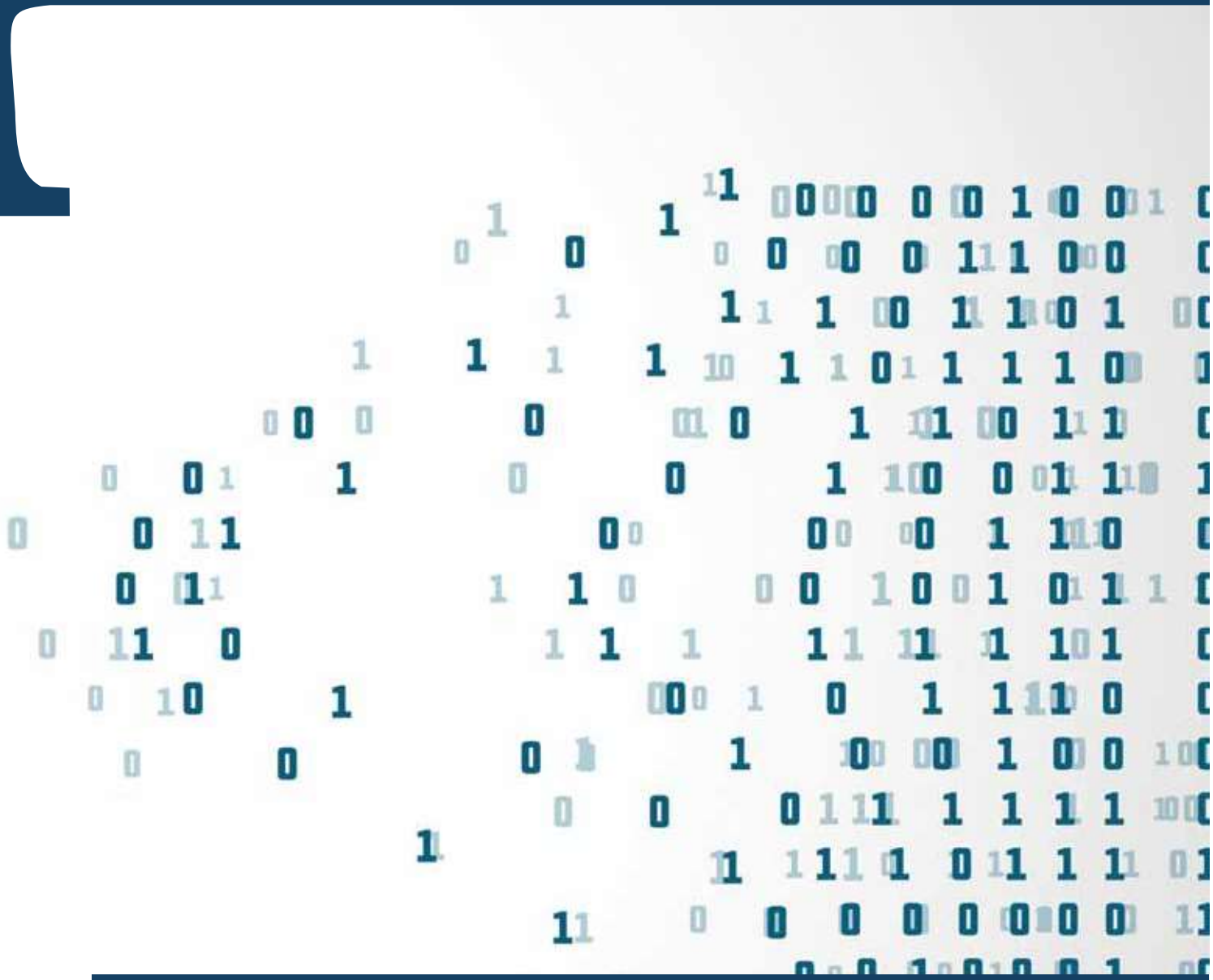

NÚMEROS DE MERSENNE E INVERSOS BINÁRIOS

Guilherme A. Santos[a] e Cristina Serpa[b]

Estudante Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa[a],
Instituto Superior de Engenharia de Lisboa e membro do CMAFcIO[b]

gas.santos@campus.fct.unl.pt[a], mcserpa@fc.ul.pt[b]

Decidimos abordar os números primos não na base decimal, mas sim na base binária. Questionamo-nos então sobre o que aconteceria se em vez de se usar os números como binários normais, tentássemos invertê-los, trocando todos os dígitos 1 por 0 e vice-versa. Assim nasce não só o conceito de inverso binário, mas também todo um conjunto de propriedades e de relações que merecem ser exploradas.

