UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

DE FERMAT A GAUSS-GEGENBAUER: DINÂMICA DE CONGRUÊNCIAS, COLARES E PALAVRAS

Maria Cristina Gonçalves Silveira de Serpa

MESTRADO EM MATEMÁTICA

2011

UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

DE FERMAT A GAUSS-GEGENBAUER: DINÂMICA DE CONGRUÊNCIAS, COLARES E PALAVRAS

Maria Cristina Gonçalves Silveira de Serpa

Dissertação orientada pelo Prof. Doutor

Jorge Sebastião de Lemos Carvalhão Buescu

MESTRADO EM MATEMÁTICA

2011

Resumo

O recurso a sistemas dinâmicos para estudar resultados de outras áreas da matemática, incluindo da matemática discreta, tem sido objecto de recentes trabalhos publicados. O pequeno teorema de Fermat, por exemplo, foi provado usando aplicações do círculo. De facto, é possível obter a congruência deste teorema através da contagem de pontos e órbitas periódicos de certo tipo de aplicações do círculo. O mesmo método pode ser usado para uma alargada generalização que é conhecida desde 1863, quando foi publicado um artigo póstumo de Gauss. A sua notação usual é devida a Gegenbauer. Apresenta-se uma notação combinatória alternativa para este resultado. Este é diferente da mais conhecida generalização: o teorema de Euler. Também existem demonstrações destes resultados usando os conceitos de palavra primitiva, palavra de Lyndon e colar. Neste trabalho mostra-se a relação entre a dinâmica de determinadas aplicações do círculo e palavras e colares. Estabelecem-se bijecções identificando cada órbita com um colar aperiódico, correspondendo a identificá-la com uma palavra de Lyndon. De facto, é possível obter todas as palavras primitivas (ou palavras de Lyndon) de comprimento n num alfabeto de cardinalidade a através de todas as órbitas de período mínimo n da aplicação do círculo $a \cdot x \pmod 1$. Reciprocamente, tendo uma palavra primitiva (ou palavra de Lyndon), podem calcular-se explicitamente os pontos da órbita periódica correspondente. Apresentam-se algumas aplicações em termos de linguagens faladas, nomeadamente utilizando as cifras de César e Atbash.

Palavras chave: congruência, palavra primitiva, palavra de Lyndon, colar, aplicação do círculo, cifra de César, cifra de Atbash

Abstract

The use of dynamical systems to study results in other areas of mathematics, including discrete mathematics, has been the subject of recent work. Fermat's little theorem, for instance, has been proved using circle maps. In fact, it is possible to obtain the congruence of this theorem by counting periodic orbits and points of certain circle maps. The same method can be used to a generalization of Fermat's little theorem known since 1863, when a posthumous paper of Gauss was published. Its usual notation is due to Gegenbauer. We give an alternative combinatorial notation for this result. This result differs substantially from the most common generalization, the Euler theorem. There are proofs of these results using the concepts of primitive word, Lyndon word and necklace. In this work we establish a relation between the dynamics of certain circle maps with words and necklaces. We set up bijections identifying each periodic orbit with an aperiodic necklace, which corresponds to identifying it with a Lyndon word. In fact, it is possible to obtain all primitive words (or Lyndon words) of length n over a finite alphabet of cardinality a through all the orbits of minimum period n of the circle map $a \cdot x \pmod 1$. Conversely, having a primitive word (or Lyndon word) we can compute explicitly the points of the corresponding periodic orbit. We give some applications in terms of spoken languages, namely, using the Caesar and Atbash ciphers.

Keywords: congruence, primitive word, Lyndon word, necklace, circle map, Caesar cipher, Atbash cipher

In memoriam

Aos meus avós, tios e irmão, que recordo com eterna saudade.

Dedicatória

Dedico este trabalho a todas as pessoas que partilharam, partilham e/ou partilharão comigo a alegria de viver, o gosto pela ciência e/ou a busca da verdade.

Agradecimentos

Em primeiro lugar agradeço ao meu orientador Prof. Jorge Buescu pelo seu entusiasmo, rigor e abertura. A primeira selecção de artigos científicos sugerida por ele foi decisiva para a concretização do tema aqui desenvolvido. O seu apoio foi fundamental para o bom desenrolar do trabalho ao longo do ano. Também foi muito estimulante o encorajamento que me deu para a divulgação dos resultados obtidos, tanto a nível da submissão a uma revista científica, como na apresentação de palestras. Agradeço ainda a disponibilidade que manifestou para me continuar a apoiar futuramente, no caso de eu seguir para doutoramento.

