Recorrências, progressões aritméticas e teoria ergódica: teoremas de van der Waerden e de Green-Tao

Telmo Peixe
Jorge Buescu

Universidade de Lisboa

O Teorema de Van der Waerden (1927) é um resultado de teoria dos números e combinatória que foi redemonstrado por Furstenberg em 1977 recorrendo a métodos e resultados de sistemas dinâmicos, nomeadamente de dinâmica topológica. Em 2004, Ben Green e Terence Tao publicaram na web a primeira demonstração de uma conjectura clássica sobre a existência de progressões aritméticas de números primos de comprimento finito arbitrariamente longo. Esses autores recorreram a métodos e resultados de várias áreas da matemática para conseguirem realizar tal demonstração. Neste artigo, dar-se-á a demonstração de Furstenberg do Teorema de Van der Waerden e algumas ideias sobre a estratégia seguida na demonstração do Teorema de Green-Tao.

A partir de 1977 e 1978 começaram a emergir algumas ligações entre os sistemas dinâmicos topológicos e a teoria de números e a combinatória. Desde então têm surgido muitos resultados que relacionam esses dois campos, fornecendo novas formas de encarar alguns teoremas clássicos de teoria dos números e de combinatória. Este fato deve-se essencialmente à reinterpretação de alguns resultados de teoria dos números sob um novo ponto de vista utilizando resultados e estratégias de sistemas dinâmicos.

A interação entre a teoria ergódica e a teoria de números e a combinatória teve a sua gênese essencialmente com a demonstração de Furstenberg do Teorema de Szemerédi ([9]). Esses métodos deram origem a uma nova área na teoria ergódica, designada "teoria de Ramsey ergódica", onde se procura estudar problemas motivados pela combinatória e teoria de números usando teoria ergódica, como por exemplo, o Teorema de Szemerédi e as suas generalizações (incluindo a versão multidimensional [8] e a versão polinomial [2]). Assim, o trabalho de Green e Tao ([17]) abre um novo capítulo na história dessa interação, na medida em que são utilizadas técnicas ergódicas adaptadas ao contexto da teoria dos números para demonstrar uma conjectura de natureza numérica e combinatória.

A teoria de números é um dos ramos mais antigos da matemática. Centra-se essencialmente no estudo dos números naturais $\mathbb{N}$, sendo um pilar fundamental da álgebra. A teoria combinatória envolve questões relacionadas com os números naturais, classes de conjuntos desses números e a estrutura desses conjuntos e classes. A teoria ergódica é a disciplina matemática que estuda sistemas dinâmicos munidos de medidas invariantes, definições que veremos com maior precisão mais adiante.

O objetivo deste trabalho é apresentar as contribuições dos sistemas dinâmicos, nomeadamente da teoria ergódica e da dinâmica topológica, na demonstração dos Teoremas de van der Waerden e de Green-Tao.

No caso do Teorema de van der Waerden, dado que foi demonstrado em 1927 recorrendo a métodos de combinatória e teoria de números, o objetivo deste trabalho é essencialmente compreender como reinterpretar o teorema sob um outro ponto de vista – o dos sistemas dinâmicos. No caso do Teorema de Green-Tao[1], o objetivo é compreender de que forma os autores recorreram a resultados e técnicas de sistemas dinâmicos, nomeadamente de teoria ergódica, como contribuição muito importante em passos fundamentais da demonstração. Deve salientar-se que este objetivo é abordado pelos autores com a consciência de que os resultados de Green e Tao são extremamente profundos e se baseiam em técnicas especiais e não triviais que requerem um estudo detalhado para uma melhor compreensão.

1 Teorema de van der Waerden

No início do século passado (cerca de 1900) P. Baudet e I. Schur ([25], Cap. 34) colocaram o seguinte problema: se o conjunto dos números naturais $\mathbb{N}$ for dividido em dois subconjuntos arbitrários, será que existe necessariamente, em algum desses subconjuntos, uma progressão aritmética de comprimento arbitrário? Recorde-se que:

Definição 1.1. *Uma **progressão aritmética** é uma sucessão de números inteiros da forma $\{a+bj\}_{j=0}^{N-1}$ para $a, b \in \mathbb{Z}$ com $b \neq 0$ e $N \geq 1$ em que N se diz o comprimento da progressão aritmética.*

Exemplos:

1. A sucessão 10, 13, 16, 19, 22, isto é, $\{10+3j\}_{j=0}^{4}$, é uma progressão aritmética em que $a=10$, $b=3$ e $N=5$;
2. A sucessão $-4, 0, 4, 8$, isto é, $\{-4+4j\}_{j=0}^{3}$, é uma progressão aritmética em que $a=-4$, $b=4$ e $N=4$.

Problemas como o de Baudet–Schur chamam-se frequentemente *problemas de coloração*. Imaginando que a partição dos inteiros em duas (ou num número finito de) classes distintas corresponde a colorir todos os elementos da mesma classe com uma única cor, o problema tem tradução imediata em termos de propriedades da coloração. Por exemplo, a conjectura de Baudet–Schur pergunta se, dada uma coloração arbitrária dos inteiros positivos com duas cores, existem progressões aritméticas de comprimento arbitrariamente elevado.

Observe-se que a conjectura de Baudet–Schur não poderia ser fortalecida para afirmar a existência de progressões aritméticas de comprimento infinito. O seguinte exemplo elementar mostra porquê. Consideremos a sucessão nos símbolos $\{0, 1\}$

$$\mathbf{s} = (0\ 11\ 000\ 1111\ 00000 \ldots)$$

construída concatenando blocos alternados de símbolos idênticos cujo comprimento cresce 1 unidade por bloco. Temos assim uma partição $\mathbb{N} = A_0 \cup A_1$, em que A_0 são os inteiros indexados pelo símbolo 0 e A_1 os indexados pelo símbolo 1. É claro que tanto A_0 como A_1 admitem progressões aritméticas de comprimento arbitrariamente elevado: por construção, A_0 contém blocos de inteiros consecutivos de comprimento $2k-1$ e A_1 de comprimento $2k$, para todo o k natural. No entanto, nem A_0 nem A_1 podem conter progressões aritméticas infinitas: em ambos os conjuntos as lacunas (diferenças entre elementos consecutivos do conjunto) crescem ilimitadamente.

Uma construção análoga para a sucessão a dois símbolos 0 e 1

$$\mathbf{t} = (0\ 1\ 00\ 01\ 10\ 11\ 000\ 001\ 010\ 011\ 100\ 101\ 110\ 111 \ldots)$$

composta pela concatenação de todos os 2^k possíveis blocos de comprimento k uma e uma só vez (que corresponde a uma semiórbita positiva densa pelo shift completo a 2 símbolos), origina também uma partição em dois conjuntos A_0 e A_1, ambos contendo progressões aritméticas de comprimento arbitrário mas não contendo nenhuma progressão aritmética infinita (basta notar que cada conjunto contém blocos de k inteiros consecutivos para todo o k).

