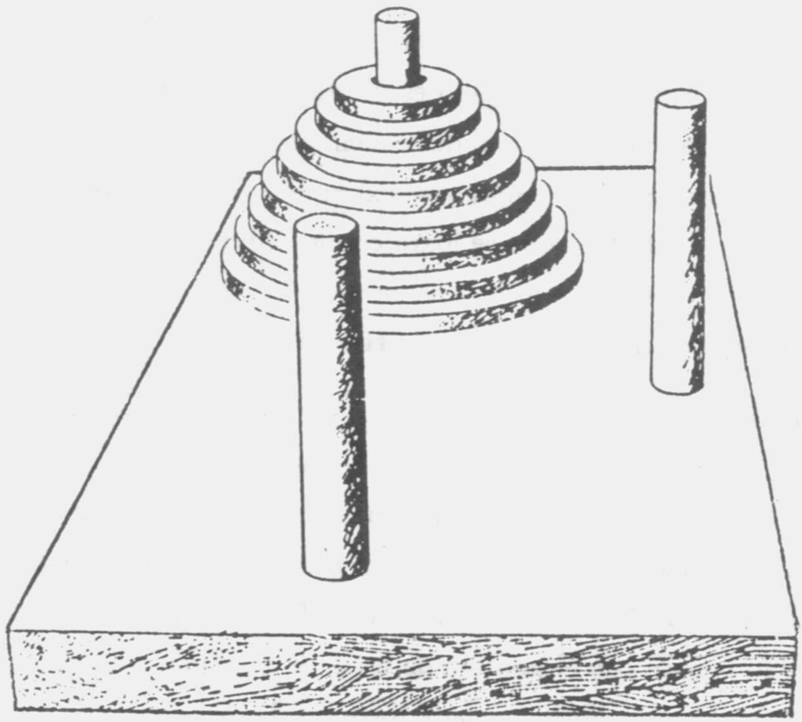
8. Las torres de Brahma y de Hanoi.

Supongamos dadas 3 clavijas en una de las cuales hay 64 discos de diámetros distintos, apilados de mayor a menor. El objeto del juego es transferir los discos de una clavija a otra, uno por vez, y de modo que ningún disco sea montado sobre otro de menor tamaño. Este problema fue planteado por el matemático francés Edouard Lucas y difundido en 1883 y se lo conoce con el nombre de torre de Brahma. La más conocida posee 8 discos y es también llamada torre de Hanoi.

Puede probarse inductivamente (ejercicio), que la cantidad de pasos necesaria es $2^n - 1$. Por ejemplo

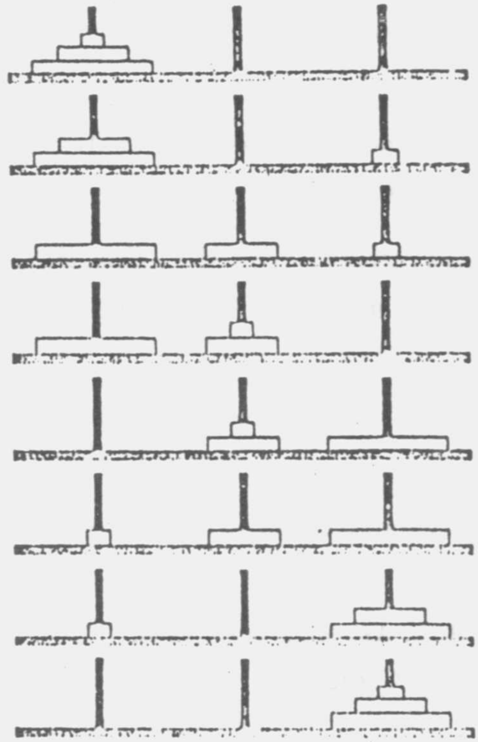
$$2^8 - 1 = 255, \quad 2^{64} - 1 = 18.446.744.073.709.551.615198.$$

En el segundo caso, a razón de un disco por segundo, la tarea completa llevaría aproximadamente $5.846 \mathrm{x}\ 10^6$ años.



TORRE DE HANOI

En la siguiente figura mostramos como transferir 3 discos en 7 pasos, a partir de la posición inicial.



Bibliografía

[B] Biggs N.L., *Discrete Mathematics*, Clarendon Press, Oxford, 1989.

[G1] Martin Gardner, *Nuevos pasatiempos matemáticos*, Alianza Editorial, 1984 . Carnaval matemático (1983)

[G2] Martin Gardner, *Festival mágico matemático*, Alianza Editorial, 1984.

[G3] Martin Gardner, *Máquinas y diagramas lógicos*, Alianza Editorial, 1985.

[G4] Gardner M., *Matemática para divertirse*, Granica Ediciones, 1989.

[Ge1] Gentile E.R., *Notas de Algebra I*, Eudeba (1976).

[Ge2] Gentile E.R., *Aritmética Elemental*, Secretaría General de la OEA, 1985.

[HP] Hashisaki J., Peterson J., *Teoría de la Aritmética*, Centro Regional de Ayuda Técnica, 1969.

[MV] Miatello R.J., Viggiani Rocha M.I., *Divisibilidad de Números Combinatorios. El Teorema de Lucas*, Revista de Educación Matemática, V. 8.2, 1993.

Facultad de Matemática, Astronomía y Física.
Universidad Nacional de Córdoba.

Facultad de Ciencias Exactas y Tecnología.
Universidad Nacional de Tucumán.