Estou grata ao Prof. Nuno da Costa Pereira pela sua atenta discussão sobre a parte relacionada com teoria dos números e, em especial, sobre a notação combinatória que lhe apresentei referente à generalização do pequeno teorema de Fermat dada por Gauss e Gegenbauer.

Os meus agradecimentos vão também para as comissões organizadoras dos eventos *Recreational Mathematics Colloquium II* e *NOMA'11 - International Workshop on Nonlinear Maps and their Applications*, que tiveram lugar na Universidade de Évora, respectivamente, de 27 a 30 de Abril de 2011 e de 15 e 16 de Setembro de 2011, pela disponibilidade demonstrada para eu participar apresentando palestras. Em ambos os casos, a receptividade dos participantes foi muito positiva. De facto, demonstram interesse em saber mais sobre o tema e em ter conhecimento do artigo que, entretanto, foi submetido para publicação.

Não posso deixar de agradecer aos meus colegas e amigos que me foram acompanhando desde o início da minha licenciatura até hoje. Foram muitos e bons os momentos que passámos juntos. Estes superam largamente os menos bons. As discussões sobre variados temas incluíam frequentemente questões

matemáticas que me ajudaram a amadurecer o conhecimento desta ciência, em paralelo com o amadurecimento enquanto pessoa humana. O entusiasmo, a alegria, o companheirismo que encontrei são inesquecíveis. Espero que me perdoem alguma falha minha, mas errar faz parte do ser humano e perdoar é uma dádiva.

Agradeço a todo o pessoal docente e não docente que contribuiu de alguma forma para a formação académica que hoje tenho, com o seu profissionalismo e simpatia.

Por último, mas não menos importante, estou grata por todo o apoio incondicional da minha família. A base de toda a minha persistência no estudo está nela. Sem ela sei que não teria sido capaz.

A todos muito obrigada.

Conteúdo

Lista de Tabelas

Lista de Figuras

"A Matemática é o alfabeto com o qual Deus escreveu o Universo."

Galileu Galilei

1 Introdução

No desenvolvimento da Matemática foram surgindo várias áreas e ramos de especialização distintos. Muito embora cada um deles tenha métodos e temáticas diferentes, existem interligações entre eles, que, por vezes, são inesperados e/ou desconhecidos. Neste trabalho vai ser feita uma interligação entre várias áreas da Matemática: teoria dos números, linguagens formais, combinatória e sistemas dinâmicos.

O assunto que vai ser tratado tem a sua origem num teorema de Pierre de Fermat, conhecido como pequeno teorema de Fermat, para ser distinguido do grande ou último teorema de Fermat. A demonstração do autor não é conhecida; no entanto, existem muitas formas de o demonstrar, recorrendo em geral a argumentos de divisibilidade e de contagem. Em primeiro lugar, sendo este um teorema clássico de teoria de números ele está incluído nos manuais desta área da Matemática (tais como, [6] e [10]), que só por si têm várias demonstrações alternativas. Veja-se, por exemplo, a selecção de demonstrações

em [25] que incluem as clássicas de autores como Leibniz, Euler, Lambert, Ivory e Thue.

Outra forma de demonstrar este resultado é através de contagens de objectos. No século XIX Petersen forneceu uma demonstração muito simples, recorrendo à ideia de contar caixas coloridas dispostas em círculos. Esta técnica é hoje em dia tratada através do estudo de colares, que são essencialmente conjuntos de símbolos, ou letras, dispostos em círculo. Recentemente foi feita uma abordagem dinâmica apresentando demonstrações através de aplicações do círculo (veja-se, por exemplo, [2], [9], [12] e [24]). A opção de provar este resultado via teoria de grupos também é possível (veja-se [13]).

Estes métodos demonstrativos são ainda mais poderosos, permitindo generalizar bastante o pequeno teorema de Fermat muito para além da generalização mais conhecida, o teorema de Euler. Deles podem obter-se congruências sem qualquer restrição nos parâmetros (números naturais) essenciais para o teorema de Fermat. Enquanto resultado de teoria dos números, esta generalização foi descoberta por Gauss que a apresentou como uma expressão algo longa, publicada em 1863. A versão usual foi dada, em 1900, por Gegenbauer por meio do símbolo de somatório envolvendo a função de Möbius.