[1] Este foi um dos trabalhos que contribuiu para a decisão de atribuir a Medalha Fields a Terence Tao em 2006.

Esses dois exemplos poderiam levar a pensar que a existência de lacunas com crescimento ilimitado é essencial para impedir a existência de progressões aritméticas infinitas. Esse não é o caso, como é ilustrado pela partição de $\mathbb{N}$ efetuada pela sequência de Thue-Morse:

$$\mathbf{u} = (0\ 1\ 10\ 1001\ 10010110\ 1001011001101001\ldots)$$

em que o bloco de comprimento 2^{k+1} se obtém recursivamente do bloco de comprimento 2^k por negação binária e concatenação. É fácil verificar, da construção, que ambos os conjuntos A_0 e A_1 têm uma lacuna máxima de 3 (consequência da bem conhecida propriedade de a sequência de Thue-Morse não admitir cubos); no entanto, é possível mostrar que não existem progressões aritméticas de comprimento infinito – como se segue de resultados de Gelfond ([11]) ou, mais simplesmente, de Allouche ([1]). Embora neste caso não seja simples fornecer construtivamente progressões aritméticas de comprimento arbitrariamente elevado apenas com elementos de A_0 ou de A_1, o Teorema de van der Waerden (Teorema 1.2, enunciado em seguida) assegura que pelo menos um dos subconjuntos A_0 ou A_1 tem essa propriedade. Na verdade, tanto A_0 como A_1 a têm, em consequência do Teorema de Szemerédi, conforme veremos adiante (Observação 2.4).

O teorema seguinte é a generalização do problema colocado por P. Baudet e I. Schur, provado por van der Waerden em 1927.

Teorema 1.2 (van der Waerden, 1927)**.** *Para qualquer partição finita dos números naturais, $\mathbb{N} = C_1 \cup \cdots \cup C_r$, existe pelo menos um C_i que contém progressões aritméticas de comprimento arbitrariamente longo.*

Na sua demonstração, van der Waerden ([29]) utilizou essencialmente técnicas de teoria de números e combinatória. No entanto, em 1977-78, Furstenberg e Weiss ([10]) apresentaram uma nova demonstração desse teorema, recorrendo então a sistemas dinâmicos, em particular à dinâmica topológica, como se apresentará nesta seção. Para tal consideremos as seguintes definições:

Definição 1.3. *Define-se **sistema dinâmico** como sendo uma aplicação contínua $T : M \to M$ em que M é um espaço métrico compacto, e que se nota por (M, T). Para $x \in M$, considera-se $T^0(x) = x$ e, para $n \in \mathbb{N}$, $T^n(x) = T(T^{n-1}(x))$, e define-se **órbita de** x como $\mathcal{O}(x) = \{T^n(x) \mid n \in \mathbb{N}\}$.*

Definição 1.4. *Se existe $k \in \mathbb{N}$ tal que $T^k(x) = x$ então x diz-se um **ponto periódico**. Se além disso, para todo o $0 < m < k$, $T^m(x) \neq x$, então x diz-se um **ponto periódico de período mínimo** k. Neste caso, $\mathcal{O}(x)$ contém exatamente k pontos distintos, $\mathcal{O}(x) = \{x, T(x), \ldots, T^{k-1}(x)\}$.*

Definição 1.5. *$x \in M$ diz-se um **ponto recorrente** por T se existir uma sucessão $(n_k)_{k\in\mathbb{N}}$ de números naturais tais que $T^{n_k}(x) \to x$ quando $n_k \to +\infty$, ou seja, se a órbita de x contém uma subsucessão com limite x.*

Observação 1.6. *Usualmente, em dinâmica topológica, define-se o conjunto ω-limite de x como $\omega(x) := \{y \in X : y = \lim_{k\to+\infty} f^{n_k}(x)$, com $n_k \to +\infty$ quando $k \to +\infty\}$. Assim, a definição 1.5 afirma que x é recorrente se, e só se, $x \in \omega(x)$.*

Definição 1.7. *Chama-se **espaço de probabilidade** a $(X, \mathfrak{m}, \mu)$ em que X é um conjunto, $\mathfrak{m}$ é uma σ-álgebra em X (i.e., uma álgebra não vazia de subconjuntos de X que é fechada para a complementação e para uniões enumeráveis) e μ uma medida de probabilidade em $(X, \mathfrak{m})$, i.e, $\mu(X) = 1$.*

Observação 1.8. *Mais geralmente, podem considerar-se espaços de medida finita, i.e, $\mu(X) < +\infty$. Neste caso, pode transformar-se a medida μ numa medida de probabilidade ν, bastando para isso definir $\nu(A) = \frac{\mu(A)}{\mu(X)}$ para cada conjunto mensurável $A \subseteq X$.*

Observação 1.9. *Um caso particularmente útil em sistemas dinâmicos é quando X é um conjunto metrizável compacto e $\mathfrak{m}$ é a respectiva σ-álgebra dos Borelianos, i.e., a σ-álgebra gerada pelos conjuntos abertos de X.*

Definição 1.10. *Considerando o espaço de probabilidade $(X, \mathfrak{m}, \mu)$, diz-se que uma transformação $T : X \to X$ **preserva medida** se $\mu(T^{-1}(A)) = \mu(A)$ para todo o $A \in \mathfrak{m}$.*

A ideia de recorrência é central em sistemas dinâmicos. Mais especificamente, quando o espaço M é limitado num sentido apropriado, por exemplo, tendo medida finita ou sendo compacto, algumas órbitas vão ter necessariamente alguma forma de recorrência, no sentido em que vão retornar arbitrariamente próximo da sua posição original. O primeiro resultado neste contexto foi formulado por Poincaré.

Teorema 1.11 (Teorema de Recorrência de Poincaré, 1890)**.** *Seja $T : X \to X$ uma transformação que preserva medida definida num espaço de probabilidade $(X, \mathfrak{m}, \mu)$. Se A é um conjunto mensurável, então para q.t.p. $x \in A$, existe algum $n \in \mathbb{N}$ tal que $T^n(x) \in A$. Consequentemente, para q.t.p. $x \in A$, existem infinitos $k \in \mathbb{N}$ tais que $T^k(x) \in A$.*

Demonstração. Seja $C_n = \{x \in A : T^j(x) \notin A, \forall j \geq n\}$. O teorema fica demonstrado se provarmos que $C_n \in \mathfrak{m}$ e $\mu(C_n) = 0$, $\forall n \in \mathbb{N}$. Quanto à primeira questão, observando que $C_n = A - \cup_{j=n}^{\infty} T^{-j}(A)$, podemos concluir facilmente que $C_n \in \mathfrak{m}$. Vejamos agora que $\mu(C_n) = 0$. Tem-se

$$C_n = A - \cup_{j=n}^{\infty} T^{-j}(A) \subseteq \cup_{j=0}^{\infty} T^{-j}(A) - \cup_{j=n}^{\infty} T^{-j}(A),$$

donde

$$\mu(C_n) \leq \mu(\cup_{j=0}^{\infty} T^{-j}(A)) - \mu(\cup_{j=n}^{\infty} T^{-j}(A)).$$

Mas como

$$\cup_{j=n}^{\infty} T^{-j}(A) = T^{-n}(\cup_{j=0}^{\infty} T^{-j}(A)),$$

segue-se que

$$\begin{aligned} \mu(\cup_{j=n}^{\infty} T^{-j}(A)) &= \mu(T^{-n}(\cup_{j=n}^{\infty} T^{-j}(A))) \\ &= \mu(\cup_{j=0}^{\infty} T^{-j}(A)), \end{aligned}$$

dado que T é uma transformação que preserva a medida μ. Logo, concluímos que $\mu(C_n) = 0$. □

Um segundo resultado ainda neste contexto é devido a Birkhoff ([3]). Veja-se também Green ([16]).