1. INTRODUÇÃO

A pesquisa de números primos é uma tarefa que ocupa uma parte dos interessados pela matemática. Estes números não são apenas uma curiosidade matemática atraente para muitos, mas têm grandes implicações em ciências aplicadas. Nos dias de hoje, esta tarefa está mais concentrada num conjunto muito especial de números primos, os números de Mersenne. Veja-se, por exemplo, o programa *GIMPS – Great Internet Mersenne Prime Search* [6], que obtém estes números com a ajuda de uma grande quantidade de computadores em rede. O último número primo de Mersenne a ser encontrado (em dezembro de 2018), até à data de escrita deste artigo, foi $2^{82589933}-1$, que conta com quase 25 milhões de dígitos e é o 51.º primo de Mersenne. Repare-se que o número 2 é essencial na definição deste tipo de número. Este número em especial tem características únicas que mais nenhum outro tem: por um lado, é o único primo que é par e, por outro, representa a base binária, o sistema de numeração básico na computação. Apesar de os números de Mersenne serem os mais estudados na procura de números primos, o que acontece, de facto, é que a quantidade de números primos existente entre dois números de Mersenne aumenta quanto maiores forem esses números de Mersenne. Este facto pode ser comprovado pela quantidade de números primos que são escritos na base binária sob a forma de n dígitos (veja-se na enciclopédia online de sucessões [7] com a referência A162145).

2. BASES E NÚMEROS DE MERSENNE

Lembremos a representação de números na base binária tal como em [2].

Definição 1. Seja $n \in \mathbb{N}$. Qualquer número inteiro positivo menor ou igual a 2^n-1 pode ser escrito de forma única como representação na base binária por

$$\sum_{s=0}^{n-1} a_s 2^s,\ a_s \in \{0,1\}\,.$$

Analogamente, podemos escrever qualquer número natural sob a forma decimal.

Definição 2. Seja $n \in \mathbb{N}$. Qualquer número natural menor ou igual a 10^n-1 pode ser escrito de forma única como representação de base 10 (decimal) por

$$\sum_{s=0}^{n-1} d_s 10^s,\ d_s \in \{0,1,2,3,4,5,6,7,8,9\}\,. \tag{2.1}$$

Definição 3. Seja $n \in \mathbb{N}$. Chamamos número de Mersenne ao número $M_n = 2^n-1$ e n-ésimo quadrante ao conjunto $Q_n = \{2^n, 2^n+1, \ldots, 2^{n+1}-1\}$. Q_n é o conjunto dos números naturais p tais que $M_n < p \leq M_{n+1}$.

Repare-se que, para cada número natural $p \in \mathbb{N}$, existe $n \in \mathbb{N}$, tal que $p \in Q_n$.

Definição 4. Seja $p \in \mathbb{N}$. Considere-se a sucessão u_n definida por $u_1 = p/2$ e

$$u_{k+1} = \begin{cases} \lfloor u_k \rfloor\,, & k \text{ é ímpar} \\ \frac{\lfloor u_k \rfloor}{2}, & k \text{ é par.} \end{cases}$$

Um número natural $p \in \mathbb{N}$, do n-ésimo quadrante, escreve-se, na base binária, sob a forma

$$p = \sum_{k=1}^{n+1} b_k 2^{k-1}, \tag{2.2}$$

onde $b_k = 2\,(u_{2k-1} - u_{2k}) \in \{0,1\}$.

Na definição dos números de Mersenne está bem presente o número 2. Neste contexto, em paralelo com a definição 3, é possível caracterizar os números de Mersenne através de operações binárias, como adiante se mostra na

proposição 2. Estas operações são aplicadas também a todos os números naturais.