O argumento de contagem de objectos advém de existir uma propriedade relacionada com os conjuntos que os agregam, que se refere à cardinalidade. É pois um facto que o número de colares aperiódicos de comprimento n formados por a diferentes tipos de símbolos é igual ao número de órbitas periódicas de período mínimo n de um determinado sistema dinâmico com a ramos (veja-se o capítulo 4). Esta coincidência entre objectos completamente distintos e de áreas da Matemática diferentes implica a existência de uma bijecção entre este dois conjuntos. Neste trabalho apresenta-se uma bijecção natural que faz a ligação entre estes dois tipos de objectos. Esta deriva da existência de uma correspondência biunívoca entre itinerários truncados de órbitas periódicas e palavras primitivas.

Este trabalho está organizado da seguinte forma. Depois de um primeiro capítulo introdutório, no segundo capítulo são dados os resultados do pequeno teorema de Fermat e suas generalizações na perspectiva da teoria dos números,

bem como algumas propriedades de funções aritméticas que também serão utilizadas nos capítulos seguintes. No terceiro capítulo introduzem-se os conceitos relacionados com as linguagens formais convergindo para a demonstração via colares dos resultados principais do segundo capítulo. O quarto capítulo aborda estes resultados numa perspectiva dinâmica, isto é, apresenta sistemas dinâmicos (aplicações do círculo) que permitem demonstrar o pequeno teorema de Fermat e generalizações. Vai ainda mais além fazendo a interligação entre os objectos tratados no terceiro capítulo e estas aplicações do círculo através da apresentação de bijecções adequadas. O último capítulo ilustra algumas aplicações dos resultados do capítulo precedente no sentido de os apresentar na óptica das linguagens faladas. Aborda ainda uma perspectiva virada para a área da criptografia, referindo consequências de aplicar as cifras de César e Atbash nos colares e sistemas dinâmicos estudados anteriormente.

2

O pequeno teorema de Fermat e suas generalizações

2.1 O pequeno teorema de Fermat

Neste capítulo o ponto de partida é o pequeno teorema de Fermat, um teorema que remonta, de acordo com o que se sabe (veja-se [6]), a 1640 através de uma carta remetida pelo próprio ao seu correspondente Bernhard Frénicle de Bessy, onde referiu não incluir a demonstração por recear ser demasiado longa. A sua prova foi pela primeira vez publicada por Euler em 1736, apesar de Leibniz ter feito uma demonstração anterior com argumentos idênticos num trabalho que não publicou. O enunciado transcrito na carta era o seguinte:

Teorema 2.1. *(**Pequeno teorema de Fermat**) Se p é um primo e a é um inteiro arbitrário não divisível por p, então p divide $a^{p-1} - 1$.*

Existem várias provas para este teorema; indicar-se-á uma das apresentadas

em [6].

Demonstração. Sejam p um primo e a um inteiro tais que $p \nmid a$.

Considerem-se os primeiros $p-1$ múltiplos positivos de a, isto é, os inteiros $a, 2a, 3a, \ldots, (p-1)\,a$. Nenhum destes números é congruente módulo p com qualquer outro, nem com zero.

De facto, se $ra \equiv sa \pmod{p}$, com $1 \leq r < s \leq p-1$, então pode cortar-se a e obter $r \equiv s \pmod{p}$, o que não é verdade. Portanto, os inteiros listados acima são congruentes módulo p com $1, 2, 3, \ldots, (p-1)$, por alguma ordem.

Multiplicando todas estas congruências obtém-se

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)\,a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \tag{2.1}$$

pelo que

$$a^{p-1}\,(p-1)! \equiv (p-1)! \pmod{p}. \tag{2.2}$$

Mas como $p \nmid (p-1)!$, pode cortar-se $(p-1)!$ e obter

$$a^{p-1} \equiv 1 \pmod{p}, \tag{2.3}$$

que expressa o enunciado do teorema. □

Veja-se outra versão equivalente, mas um pouco mais geral, deste teorema, pois não impõe restrições sobre a.