Teorema 1.12 (Teorema de Recorrência de Birkhoff, 1927)**.** *Seja $T : X \to X$ uma transformação contínua definida em X, espaço topológico compacto. Então X tem um ponto recorrente.*

Tanto o Teorema de Poincaré como o Teorema de Birkhoff estabelecem propriedades de recorrência; no caso do primeiro, o contexto é o da dinâmica que preserva medida, no caso do segundo, é o da dinâmica topológica. Uma versão topológica do teorema 1.11 pode ser encontrada em [19].

Observe-se que o Teorema de Recorrência de Birkhoff é mais fraco do que o Teorema de Recorrência de Poincaré dado que apenas garante a existência de uma órbita recorrente.

Furstenberg ([7]) generalizou esses dois teoremas de recorrência para o contexto de várias transformações que comutam entre si. Consideremos as seguintes definições.

Definição 1.13. *Seja M espaço métrico e sejam $T_1, T_2, \ldots, T_m : M \to M$. Diz-se que T_i e T_j são **transformações que comutam entre si** se $T_i \circ T_j = T_j \circ T_i$, $\forall i, j \in \{1, \ldots, m\}$.*

Definição 1.14. *Um ponto $x \in M$ diz-se **recorrente múltiplo** para $T_1, T_2, \ldots, T_m$ se existe uma sucessão de números naturais $n_k \to +\infty$ com $T_1^{n_k}(x) \to x$, $T_2^{n_k}(x) \to x$, ..., $T_m^{n_k}(x) \to x$, quando $k \to +\infty$.*

O seguinte Teorema de Furstenberg ([6]) generaliza o Teorema de Recorrência de Birkhoff, na medida em que garante a existência de um ponto que é simultaneamente recorrente para um conjunto de transformações que comutam entre si.

Teorema 1.15 (Teorema de Recorrência Múltipla de Birkhoff, 1978)**.** *Seja M um espaço métrico compacto e sejam $T_1, T_2, \ldots, T_m : M \to M$ transformações contínuas que comutam entre si. Então M tem um ponto recorrente múltiplo.*

Observe-se que o Teorema de Recorrência de Birkhoff, por si só, garante apenas a existência de m pontos x_i, em geral distintos, tais que cada x_i é recorrente para o sistema dinâmico (M, T_i), com $i \in \{1, \ldots, m\}$. O Teorema de recorrência múltipla faz uma afirmação muito mais forte: existe um mesmo ponto $x \in M$ recorrente em simultâneo para *todas* as transformações T_i. Mais ainda, a sucessão $(n_k)_{k\in\mathbb{N}}$ que conduz a essa recorrência é a mesma para todas as T_i.

Estes são resultados estudados em teoria ergódica e dinâmica topológica; o objetivo deste trabalho é mostrar como se pode provar o Teorema de van der Waerden a partir do Teorema de Recorrência Múltipla de Birkhoff. Comecemos então por demonstrar, conforme [21], o seguinte resultado:

Proposição 1.16. *Sejam (M, d) um espaço métrico compacto, $T : M \to M$ uma transformação contínua e $x_0 \in M$. Então, para todo o $\ell \geq 1$ e todo o $\epsilon > 0$, existe $y \in \mathcal{O}(x_0)$ e $n \geq 1$ tal que $y, T^n(y), T^{2n}(y), \ldots, T^{\ell n}(y)$ distam menos de ϵ uns dos outros.*

Demonstração. Seja Y o fecho da órbita de x_0: $Y = \overline{\mathcal{O}(x_0)}$, e sejam $T_1 = T$, $T_2 = T^2$, $T_3 = T^3$, ..., $T_\ell = T^\ell$. Então Y é um espaço métrico compacto e as transformações $T_1, T_2, \ldots, T_\ell$ formam um conjunto de transformações definidas em Y e com valores em Y que comutam. Pelo Teorema de Recorrência Múltipla de Birkhoff existe um ponto recorrente múltiplo $y' \in Y$, i.e., existe uma sucessão de números naturais $n_k \to +\infty$ tal que

$$T_1^{n_k}(y') \to y', T_2^{n_k}(y') \to y', \ldots, T_\ell^{n_k}(y') \to y'.$$

Em particular, para algum $n = n_k$, segue-se que

$$y', T_1^n(y'), T_2^n(y'), \ldots, T_\ell^n(y') \in B_{\epsilon/2}(y'),$$

em que $B_{\epsilon/2}(y')$ representa a bola aberta de centro em y' e raio $\epsilon/2$, donde, para cada $i \in \{1, \ldots, \ell\}$, existe $\gamma_i > 0$ tal que

$$B_{\gamma_i}(T_i^n(y')) \subseteq B_{\epsilon/2}(y').$$

Assim, como T_i^n é contínua, para todo o $\gamma_i > 0$, existe $\delta_i > 0$ tal que, se $z \in B_{\delta_i}(y')$, então

$$T_i^n(z) \in B_{\gamma_i}(T_i^n(y')).$$

Se tomarmos $\delta = \min\{\delta_1, \delta_2, \ldots, \delta_\ell, \epsilon/2\}$, segue-se que, se $z \in B_\delta(y')$, então

$$T_i^n(z) \in B_{\epsilon/2}(y').$$

Como $y' \in Y = \overline{\mathcal{O}(x_0)}$, segue-se que existe $y = T^m(x_0) \in \mathcal{O}(x_0)$ tal que

$$y \in B_\delta(y') \subseteq B_{\epsilon/2}(y').$$

Então, para todo o $i \in \{1, \ldots, \ell\}$, $T_i^n(y) \in B_{\epsilon/2}(y')$. Assim, $y = T^m(x_0)$ satisfaz

$$d(T_i^n(y), T_j^n(y)) < \epsilon, \forall i, j \in \{0, \ldots, \ell\},$$

em que $T_0^n = T^{0n} = Id$. Mas como $T_i^n(y) = T^{in}(y)$, $\forall i \in \{0, \ldots, \ell\}$, tem-se