Definição 5. O inverso binário $S(p)$ de um número natural p é obtido pelo algoritmo

i) representar o número p na base binária;

ii) na representação i) substituir o dígito 0 pelo dígito 1 e o dígito 1 pelo dígito 0;

iii) representar o número obtido em ii) na base decimal.

Observação 1. Em computação, o inverso binário corresponde a uma operação chamada complemento um, cujo propósito é representar números com sinal em sistemas binários (veja-se, por exemplo [5, capítulo 4.1]). No entanto, neste texto não o usaremos neste sentido.

Recorrendo à definição 4 da sucessão u_n, é possível representar o inverso binário da seguinte forma.

Proposição 1. *Sejam $n \in \mathbb{N}$ e $p \in Q_n$. Se p tem a representação binária (2.2), então o seu inverso binário é a função $S : \mathbb{N} \to \mathbb{N}$ definida por*

$$S(p) = \sum_{k=1}^{n+1} (1 - b_k)\, 2^{k-1},$$

onde $b_k = 2(u_{2k-1} - u_{2k}) \in \{0, 1\}$.

Agora caracterizamos os números de Mersenne através da sua representação em inverso binário.

Proposição 2. *Um número natural p é de Mersenne se e só se $S(p) = 0$.*

Demonstração. Um número de Mersenne é da forma

$$M_n = 2^n - 1 = \sum_{k=1}^{n} 2^{k-1},$$

para algum $n \in \mathbb{N}$. Tem-se que $\sum_{k=1}^{n} 2^{k-1} = \sum_{k=1}^{n} b_k 2^{k-1}$ se e só se

$$b_k = 1, \forall k \in \{1, \ldots, n\}.$$

Como $b_k = 1 \Leftrightarrow (1 - b_k) = 0$, $\forall k \in \{1, \ldots, n\}$, isto é equivalente a $S(x) = 0$. □

A operação inverso binário S pode ser facilmente obtida se, à partida, se souber em que quadrante o número se encontra.

Proposição 3. *Sejam $n \in \mathbb{N}$ e $p \in Q_n$. Então $S(p) = 2^{n+1} - p - 1$.*

Demonstração. Sejam $n \in \mathbb{N}$ e $p \in Q_n$. Pela forma como p e $S(p)$ se escrevem em base binária, tem-se

$$\begin{aligned} p + S(p) &= \sum_{k=1}^{n+1} b_k 2^{k-1} + \sum_{k=1}^{n+1} (1 - b_k)\, 2^{k-1} \\ &= \sum_{k=1}^{n+1} 2^{k-1} \left((1 - b_k) + b_k \right) \\ &= \sum_{k=1}^{n+1} 2^{k-1} \\ &= 2^{n+1} - 1. \end{aligned}$$

Os corolários que se seguem são imediatos. □

Corolário 1. *Seja $n \in \mathbb{N}$. Então $M_{n+1} = p + S(p)$, $\forall p \in Q_n$.*

Corolário 2. *Seja p um número natural. Então p é par se o seu inverso binário é ímpar e é ímpar se o seu inverso binário é par.*

Corolário 3. *Dentro de um mesmo quadrante Q_n, $S(p)$ é uma função decrescente.*

Corolário 4. *Sejam $n \in \mathbb{N}$ e $p, q \in Q_n$. Então $p - q = S(q) - S(p)$.*

Isto significa que, em particular, dentro de um mesmo quadrante n, o último algarismo do inverso binário de p, $S(p)$, depende apenas do último algarismo de p.

Exemplo 1. Considere-se o quadrante Q_5. Tem-se que 47 (com inverso binário 16) e 57 (com inverso binário 6) pertencem a Q_5. Isto é equivalente a afirmar que sempre que um número natural $p \in Q_5$ tiver como último algarismo o número 7, então o seu inverso binário, $S(p)$, tem como último algarismo o número 6.