Teorema 2.2. *Sejam p um primo e a um inteiro, então*

$$a^p \equiv a \ (mod\ p). \tag{2.4}$$

Demonstração. Se $p|a$, tem-se $a^p \equiv 0 \equiv a \pmod{p}$.

Se $p \nmid a$, basta multiplicar ambos os membros da congruência (2.3) por a. □

Note-se que as formulações (2.3) e (2.4) são equivalentes, pelo que pode dizer-se que o pequeno teorema de Fermat é dado por uma das duas formas alternativas.

2.2 Funções aritméticas

Neste trabalho, para o que se vai seguir, interessa generalizar este resultado. Tendo em vista este propósito introduzir-se-ão conceitos e resultados que permitem fazer isso (veja-se, por exemplo, [6] e [10]).

Definição 2.3. Uma *função aritmética* é uma função cujo domínio é o conjunto de números inteiros positivos. Diz-se que uma função aritmética é *multiplicativa* se $f(mn) = f(m) f(n)$ sempre que $\text{mdc}(m, n) = 1$.

Teorema 2.4. *Seja f uma função multiplicativa. Então a função F definida por $F(n) = \sum_{d|n} f(d)$ também é multiplicativa.*

Demonstração. (conforme [6]) Sejam m e n dois inteiros positivos primos entre si. Cada divisor d de mn pode ser escrito de forma única como um produto de um divisor d_1 de m e de um divisor d_2 de n, com $\text{mdc}(d_1, d_2) = 1$. Logo,

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) \\ &= F(m) F(n), \end{aligned}$$

pelo que F é uma função multiplicativa. □

A função definida já de seguida tem o nome do seu autor que a apresentou em 1832 com a notação de a_n (veja-se [8]).

Dado $n \in \mathbb{N}$, seja

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \tag{2.5}$$

a sua factorização em primos.

Definição 2.5. A *função de Möbius* $\mu(n)$ é definida da seguinte forma:

(i) $\mu(1) = 1$;

(ii) $\mu(n) = 0$ se em (2.5) algum $\alpha_j \geq 2$;

(iii) $\mu(n) = (-1)^k$ se $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$.

Teorema 2.6. *Para todo o* $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}. \tag{2.6}$$

Demonstração. (conforme [6]) A prova é feita por casos.

No caso em que $n = 1$, tem-se $\sum_{d|1} \mu(d) = \mu(1) = 1$.

Para $n = p^k$, seja $F(n) = \sum_{d|n} \mu(d)$. Então

$$\begin{aligned} F(n) &= \sum_{d|p^k} \mu(d) \\ &= \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu\left(p^k\right) \\ &= \mu(1) + \mu(p) \\ &= 1 + (-1) \\ &= 0. \end{aligned}$$

Para o caso geral, como μ é uma função multiplicativa pode aplicar-se o teorema 2.4. Utilizando a factorização em números primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ obtém-se $F(n) = F\left(p_1^{k_1}\right) F\left(p_2^{k_2}\right) \cdots F\left(p_r^{k_r}\right) = 0$. □

Lema 2.7. Sejam c, d e n números inteiros. Então

$$d|n \wedge c|\,(n/d) \Leftrightarrow c|n \wedge d|\,(n/c)\,. \tag{2.7}$$

Demonstração. Suponha-se que $d|n \wedge c|\,(n/d)$. Então existem a e b tais que $n = ad$ e $n/d = bc$. Logo $a = bc$, $n = bcd$ e $n/c = bd$, isto é, $c|n$ e $d|\,(n/c)$.

O recíproco é idêntico trocando os papéis de d com c. □

Teorema 2.8. ***(Fórmula de inversão de Möbius)*** *Sejam F e f duas funções aritméticas relacionadas pela fórmula*

$$F(n) = \sum_{d|n} f(d). \tag{2.8}$$

Então

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d). \tag{2.9}$$

Observação 2.9. Os dois somatórios em (2.9) são iguais uma vez que d e $d' = \frac{n}{d}$ são variáveis mudas que tomam o mesmo conjunto de valores.