$$d(T^{in}(y), T^{jn}(y)) < \epsilon, \forall i, j \in \{0, \ldots, \ell\}.$$

□

Define-se em seguida um sistema dinâmico ao qual se aplicará a Proposição 1.16. Considere-se $\Gamma = \{1, 2, \ldots, q\}$ um conjunto finito de símbolos a partir do qual se constrói o espaço $X = \Gamma^{\mathbb{N}}$ de todas as sucessões semi-infinitas de elementos de Γ. Assim, uma sucessão $x \in X$ é da forma $x = (x_0, x_1, x_2, \ldots)$ em que cada $x_i \in \Gamma$. Define-se em X a aplicação $d : X \times X \to \mathbb{R}$ dada por $d(x, x) = 0$ e $d(x, y) = \frac{1}{k+1}$ para $x \neq y$, em que k é o menor inteiro tal que $x_k \neq y_k$. Facilmente se comprova que d define uma métrica (produto) em X, pelo que (X, d) é um espaço métrico compacto (pois X é o produto cartesiano de conjuntos finitos, cada um dos quais munido com a topologia discreta, é compacto, o que pelo Teorema de Tychonoff implica a compacidade de X). Considere-se agora a aplicação $T : X \to X$ definida por $T(x) = y$ em que $y_i = x_{i+1}$ para todo o $i \in \mathbb{N}_0$. É a este sistema dinâmico (X, T) que se vai aplicar a Proposição 1.16. Assim, tomando $x \in X$ e $0 < \epsilon < 1$, tem-se que para qualquer $\ell \geq 1$, existem $y \in \mathcal{O}(x)$ e $n \geq 1$ tais que $y, T^n(y), T^{2n}(y), \ldots, T^{\ell n}(y)$ distam menos de ϵ uns dos outros, ou seja, são sucessões infinitas que coincidem no primeiro termo. Mostrou-se assim o resultado:

Proposição 1.17. *Para qualquer $x \in X$ e qualquer $\ell \geq 1$, existem $m, n \geq 1$ tais que $x_m = x_{m+n} = x_{m+2n} = \cdots = x_{m+\ell n}$.*

Demonstração do Teorema de van der Waerden: Seja $\ell \in \mathbb{N}$ e seja $\mathscr{P}$ uma partição de $\mathbb{N}$ em q subconjuntos, $\mathbb{N} = C_1 \cup \cdots \cup C_q$. A partição $\mathscr{P}$ determina um elemento $x = (x_1, x_2, x_3, \ldots) \in \Gamma^{\mathbb{N}}$ da seguinte forma: $x_j = i$ se

$j \in C_i$. Aplicando a Proposição 1.17, segue-se que existe $m \geq 1$ tal que

$$x_m = x_{m+n} = x_{m+2n} = \cdots = x_{m+\ell n},$$

donde os inteiros $m, m+n, m+2n, \ldots, m+\ell n$ pertencem todos ao mesmo C_i para algum $i \in \{1, \ldots, q\}$, e portanto C_i contém uma progressão aritmética de comprimento $\ell + 1$. □

2 Teorema de Green-Tao

Alguns registros históricos evidenciam que a procura de padrões aditivos nos números primos tem sido um assunto recorrente na história da matemática. Uma conjectura clássica que muito estimulou a curiosidade dos matemáticos, provavelmente devido à sua simplicidade de apresentação e dificuldade de demonstração, afirma que no conjunto dos números primos existem progressões aritméticas de comprimento arbitrariamente longo.

Considere-se alguns exemplos de progressões aritméticas de primos (conforme [27], atualizado):

- 2
- $2, 3$
- $3, 5, 7$
- $5, 11, 17, 23$
- $5, 11, 17, 23, 29$
- $7, 37, 67, 97, 127, 157$
- $7, 157, 307, 457, 607, 757$
- $\ldots$
- $5749146449311 + 26004868890n$, $n = 0, \ldots, 20$, e também $11410337850553 + 4609098694200n$, $n = 0, \ldots, 21$ (Moran, Pritchard e Thyssen ([24]), em 1995)
- $56211383760397 + 44546738095860n$, $n = 0, \ldots, 22$ (Frind, Underwood e Jobling ([4]), em 2004)
- $515486946529943 + 136831 \times 223092870n$, $n = 0, \ldots, 23$, e também $6171054912832631 + 366384 \times 223092870n$, $n = 0, \ldots, 24$ (Chermoni e Wroblewski ([23]), em 2008)
- $43142746595714191 + 23681770 \times 223092870n$, $n = 0, \ldots, 25$ (Perichon ([23]), em 2010)

A origem desta conjectura clássica sobre os números primos não é de todo surpreendente, dado que a existência de progressões aritméticas arbitrariamente longas nos primos é sugerida por heurísticas relativamente simples baseadas no Teorema dos Números Primos e abaixo explicitadas. Note-se que a inexistência de progressões aritméticas de comprimento infinito nos primos se segue de resultados clássicos de teoria dos números que afirmam que as lacunas entre primos podem ser arbitrariamente grandes.

No restante deste artigo, $|A|$ representa a cardinalidade do conjunto A e $\sim$ representa "assintoticamente equivalente" quando $N \to +\infty$.

Teorema 2.1 (Teorema dos Números Primos de Hadamard e de la Vallée Poussin, 1896)**.** *Para $N \in \mathbb{N}$ suficientemente grande, tem-se que*

$$|\{p \text{ primo} : p \leq N\}| \sim \frac{N}{\log N} \sim \int_2^N \frac{dx}{\log x}.$$

Tendo por base este teorema podem desenvolver-se heurísticas relativamente simples que sugerem a existência de aproximadamente $\frac{N^2}{(\log N)^k}$ progressões aritméticas de comprimento k constituídas por primos, $p_1, \ldots, p_k$, em que cada p_i é no máximo N. A seguinte argumentação segue de perto Green ([15]).

Pelo Teorema dos Números Primos tem-se que,

$$\mathbb{P}(x \text{ é primo } : 1 \leq x \leq N) \sim \frac{1}{\log N},$$

em que $\mathbb{P}(x \text{ é primo } : 1 \leq x \leq N)$ representa a probabilidade de um inteiro entre 1 e N ser primo. Considere-se agora o conjunto de todas as progressões aritméticas de comprimento k

$$x, x+d, \ldots, x+(k-1)d,$$

com $x, d \in \{1, \ldots, N\}$. Escolhendo x e d ao acaso de entre as N^2 possibilidades e notando E_j como o acontecimento "$x + jd$ é primo, para $j \in \{0, \ldots, k-1\}$", tem-se

$$\mathbb{P}(E_j) \sim \frac{1}{\log N}\,.$$

Assumindo que os acontecimentos E_j são independentes, tem-se consequentemente

$$\begin{aligned}&\mathbb{P}(x, x+d, \ldots, x+(k-1)d \text{ são primos})\\ &\quad = \mathbb{P}\Big(\bigwedge_{j=0}^{k-1} E_j\Big) \sim \frac{1}{(\log N)^k}\,,\end{aligned}$$

donde se poderá concluir que $|\{x, d \in \{1, \ldots, N\} : x, x+d, \ldots, x+(k-1)d \text{ são primos}\}| \sim \frac{N^2}{(\log N)^k}$, que representa uma função crescente de N, para k fixo.