Proposição 4. *Sejam $p_1 \in Q_b$ e $p_2 \in Q_a$, com $a, b \in \mathbb{N}$ e $b > a$, tem-se que:*

$$(p_1 - p_2) + (S(p_1) - S(p_2)) = M_{(b-a)} 2^{a+1}.$$

Demonstração.
$(p_1 - p_2) + (S(p_1) - S(p_2)) = (p_1 + S(p_1)) - (p_2 + S(p_2))$. Pela proposição 3 tem-se que, para $p \in Q_n$,

$p + S(p) = 2^{n+1} - 1$. Assim

$$\begin{aligned}(p_1 + S(p_1)) - (p_2 + S(p_2)) &= \left(2^{b+1} - 1\right) - \left(2^{a+1} - 1\right) \\ &= 2^{b+1} - 2^{a+1} = 2^{a+1}\left(2^{b-a} - 1\right) \\ &= 2^{a+1} M_{(b-a)} = M_{(b-a)} 2^{a+1}.\end{aligned}$$

Este resultado permite-nos concluir que a soma das diferenças entre dois números naturais e a dos seus inversos binários são iguais ao produto de um determinado número de Mersenne por uma potência de 2. □

Corolário 5. *Seja $a \in \mathbb{N}$. Considerem-se os números naturais $p_1 \in Q_{a+1}$ e $p_2 \in Q_a$. Então $(p_1 - p_2) + (S(p_1) - S(p_2)) = 2^{a+1}$.*

Demonstração. O resultado obtém-se com $b = a + 1$ na proposição 4. □

Corolário 6. *Sejam $a, b \in \mathbb{N}$ e considerando, sem perda de generalidade, que $b > a$. Então*

$$M_{(b-a)} 2^{a+1} = \sum_{k=a+1}^{b} 2^k.$$

Demonstração. Sejam $a, b \in \mathbb{N}$ e $b > a$. Tem-se

$$\begin{aligned}\sum_{k=a+1}^{b} 2^k &= 2^{b+1} - 2^{a+1} = 2^{a+1}\left(2^{b-a} - 1\right) \\ &= 2^{a+1} M_{(b-a)} = M_{(b-a)} 2^{a+1}.\end{aligned}$$ □

Proposição 5. *Sejam $a \in \mathbb{N}$, $p_1 \in Q_{a+1}$ e $p_2 \in Q_a$, tais que $p_1 = p_2 + 10c$, com $c \in \mathbb{N}$. Então o último algarismo de $S(p_1)$ é o último algarismo da soma do último algarismo de $S(p_2)$ com o último algarismo de 2^{a+1}.*

Demonstração. Considerem-se $a \in \mathbb{N}$, $p_1 \in Q_{a+1}$ e $p_2 \in Q_a$. Pelo corolário 16,

$$(p_1 - p_2) + (S(p_1) - S(p_2)) = 2^{a+1}.$$

Considerem-se os números escritos na base decimal

$$2^{a+1} = \sum_{s=1}^{n-1} d_s 10^s + d_0,\ d_s \in \{0,1,2,3,4,5,6,7,8,9\},$$

e

$$S(p_2) = \sum_{s=1}^{n-1} q_s 10^s + q_0,\ q_s \in \{0,1,2,3,4,5,6,7,8,9\},$$

onde d_0, e q_0 representam o algarismo das unidades. Suponha-se que $p_1 = p_2 + 10c$, com $c \in \mathbb{N}$. Então

$$\begin{aligned}&(p_1 - p_2) + (S(p_1) - S(p_2)) = 2^{a+1} \\ &\Leftrightarrow 10c + (S(p_1) - S(p_2)) = 2^{a+1} \\ &\Leftrightarrow S(p_1) - S(p_2) = 2^{a+1} - 10c \\ &\Leftrightarrow S(p_1) = \left(\sum_{s=1}^{n-1} d_s 10^s + \sum_{s=1}^{n-1} q_s 10^s - 10c\right) + (q_0 + d_0).\end{aligned}$$

Desta última igualdade e sabendo que q_0 e d_0 são os únicos parâmetros que influenciam as unidades, fica provado o pretendido. □

3. PICOS E SUCESSÃO DE LICHTENBERG

Definição 6. Considere-se o sistema $(\mathbb{N}, S)$. Seja $p \in \mathbb{N}$ à sucessão

$$p, S(p), \ldots, S^m(p), \ldots$$

chamamos S-órbita de p, onde $S^0(p) = p$ e $S^{n+1}(p) = S(S^n(p))$.