Demonstração. (conforme [6]) Fazendo os cálculos, tem-se

$$\begin{aligned}\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c) \right) \\ &= \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d)\, f(c) \right).\end{aligned}$$

Pela propriedade (2.7), obtém-se

$$\begin{aligned}\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) &= \sum_{c|n} \left(\sum_{d|(n/c)} f(c)\, \mu(d) \right) \\ &= \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right).\end{aligned}$$

Aplicando o teorema 2.6 sabe-se que $\sum_{d|(n/c)} \mu(d) = 0$, excepto para $n/c = 1$,

isto é, para $n = c$, caso em que $\sum_{d|(n/c)} \mu(d) = 1$. Assim,

$$\begin{aligned}\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right) \\ &= \sum_{c=n} (f(c) \cdot 1) \\ &= f(n),\end{aligned}$$

que é o resultado pretendido. □

Definição 2.10. Chama-se *função de Euler* à função $\phi(m)$ que dá o número de inteiros positivos primos com m que não são maiores que m. Isto é, dá o número de inteiros n tal que $0 < n \leq m$ e m.d.c. $(n, m) = 1$.

Observação 2.11. A função de Euler é multiplicativa e para p primo tem-se $\phi(p) = p - 1$.

Teorema 2.12. *Sejam p um número primo e $k > 0$. Então*

$$\phi\left(p^k\right) = p^k - p^{k-1}. \tag{2.10}$$

Demonstração. (conforme [6]) É claro que mdc $\left(n, p^k\right) = 1$ se e só se $p \nmid n$. Existem p^{k-1} inteiros entre 1 e p^k divisíveis por p. Estes são p, $2p$, $3p$, ..., $p^{k-1}p$.

Então o conjunto $\left\{1, 2, \ldots, p^k\right\}$ tem exactamente $p^k - p^{k-1}$ inteiros que são relativamente primos com p^k. Logo, por definição obtém-se $\phi\left(p^k\right) = p^k - p^{k-1}$. □

Corolário 2.13. Sejam p um número primo e $k > 0$. Então

$$\phi\left(p^{k+1}\right) = p\phi\left(p^k\right). \tag{2.11}$$

Demonstração. Pelo teorema anterior, verifica-se que

$$\phi\left(p^{k+1}\right) = p^{k+1} - p^k. \tag{2.12}$$

Logo

$$\begin{aligned}\phi\left(p^{k+1}\right) &= p^{k+1} - p^k \\ &= p\left(p^k - p^{k-1}\right) \\ &= p\phi\left(p^k\right),\end{aligned}$$

o que conclui a demonstração. □

2.3 O teorema de Euler

A generalização usual do pequeno teorema de Fermat é o teorema de Euler, ou teorema de Fermat-Euler, como por vezes também é conhecido (veja-se [6] e [10]).

Teorema 2.14. *(**Teorema de Euler**) Sejam a, m inteiros tais que m.d.c.$(a, n) = 1$. Então*

$$a^{\phi(n)} \equiv 1 \ (mod\ n). \tag{2.13}$$

Demonstração. (conforme [6]) Primeiro suponha-se que $n = p^k$, com p primo, $p \nmid a$ e $k > 0$ e prova-se, por indução em k, que

$$a^{\phi\left(p^k\right)} \equiv 1 \pmod{p^k}. \tag{2.14}$$

Para $k = 1$, a expressão (2.14) reduz-se a $a^{\phi(p)} \equiv 1 \pmod{p}$, que é o pequeno teorema de Fermat.

Suponha-se que (2.14) se verifica para certo k. Veja-se que também se verifica para $k + 1$.

Pelo corolário 2.13 tem-se

$$\begin{aligned}a^{\phi\left(p^{k+1}\right)} &= a^{p\phi\left(p^k\right)} \\ &= \left(a^{\phi\left(p^k\right)}\right)^p.\end{aligned}$$

Por (2.14) sabe-se que existe um inteiro q tal que $a^{\phi\left(p^k\right)} = 1 + qp^k$. Usando o

teorema binomial obtém-se

$$\begin{aligned} a^{\phi\left(p^{k+1}\right)} &= \left(a^{\phi\left(p^{k}\right)}\right)^{p} \\ &= \left(1+qp^{k}\right)^{p} \\ &= 1+\binom{p}{1}qp^{k}+\binom{p}{2}\left(qp^{k}\right)^{2}+\cdots+\binom{p}{p-1}\left(qp^{k}\right)^{p-1}+\left(qp^{k}\right)^{p} \\ &\equiv 1+\binom{p}{1}qp^{k} \pmod{p^{k+1}}. \end{aligned}$$

Mas $p|\binom{p}{1}$, pelo que $p^{k+1}|\binom{p}{1}qp^{k}$. Aplicando à última congruência tem-se

$$a^{\phi\left(p^{k+1}\right)} \equiv 1 \pmod{p^{k+1}}, \tag{2.15}$$

que conclui a prova por indução de (2.14).