Outras conjecturas (algumas das quais ainda em aberto) que foram surgindo ao longo da história evidenciam um interesse continuado na procura de padrões aditivos nos primos, como se pode ver por meio dos seguintes exemplos:

(1) A Conjectura dos Primos Gêmeos (ainda em aberto), que se pensa ser devida a Euclides (cerca de 300 AC): existem infinitos pares da forma $(p, p+2)$ de números primos que distam duas unidades entre si: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $\ldots$;

(2) A Conjectura de Goldbach dos Números Ímpares (1742, em aberto): qualquer número ímpar maior ou igual a sete pode ser escrito como soma de três números primos: $7 = 2+2+3$, $9 = 2+2+5$, $11 = 3+3+5, \ldots$;

(3) A Conjectura de Goldbach dos Números Pares (Euler, 1742, em aberto): qualquer número par maior ou igual a quatro pode ser escrito como soma de dois números primos: $4 = 2+2$, $6 = 3+3$, $8 = 3+5, \ldots$;

(4) Teorema de Lagrange e Waring (1770): toda a progressão aritmética de primos com comprimento k tem razão divisível por todos os primos menores do que k (em particular, não existem progressões aritméticas infinitas de primos);

(5) Teorema de Dirichlet sobre primos em progressões aritméticas (1837): se k e ℓ são inteiros positivos primos entre si, i.e., $\mathrm{mdc}(k, \ell) = 1$, então a progressão aritmética ℓ, $\ell + k$, $\ell + 2k$, $\ell + 3k$, $\ldots$ contém infinitos primos. Por exemplo, $\{3 + 4j\}_{j \in \mathbb{N}_0} = \{\mathbf{3}, \mathbf{7}, \mathbf{11}, 15, \mathbf{19}, \mathbf{23}, 27, \mathbf{31}, 35, \ldots\}$;

(6) Conjectura de Hardy e Littlewood (1923): se $a_1, \ldots, a_k$ e $b_1, \ldots, b_k$ são inteiros não negativos tais que $P(x) = \prod_{i=1}^{k} (a_i x + b_i)$ não é identicamente 0 $(\mathrm{mod}\ p)$ com p primo, então existem infinitos inteiros n tais que $\{a_i n + b_i : 1 \leq i \leq k\}$ é constituído apenas por números primos;

Observação 2.2. *Esta conjectura inclui a conjectura dos primos gêmeos vista em (1) como um caso particular e trivialmente implica que o conjunto dos números primos contém progressões aritméticas arbitrariamente longas ([18]).*

(7) Teorema de van der Waerden (1927): para qualquer partição finita dos números naturais, $\mathbb{N} = C_1 \cup \cdots \cup C_r$, existe um C_i que contém progressões aritméticas de comprimento arbitrariamente longo (finito);

(8) Conjectura de Erdös e Turan (1936): todo o conjunto $A \subset \mathbb{N} \setminus \{0\}$ tal que

$$\sum_{a \in A} \frac{1}{a} = +\infty$$

contém progressões aritméticas arbitrariamente longas (em aberto, inclusive para progressões aritméticas de comprimento três; este era um dos "prize money problems" de Paul Erdös pelo qual ele oferecia uma quantia em dinheiro a quem o conseguisse resolver);

Observação 2.3. *Em 1737, Euler mostrou que, sendo P o conjunto dos números primos,*

$$\sum_{p \in P} \frac{1}{p} = +\infty\,.$$

Assim, a conjectura (8) é uma forma forte de generalização do Teorema de Green-Tao.

(9) Teorema de Vinogradov (1937): qualquer número ímpar suficientemente grande pode ser escrito como soma de três números primos (Liu e Wang em 2002 mostraram que todo o $n > 10^{1346}$ ímpar se escreve como soma de três primos);

(10) Teorema de van der Corput (1939): existem infinitas progressões aritméticas de primos de comprimento três;

(11) Teorema de Roth (1956): se $A \subseteq \mathbb{Z}$ tem densidade superior positiva, i.e.,

$$d^*(A) := \limsup_{N\to+\infty} \frac{1}{N}|A \cap \{1,\ldots,N\}| > 0\,,$$

então A contém infinitas progressões aritméticas de comprimento três;

(12) Teorema de Chen (1966): existe um número infinito de pares da forma $(p, p+2)$ com p primo e $p+2$ quase-primo (número que é primo ou produto de dois primos): $(3,5)$, $(7,9)$, $(11,13)$, $(13,15)$, $(17,19)$, $(19,21)$, $(23,25)$, $\ldots$;

(13) Teorema de Szemerédi (1975): se $A \subseteq \mathbb{Z}$ tem densidade superior positiva, então A contém infinitas progressões aritméticas de comprimento k, para todo o $k \geq 3$ inteiro;

Observação 2.4. *Este teorema implica o Teorema de van der Waerden (1927). Em particular, mostra a existência de progressões aritméticas de comprimento arbitrariamente longo em ambos os conjuntos da partição de* $\mathbb{N}$ *efetuada pela sequência de Thue-Morse, referida na Seção 1.*

(14) Teorema de Heath-Brown (1981): existem infinitas progressões aritméticas de comprimento quatro, em que três dos elementos são primos e um é quase-primo;

(15) Teorema de Balog (1992): para todo o k inteiro positivo, existem $p_1, \ldots, p_k$ primos distintos tais que $\frac{p_i+p_j}{2}$ também é primo, $\forall i, j \in \{1,\ldots,k\}$. Por exemplo, para $k = 2$, tem-se que 3 e 7 são primos e $\frac{3+3}{2} = 3$, $\frac{3+7}{2} = 5$ e $\frac{7+7}{2} = 7$ também são primos. Para $k = 3$, tem-se que $3, 7$ e 19 também satisfazem as condições do resultado de Balog;

(16) Teorema de Green-Tao (2004): o conjunto dos números primos contém infinitas progressões aritméticas de comprimento k, para qualquer $k \geq 1$ inteiro;

(17) Teorema de Green e Tao (2004): existem infinitas progressões aritméticas de comprimento três constituídas por primos de Chen (primos p em que $p+2$ é quase-primo). Por exemplo: $(3,5,7)$, $(5,11,17)$, $(3,11,19)$, $\ldots$;

(18) Teorema de Tao e Ziegler (2006): sejam $P_1, \ldots, P_k$ polinômios em $\mathbb{Z}[x]$ tais que $P_i(0) = 0$, $\forall i \in \{1,\ldots,k\}$. Então existe um número infinito de inteiros n e r tais que $n + P_1(r), \ldots, n + P_k(r)$ são todos primos.

O principal objetivo nesta seção é salientar os passos fundamentais (evitando as definições formais e questões técnicas não triviais) que Green e Tao desenvolveram para demonstrar o Teorema (enunciado anteriormente em (16)) acerca da existência de progressões aritméticas nos primos.