Observação 2. O sistema $(\mathbb{N}, S)$ pode ser considerado um sistema dinâmico discreto. No entanto, para o propósito deste trabalho, não se afigura necessário associar uma σ-álgebra nem uma medida de probabilidade (veja-se, por exemplo [1]).

Corolário 7. A função $S : \mathbb{N} \to \mathbb{N}$ não é invertível.

Demonstração. Pela proposição 2, todos os números de Mersenne têm imagem 0 pela função S.

Proposição 6. *Sejam $p, a, n \in \mathbb{N}$ tais que p não é um número de Mersenne e $S^{2n-1}(p) \in Q_a$. Então*

$$S^{2n-1}(p) + S^{2n}(p) = 2^{a+1} - 1 = M_{a+1}.$$

Demonstração. Este resultado obtém-se da proposição 3, substituindo p por $S^{2n-1}(p)$ e n por a. □

Proposição 7. *Seja $p \in \mathbb{N}$. Então existe $n \in \mathbb{N}$ tal que $S^n(p) = 0$.*

Demonstração. Seja $p \in \mathbb{N}$. Se p é um número de Mersenne então $S(p) = 0$.

Suponhamos que $p \in Q_m$ não é um número de Mersenne, para certo $m \in \mathbb{N}$. Sabemos, pelo corolário 3, que $S(p)$ é decrescente dentro de cada quadrante e que $1 \leq S(p) \leq 2^m - 1$. Logo $p > S(p)$. Analogamente, $S(p) > S^2(p)$ e $S^n(p) > S^{n+1}(p)$, $\forall n \in \mathbb{N}$. Como $S^n(p)$

é inteiro, $\forall n \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que

$$p > S(p) > S^2(p) > \ldots > S^k(p) = 0. \qquad 3.1)$$

□

Definição 7. Chamamos índice de $p \in Q_m$ ao valor k da equação (3.1). Chamamos pico P_n ao número natural $p \in Q_{n-1}$ tal que, qualquer que seja $q \in Q_{n-1}$, se tem $k(q) \leq k(p)$.

Na prática, chamamos pico ao número natural que, dentro de um mesmo quadrante n, necessita de ser invertido o maior número de vezes de modo a chegar a 0. O pico P_n, por definição, situa-se entre M_{n-1} e o M_n. A existência de apenas um pico por quadrante deve-se ao facto de apenas existir um único número com todos os n dígitos alternados (que é P_n)[1] em cada quadrante.

Pensemos agora na sucessão dos picos P_n e que propriedades poderão ter estes números em especial. Numa pesquisa nas sequências já conhecidas (veja-se [7], A000975), encontra-se esta mesma sucessão chamada de sucessão de Lichtenberg (veja-se [3]), associada ao jogo chinês Baguenaudier[2], indicando o número mínimo de movimentos necessários para resolver um jogo com n anéis. Verifica-se que esta sucessão representa também todos os números cuja representação binária não tem dígitos repetidos consecutivos, por outras palavras, os picos. Uma forma recursiva de obter estes números é $P_{2n} = 2P_{2n-1}$, $P_{2n+1} = 2P_{2n} + 1$ (veja-se [7], A000975). A sua forma explícita é dada por (conforme [8], página 16)

$$P_n = \begin{cases} \frac{1}{3}\left(2^{n+1} - 2\right), & n \text{ é par.} \\ \frac{1}{3}\left(2^{n+1} - 1\right), & n \text{ é ímpar.} \end{cases}$$

Ou (ver [3])

$$P_n = \frac{1}{3}\left(M_{n+1} - 1 + n_0\right),$$

onde $n_0 = n \bmod 2$. A notação para P_n também pode ser l_n (ver [3]).

É também interessante mencionar que esta solução está relacionada com o código de Gray (ver [8]).[3]

Proposição 8. *Seja $n \in \mathbb{N}$. Então*

$$P_{n-1} + P_n = M_n.$$

Este resultado é já conhecido na literatura sobre a sucessão de Lichtenberg (ver [4]).

Das proposições 3 e 8, conclui-se que o inverso binário do pico P_n é o pico P_{n-1}. Como consequência, pelo corolário 2, tem-se que se P_n é par, então P_{n-1} é ímpar e vice-versa.