Considere-se m.d.c. $(a,n)=1$ e a factorização de n em números primos $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Para cada $i \in \{1,2,\ldots,r\}$ aplique-se a congruência (2.14):

$$a^{\phi\left(p_i^{k_i}\right)} \equiv 1 \pmod{p_i^{k_i}}. \tag{2.16}$$

Como $\phi(n)$ é divisível por $\phi\left(p_i^{k_i}\right)$, pode elevar-se cada membro destas congruências a $\phi(n)/\phi\left(p_i^{k_i}\right)$ e obter

$$a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}. \tag{2.17}$$

Na medida em que os $p_i^{k_i}$ são primos entre si, obtém-se

$$a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}} \tag{2.18}$$

que é o mesmo que (2.13). □

2.4 Outras generalizações

Como foi visto, dados dois inteiros n e a, as congruências até agora estabelecidas têm restrições. No primeiro caso exige-se que n seja um número primo (pequeno teorema de Fermat) e, na sua generalização usual (teorema de Euler) tem-se ainda uma restrição de m.d.c. $(a, n) = 1$.

O próximo passo de generalização é obter congruências sem restrições em n e a. Esquematicamente pode sintetizar-se esta ideia através da tabela 2.1 (conforme [24]).

	m.d.c. $(a, n) = 1$	$\forall a$
$n = p$ primo	Fermat: $a^{p-1} \equiv 1 \pmod{p}$	$a^p \equiv a \pmod{p}$
n composto	Euler: $a^{\phi(n)} \equiv 1 \pmod{n}$	?

Tabela 2.1: A questão da generalização do pequeno teorema de Fermat.

Segundo Dickson, na sua descrição da história da teoria dos números (veja-se [8]) o resultado que se pretende é conhecido e foi apresentado de várias formas. Ele refere que a primeira versão foi conhecida a partir de um artigo póstumo de Gauss, publicado em 1863, que afirmava que se $N = p_1^{e_1} \cdots p_s^{e_s}$, onde $p_1, \cdots, p_s$ são primos distintos, então

$$F(a, N) = a^N - \sum_{i=1}^{s} a^{N/p_i} + \sum_{i<j} a^{N/p_i p_j} - \sum_{i<j<k} a^{N/p_i p_j p_k} + \ldots + (-1)^s a^{N/p_1 \ldots p_s}$$

é divisível por N. Nos anos 1882 e 1883 foram dadas quatro demonstrações directas deste resultado por Kantor, Weyr, Lucas e Pellet. A formulação mais usada actualmente foi dada em 1900 por Gegenbauer, estabelecendo que $F(a, n) = \sum_{d|n} \mu(d)\, a^{n/d}$. O resultado preciso é o seguinte.

Teorema 2.15. *Para quaisquer a, n inteiros positivos,*

$$\sum_{d|n} \mu(d)\, a^{n/d} \equiv 0 \pmod{n}. \tag{2.19}$$

Demonstração. Suponha-se, em primeiro lugar, que n é divisível por um único

número primo p. Sendo $n = p^\alpha$ tem-se

$$\begin{aligned}\sum_{d|n}\mu(d)\, a^{n/d} &= a^{p^\alpha} - a^{p^{\alpha-1}} \\ &= a^{p^{\alpha-1}}\left(a^{p^\alpha - p^{\alpha-1}} - 1\right).\end{aligned}$$

Por (2.10), o número de inteiros em $[1, p^\alpha]$ primos com p^α é $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Pode então escrever-se

$$a^{p^\alpha} - a^{p^{\alpha-1}} = a^{p^{\alpha-1}}\left(a^{\phi(p^\alpha)} - 1\right). \tag{2.20}$$