Teorema 2.5 (Teorema de Green-Tao)**.** *O conjunto dos números primos contém infinitas progressões aritméticas de comprimento k, para qualquer $k \geq 1$ inteiro.*

Em [17], Green e Tao provam uma afirmação mais forte do que a referida no Teorema 2.5. Eles mostram que qualquer subconjunto "suficientemente denso" dos primos contém progressões aritméticas arbitrariamente longas (finitas).

Teorema 2.6 (Teorema de Szemerédi nos primos ([17]))**.** *Seja A um subconjunto dos números primos com*

$$\limsup_{N\to+\infty} \frac{1}{\pi(N)}|A \cap \{1,\ldots,N\}| > 0\,,$$

em que $\pi(N)$ é o número de primos em $\{1,\ldots,N\}$. Então A contém infinitas progressões aritméticas de comprimento k, para todo o inteiro $k \geq 1$.

Observação 2.7. *Para $k = 3$, este resultado foi provado por Green ([14]).*

O Teorema 2.5, de Green e Tao, é um resultado de alguma forma surpreendente, resolvendo uma conjectura antiga que ao longo dos tempos atraiu muita investigação. A sua demonstração é extremamente interessante dado que resulta da fusão de métodos e resultados de teoria de números, teoria ergódica, análise harmônica, combinatória e geometria discreta, sendo também por isso mais exigente a sua compreensão detalhada. O ponto de partida é o célebre Teorema de Szemerédi de 1975, enunciado em (13). Uma das ideias fundamentais da demonstração é a generalização desse teorema, mostrando que um subconjunto denso de uma família suficientemente *pseudo-aleatória* (termo que será explicado mais abaixo) de inteiros contém progressões aritméticas arbitrariamente longas.

Existem três pontos fundamentais na demonstração. O primeiro é o Teorema de Szemerédi em si próprio. No entanto, como o conjunto dos números primos não tem densidade superior positiva, o Teorema de Szemerédi não pode ser diretamente aplicado, sendo então o segundo ponto fundamental da demonstração de Green e Tao um determinado princípio de transferência que vai permitir a aplicação do Teorema de Szemerédi num contexto mais geral. Assim, será possível deduzir do Teorema de Szemerédi que qualquer subconjunto de um conjunto suficientemente pseudo-aleatório de densidade relativa positiva contém progressões aritméticas de comprimento arbitrariamente longo. O terceiro ponto fundamental é o uso de propriedades específicas dos primos e da sua distribuição, baseados em resultados recentes de Goldston e Yildirim ([12]) que mostram que o Teorema de Szemerédi "generalizado" se pode aplicar ao conjunto dos números primos.

2.1 Demonstração do Teorema de Green-Tao: ideias fundamentais

Como foi anteriormente referido, o Teorema de Green e Tao não pode ser obtido diretamente do Teorema de Szemerédi porque o conjunto dos números primos tem densidade superior nula (como é relativamente fácil verificar diretamente pela definição de densidade superior e do Teorema 2.1). A ideia foi então modificar o Teorema de Szemerédi para o contexto dos números primos.

Green e Tao designam o Teorema 2.6 por *Teorema de Szemerédi nos primos* dado que, se se substituir o subconjunto dos números primos pelo conjunto dos inteiros positivos $\mathbb{Z}^+$, obtém-se o Teorema de Szemerédi ([26]), enunciado em (13). Esse teorema refere-se a um subconjunto dos inteiros com densidade superior positiva. No entanto, existem outras formulações equivalentes desse teorema. Apresentamos em seguida uma versão finita.

Proposição 2.8 (Teorema de Szemerédi finito ([26])**.** *Seja $\delta > 0$ um número real fixo e seja $k \geq 3$ um inteiro. Então existe $N_0(\delta, k) < \infty$ tal que, se $N \geq N_0(\delta, k)$ e $A \subset \{1, \dots, N\}$ com $|A| \geq \delta N$, A contém uma progressão aritmética de comprimento k.*

Existem várias demonstrações do Teorema de Szemerédi. A demonstração original de Szemerédi ([26]) é essencialmente combinatória. No entanto, como se mencionou no capítulo anterior, em 1977, Furstenberg proporcionou um desenvolvimento muito importante com a apresentação de uma demonstração do Teorema de Szemerédi usando essencialmente argumentos de teoria ergódica ([9]; ver também [5] e [22]).

Green e Tao desenvolvem os seus argumentos no contexto finito de $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$, com N primo suficientemente grande, contrastando com o contexto usual da teoria ergódica no qual se usam estratégias mais fracas (como o Axioma da Escolha) para passar para um sistema infinito que preserva medida. Os autores clarificam que no contexto finito se podem usar argumentos e conceitos da teoria ergódica, pois os erros em que se incorre não são significativos, na medida em que envolvem termos que tendem para zero no infinito.

Apresentamos em seguida uma outra formulação do Teorema de Szemerédi que sugere uma analogia mais próxima com a teoria ergódica. Green e Tao usam a notação de esperança condicional

$$\mathbb{E}(f(x) \mid x \in B) := \frac{1}{|B|} \sum_{x \in B} f(x)$$

para representar a média por f de como as variáveis x estão ordenadas no conjunto B, e usam $o(1)$ para representar uma quantidade que tende para zero quando $N \to +\infty$.

Proposição 2.9 (Teorema de Szemerédi reformulado)**.** *Sejam $0 < \delta \leq 1$ um número real e $k \geq 3$ um inteiro. Se N é um inteiro suficientemente grande e $f : \mathbb{Z}_N \to \mathbb{R}^+$ uma função não negativa tal que, $0 \leq f(x) \leq 1$ para todo o $x \in \mathbb{Z}_N$ e $\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) \geq \delta$, então*

$$\begin{aligned} &\mathbb{E}(f(x)f(x+r)\dots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N) \\ &\qquad \geq c(k,\delta) - o_{k,\delta}(1) \end{aligned}$$

para alguma constante $c(k,\delta) > 0$, independente de f e de N, e $o_{k,\delta}(1)$ um termo que depende de k e δ e que tende para zero no infinito.

Existem duas diferenças fundamentais entre esta formulação e a versão finita. Uma é que nesta formulação nos encontramos num contexto de funções e não de conjuntos. Contudo, observe-se que podemos passar do contexto de conjuntos para funções usando, por exemplo, argumentos probabilísticos. A outra diferença é que o Teorema de Szemerédi reformulado implica a existência de aproximadamente N^2 progressões aritméticas e não apenas uma, como afirma o Teorema de Szemerédi finito. No entanto, esse resultado pode ser deduzido a partir do Teorema de Szemerédi finito usando um artifício combinatório, e que os próprios autores afirmam ser um argumento não trivial. Uma demonstração do Teorema de Szemerédi reformulado pode ser encontrada em [28].

Definição 2.10. *Diz-se que $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ é uma **medida**[2] se*

$$\mathbb{E}(\nu(x) \mid x \in \mathbb{Z}_N) = 1 + o(1)\,.$$

Green e Tao consideram uma classe de medidas, que designam de *k-pseudo-aleatória*, que satisfazem uma *condição de formas lineares* e uma *condição de correlação*, em termos do parâmetro k. Sem dar as definições formais, que podem ser encontradas em [17], salientamos que essas duas condições estão relacionadas com o conceito de *weak-mixing* da teoria ergódica. Essas medidas são as que interessam, pois têm suporte em conjuntos relativamente esparsos. A generalização da Proposição 2.9 para o contexto de uma medida k-pseudo-aleatória é dada pelo seguinte teorema.