Mais uma propriedade obtida por Lichtenberg (veja-se [3]), que obtém um pico através de um pico anterior e um número de Mersenne. Esta pode ser obtida como consequência da proposição 8.

Proposição 9. *Seja $n \in \mathbb{N}$. Tem-se que*

$$P_n = P_{n-2} + M_{n-1} + 1.$$

A propriedade seguinte foi também já demonstrada por Lichtenberg (veja-se [3]).

Proposição 10. *Seja $n \in \mathbb{N}$. Então*

$$P_n = 2P_{n-1} + n_0 = \begin{cases} 2P_{n-1} + 1, & n \text{ é par.} \\ 2P_{n-1}, & n \text{ é ímpar,} \end{cases}$$

onde $n_0 = n \bmod 2$.

Neste artigo foram trabalhadas relações entre números de Mersenne e binários. Foi introduzida a noção de pico. Como verificámos, existe um pico entre cada dois números de Mersenne. Várias propriedades foram deduzidas e relacionadas com estes números. Daqui surge-nos a curiosidade de identificar picos que são primos. Pela descrição da sucessão de Lichtenberg ([7], A000975) só o 2 e o 5 são picos primos, isto é, todos os outros picos são compostos. Ou seja, na procura de primos podem descartar-se todos os picos que não sejam 2 e 5. Existem outras relações interessantes sobre estes números ([7], A000975), como sejam jogos: *The brain puzzler*, *Strikketoy*, ou *Knitwear*; construções matemáticas: Hadamard matrix, permutações, coloração de polígonos planares, Hamming distance, estando ainda muito por explorar. Estas últimas relações referidas não são aqui explicadas para não alongar o artigo e aconselha-se o leitor interessado a pesquisar o que significam.

AGRADECIMENTOS

O primeiro autor agradece ao professor Carlos Silva, da Escola Secundária José Afonso, pela inspiração e pela motivação numa fase inicial deste estudo.

A segunda autora agradece o apoio parcial da FCT – Fundação para a Ciência e Tecnologia com a referência UID/MAT/04561/2019.

REFERÊNCIAS

[1] Dajani, K., Kraaikamp, C., *Ergodic Theory of Numbers, The Carus Mathematical Monographs*, No. 29, The Mathematical Association of America, Washington (2002).

[2] Hardy, G.H., Wright, E.M., *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford Science Publications (1979).

[3] Hinz, A. M., *The Lichtenberg Sequence*, Fibonacci Quart., 55 (1) (2017), 2-12.

[4] Hinz, A. M., Klavžar, S. , U. Milutinović, Petr, C., *The Tower of Hanoi – Myths and Maths*, Springer, Basel, (2013).

[5] Knuth, D. E., *The Art of Computer Programming, Vol. 2. Seminumerical algorithms*, Addison-Wesley, USA (1997).

[6] Mersenne Research Inc., *www.mersenne.org*, acedido em 18/05/2019.

[7] Sloane, N. J. A., *The on-line encyclopedia of integer sequences*, disponível em *https://oeis.org/*, acedido em 18/05/2019.

[8] Gardner, M., *The Binary Gray Code. In Knotted Doughnuts and Other Mathematical Entertainments*, New York: W. H. Freeman, pp. 15-17, 1986.

SOBRE OS AUTORES

Guilherme A. Santos Aluno de licenciatura em Matemática da FCT – UNL – Faculdade de Ciência e Tecnologias da Universidade Nova de Lisboa.

Cristina Serpa Professora Adjunta Convidada no ISEL – Instituto Superior de Engenharia de Lisboa e membro integrado no CMAF-cIO – Centro de Matemática, Aplicações Fundamentais e Investigação Operacional.

[1] Veja-se o exemplo dado em [8], página 16.

[2] O jogo consiste numa barra fixa com vários anéis entrelaçados e numa outra barra que está presa a esses anéis. O jogo tem início com uma determinada configuração e termina quando se soltar a barra presa aos anéis da barra fixa. Um movimento faz-se alterando a posição da barra presa aos anéis.

[3] O código de Gray é um sistema de código binário, inventado por Frank Gray, que contém a propriedade de apenas se alterar um único dígito entre dois números sucessivos.