Teorema 2.11 (Teorema de Szemerédi relativo a uma medida k-pseudo-aleatória ([17]))**.** *Sejam $0 < \delta \leq 1$ um número real e $k \geq 3$ um inteiro. Suponhamos que $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ é k-pseudo-aleatória*[3]*. Se N é um inteiro suficientemente grande e $f : \mathbb{Z}_N \to \mathbb{R}^+$ é uma função não negativa tal que, $0 \leq f(x) \leq \nu(x)$ para todo o $x \in \mathbb{Z}_N$ e $\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) \geq \delta$, então*

$$\begin{aligned} &\mathbb{E}(f(x)f(x+r)\dots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N) \\ &\qquad \geq c(k,\delta) - o_{k,\delta}(1) \end{aligned}$$

para alguma constante $c(k,\delta) > 0$, independente de f e de N, e $o_{k,\delta}(1)$ um termo que depende de k e δ e que tende para zero no infinito.

No primeiro passo da demonstração deste teorema começa, mais especificamente, a investigação original de Green e Tao quando abordam mais profundamente os argumentos de Gowers ([13]). Se $f : \mathbb{Z}_N \to \mathbb{R}^+$ é uma função, então a contagem normalizada de progressões aritméticas de comprimento k

$$\mathbb{E}(f(x)f(x+r)\dots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N)$$

é controlada por certas normas $\|\cdot\|_{U^d}$, que Green e Tao designam por *normas uniformes de Gowers* e cujas definições formais se podem encontrar em [17]. Os autores usam o termo *uniforme de Gowers* para, de um modo geral, descrever uma função que é pequena relativamente

[2] Considerando $\nu_{const} \equiv 1$ como a distribuição de probabilidade uniforme em $\mathbb{Z}_N$, podemos ver ν como outra distribuição de probabilidade num subconjunto de $\mathbb{Z}_N$ de densidade muito pequena (por exemplo, nos quase-primos de $[1, N]$).

[3] Conforme definição formal, uma medida ser *k-pseudo-aleatória* significa que é uma medida pseudo-aleatória que satisfaz em k as condições de formas lineares e de correlação.

a alguma norma $\|\cdot\|_{U^d}$. Salientam ainda que esse termo não deve ser confundido com o termo *pseudo-aleatório*, que neste contexto apenas diz respeito às medidas em $\mathbb{Z}_N$.

Em termos gerais, a demonstração do Teorema 2.11 baseia-se essencialmente num argumento que não é mais do que uma mistura de argumentos quantitativos de teoria ergódica conjuntamente com algumas estimativas combinatórias relacionadas com as *normas (uniformes) de Gowers* e a regularidade esparsa dos hipergrafos. Deve salientar-se que uma parte significativa das ideias chave de Green e Tao se concretizam na demonstração desse teorema (constitui as seções 4-8 das 10 secções essenciais que compõem todo o artigo).

O passo seguinte de Green e Tao é a aplicação do Teorema 2.11 ao caso específico dos primos, estabelecendo um "majorante pseudo-aleatório" para uma versão modificada da função de von Mangoldt Λ, definida por

$$\Lambda(n) = \begin{cases} \log p & \text{se } \exists\, m \in \mathbb{N} \text{ e } p \text{ primo t.q. } n = p^m\,, \\ 0 & \text{caso contrário,} \end{cases}$$

e que pode ser vista como uma função característica dos primos.

Observação 2.12. *Usando propriedades algébricas dos inteiros e da função logaritmo, é fácil mostrar que a função de von Mangoldt satisfaz*

$$\sum_{d|n} \Lambda(d) = \log n, \forall n \in \mathbb{N}\,,$$

afirmação que é equivalente ao Teorema Fundamental da Aritmética.

Uma possível escolha para ν (como medida pseudo-aleatória) seria a função Λ, mas infelizmente, verificar que Λ satisfaz a condição de formas lineares e a condição de correlação é quase tão difícil como mostrar que os primos contêm progressões aritméticas longas. Assim, Green e Tao procuraram uma medida ν que majorasse a função Λ pontualmente e, baseando-se no trabalho recente de Goldston e Yildirim ([12]) sobre o tamanho das lacunas nos primos, definiram uma medida com as características procuradas. Uma vantagem da escolha dessa medida é que a prova de que satisfaz a condição de formas lineares e a condição de correlação se baseia essencialmente no trabalho já realizado por Goldston e Yildirim.

Pelo Teorema 2.1 (Teorema dos Números Primos) tem-se que o valor médio $\Lambda(n)$ é $1 + o(1)$. Para se provar o Teorema 2.5 (Teorema de Green-Tao, assim como o Teorema 2.6 (Teorema de Szemerédi nos primos), será suficiente definir uma medida $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ tal que $\nu(n) \geq c(k)\Lambda(n)$ para alguma constante $c(k) > 0$ (que apenas depende de k) e que seja k-pseudo-aleatória. Infelizmente, tal medida não pode existir dado que os primos, assim como a função de von Mangoldt, se concentram em certas classes de resíduos, o que impossibilita, por exemplo, encontrar um majorante k-pseudo-aleatório com a propriedade desejada $\nu(n) \geq c(k)\Lambda(n)$.

Para contornar essa dificuldade, Green e Tao desenvolvem um artifício, que designam por "W-truque", que lhes permite eliminar as obstruções aritméticas à pseudo-aleatoriedade que advém dos primos pequenos. Assim, definindo uma nova função, que designam por função de von Mangoldt modificada $\tilde{\Lambda}$, conseguem garantir a existência de uma medida k-pseudo-aleatória que majora os primos, de acordo com a proposição seguinte.

Proposição 2.13. *Considere-se $\epsilon_k := \frac{1}{2^k(k+4)!}$ e seja N um número primo suficientemente grande. Então existe uma medida k-pseudo-aleatória $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ tal que $\nu(n) \geq k^{-1}2^{-k-5}\tilde{\Lambda}(n)$ para todo o $\epsilon_k N \leq n \leq 2\epsilon_k N$.*

Finalmente, usando esta Proposição e o Teorema 2.11, Green e Tao provam a existência de progressões aritméticas arbitrariamente longas nos primos (Teorema 2.5).

3 Conclusão

Através deste trabalho podemos aperceber-nos de que forma se pode encarar um problema de teoria de números e combinatória sob o ponto de vista dos sistemas dinâmicos. Essa foi uma área que emergiu na matemática em meados dos anos 1970 com matemáticos como Furstenberg, Weiss, Hindman, Bergelson, entre outros.

As estratégias que têm sido desenvolvidas no campo que relaciona teoria de números e combinatória com sistemas dinâmicos, para além de terem sido úteis na reinterpretação de resultados de teoria de números e combinatória, têm também sugerido outros problemas de interesse independente dentro do campo dos sistemas dinâmicos. Veja-se, por exemplo, [6].

Um dos grandes objetivos do estudo das estratégias desenvolvidas por Green e Tao na demonstração do seu teorema ([17]) é compreender de que forma estas podem ser adaptadas para se poderem obter novos resultados utilizando teoria ergódica. Podemos referir, a título de exemplo, a utilização da teoria ergódica para mostrar a existência de padrões em certos conjuntos com densidade zero.

Assim, podemos esperar que a ligação entre essas áreas da matemática, aparentemente tão distintas, possa continuar a produzir resultados matematicamente importantes como foi a demonstração do Teorema de Green e Tao.

Agradecimentos. Os autores agradecem ao Professor Pedro Duarte, Professor Jorge Nuno Silva, Professor Miguel Ramos e Professor Costa Pereira pelas conversas construtivas e sugestões para melhor esclarecimento de alguns assuntos. Agradecemos em particular aos *referees* anônimos pela leitura atenta do artigo e pelas correções e sugestões realizadas, e que foram integradas na presente versão do artigo. A procura de exemplos não triviais de aplicação do Teorema de van der Warden, sugerida pelos referees, levou a que Peixe e Buescu contactassem os autores Jeffrey Shallit e Jean-Paul Allouche apresentando-lhes uma conjectura relacionada com a sequência de Thue-Morse. Esta conjectura despertou o interesse dos autores, Johannes F. Morgenbesser, Jeffrey Shallit e Thomas Stoll tendo-os motivado para a descoberta de resultados que foram recentemente publicados em [20].

Referências

[1] ALLOUCHE, J.-P. Somme des chiffres et transcendance. *Bulletin de la Societé Mathématique de France*, v. 110, n. 3, p. 279–285, 1982.

[2] BERGELSON, V.; LEIBMAN, A. Polynomial extensions of van der Waerden's and Szemerédi's theorems. *Journal of the American Mathematical Society*, v. 9, p. 725–753, 1996.

[3] BIRKHOFF, G. D. *Dynamical systems.* New York: AMS, 1927. (American Mathematical Society. Colloquium Publications, 9)

[4] FRIND, M.; JOBLING, P.; UNDERWOOD, P. *23 primes in arithmetic progression.* Disponível em *<http://primes.plentyoffish.com>*

[5] FURSTENBERG, H. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *Journal d'Analyse Mathématique*, v. 31, p. 204–256, 1977.

[6] FURSTENBERG, H. *Recurrence in ergodic theory and combinatorial number theory*. Princeton: Princeton University Press, 1981.

[7] FURSTENBERG, H. Poincaré recurrence and number theory. *Bulletin of the American Mathematical Society*, v. 5, n. 3, p. 211–234, 1981.

[8] FURSTENBERG, H.; KATZNELSON, Y. An ergodic Szemerédi theorem for commuting transformations. *Journal d'Analyse Mathématique*, v. 34, p. 275–291, 1979.

[9] FURSTENBERG, H.; KATZNELSON, Y.; ORNSTEIN, D. The ergodic theoretical proof of Szemerédi's Theorem. *Bulletin of the American Mathematical Society*, v. 7, n. 3, p. 527–552, 1982.

[10] FURSTENBERG, H.; WEISS, B. Topological dynamics and combinatorial number theory. *Journal d'Analyse Mathématique*, v. 34, p. 61–85, 1978.

[11] GELFOND, A. O. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arithmetica*, v. 13, p. 259–265, 1967/1968.

[12] GOLDSTON, D. A.; YILDIRIM, C. Y. Higher correlation of divisor sums related to primes. III. Small gaps between primes. *Proceedings of the London Mathematical Society. Third Series.* v. 95, n. 3, p. 653–686, 2007.

[13] GOWERS, T. A new proof of Szemerédi's theorem. *Geometric and Functional Analysis*, v. 11, n. 3, p. 465–588, 2001.

[14] GREEN, B. Roth's theorem in the primes. *Annals of Mathematics*, v. 161, p. 1609–1636, 2005.

[15] GREEN, B. Long arithmetic progressions of primes. *Clay Mathematics Proceedings*, v. 7, p. 149–167, 2007.

[16] GREEN, B. *Van der Waerden by topological dynamics.* University of Cambridge, 2008. Disponível em: *<http://www.dpmms.cam.ac.uk/∼bjg23/ergodic/top-dynamics-1.pdf>*

[17] GREEN, B.; TAO, T. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, v. 167, p. 481–547, 2008.

[18] KRA, B. The Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view. *Bulletin of the American Mathematical Society*, v. 43, n. 1, p. 3–23, 2006.

[19] MAÑÉ, R. *Introdução à teoria ergódica.* Rio de Janeiro: IMPA, 1983. (Projeto Euclides)

[20] MORGENBESSER, J. F.; SHALLIT, J.; STOLL, T. Thue-Morse at multiples of an integer. *Journal of Number Theory*, v. 131, n. 8, p. 1498–1512, 2011.

[21] MULVEY, I. Recurrent ideas in number theory: the Multiple Birkhoff Recurrence Theorem used to prove van der Waerden's Theorem. *Mathematics Magazine*, v. 70, n. 5, p. 358–361, 1997.

[22] POLLICOTT, M.; YURI, M. *Dynamical systems and ergodic theory.* Cambridge: Cambridge University Press, 1998. (London Mathematical Society Student Texts, 40)

[23] PRIMES in Arithmetic Progression Records. Disponível em *<http://users.cybercity.dk/∼dsl522332/math/aprecords.htm>*

[24] PRITCHARD, P.; MORAN, A.; THYSSEN, A. Twenty-two primes in arithmetic progression. *Mathematics of Computation*, v. 64, p. 1337–1339, 1995.

[25] SOIFER, A. *The mathematical coloring book: mathematics of coloring and the colorful life of its creators*. With forewords by Branko Grünbaum, Perer D. Johnson Jr., and Cecil Rousseau. New York: Springer, 2009.

[26] SZEMERÉDI, E. On sets of integers containing no k elements in arithmetic progression. *Acta Arithmetica*, v. 27, p. 199–245, 1975.

[27] TAO, T. Long arithmetic progressions in the primes. In: ANNUAL MEETING OF THE AUSTRALIAN MATHEMATICAL SOCIETY, 50. Sydney: AustMS, 2006.

[28] TAO, T. A quantitative ergodic theory proof of Szemerédi's theorem. *Electronic Journal of Combinatorics*, v. 13, n. 1, R99, 2006.

[29] VAN DER WAERDEN, B. L. Beweis einer Baudetschen vermutung. *Nieuw Archief voor Wiskunde*, v. 15, p. 212–216, 1927.

Telmo Peixe - `telmopeixe@gmail.com`
Jorge Buescu - `jbuescu@ptmat.fc.ul.pt`

Departamento de Matemática
Faculdade de Ciências
Universidade de Lisboa
1749-016 Lisboa, Portugal