Se $p \nmid a$, pelo teorema de Euler, tem-se $a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$. Na hipótese de p ser divisor de a também $p^{p^{\alpha-1}} | a^{p^{\alpha-1}}$ e como $p^{\alpha-1} \geq 2^{\alpha-1} \geq \alpha$ segue-se que $p^\alpha | a^{p^{\alpha-1}}$. Assim em ambos os casos se conclui que $p^\alpha | a^{p^{\alpha-1}}\left(a^{\phi(p^\alpha)} - 1\right)$ e portanto

$$a^{p^\alpha} - a^{p^{\alpha-1}} \equiv 0 \pmod{p^\alpha}. \tag{2.21}$$

Passa-se agora ao caso geral em que n se decompõe num produto de factores primos da forma $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Fixado $k \in \{1, \ldots, m\}$, seja $n_k = n/p_k^{\alpha_k}$. Para cada d divisor de n_k, designe-se $b_d = a^{\frac{n_k}{d}}$. Tem-se então

$$\begin{aligned}\sum_{d|n}\mu(d)\, a^{n/d} &= \sum_{d|n_k}\mu(d)\, a^{n/d} + \sum_{d|n_k}\mu(dp_k)\, a^{n/dp_k} \\ &= \sum_{d|n_k}\mu(d)\left(b_d^{p_k^{\alpha_k}} - b_d^{p_k^{\alpha_k - 1}}\right)\end{aligned}$$

e da parte do enunciado já estabelecida resulta

$$b_d^{p_k^{\alpha_k}} - b_d^{p_k^{\alpha_k - 1}} \equiv 0 \pmod{p_k^{\alpha_k}} \tag{2.22}$$

se $d | n_k$.

É pois

$$\sum_{d|n}\mu(d)\, a^{n/d} \equiv 0 \pmod{p_k^{\alpha_k}} \tag{2.23}$$

e portanto também

$$\sum_{d|n} \mu(d)\, a^{n/d} \equiv 0 \pmod{n}, \tag{2.24}$$

pois os $p_k^{\alpha_k}$ são primos entre si. □

Em seguida fornece-se uma notação alternativa deste teorema, com base em conceitos de combinatória. Esta versão foi desenvolvida no decurso do trabalho de tese e partilhada com o Prof. Nuno da Costa Pereira o qual nos sugeriu a demonstração acima descrita para o teorema 2.15 e ainda uma forma simples (abaixo apresentada) de provar que ambas as notações são equivalentes, isto é, são equivalentes as congruências (2.19) e (2.27) (essencialmente é a prova do teorema 2.21). Introduz-se primeiro a notação prévia necessária.

O significado combinatório básico do coeficiente binomial $\binom{n}{k}$ é o número de todos os subconjuntos de k elementos de um conjunto de n elementos.

Conforme a notação de J. Matoušek e J. Nešetřil [16] tem-se o que se segue.

Definição 2.16. Sejam X um conjunto e k um inteiro não negativo. Pelo símbolo $\binom{X}{k}$ denota-se o conjunto de todos os subconjuntos de k elementos do conjunto X.

Exemplo 2.17. Seja $\{a, b, c\}$ um conjunto. Então

$$\binom{\{a,b,c\}}{2} = \{\{a,b\}, \{a,c\}, \{b,c\}\}. \tag{2.25}$$

Observação 2.18. O símbolo $\binom{x}{k}$ tem agora dois significados dependendo se x é um número ou um conjunto.

A proposição seguinte estabelece uma ligação entre estes dois significados.

Proposição 2.19. Para cada conjunto finito X, o número de todos os seus subconjuntos de k elementos é igual a $\binom{|X|}{k}$.

Simbolicamente, esta proposição pode ser reescrita da seguinte forma

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}. \tag{2.26}$$

Demonstração. Considere-se $n = |X|$. Contem-se todas as possibilidades de k componentes ordenadas do conjunto X (sem repetições de elementos) de duas maneiras.

Por um lado, sabe-se que o número de possibilidades de k componentes é $n\,(n-1)\cdots(n-k+1)$. Por outro lado, para um subconjunto $M \in \binom{X}{k}$ de k elementos, podem criar-se $k!$ diferentes possibilidades de k elementos ordenados, e cada possibilidade de k elementos ordenados é obtido de exactamente um subconjunto M de k elementos desta maneira.

Assim, $n\,(n-1)\cdots(n-k+1) = k!\left|\binom{X}{k}\right|$. □

Em combinatória, as notações $\binom{x}{k}$ e C_k^x têm exactamente o mesmo significado. Neste sentido, a notação que vai ser utilizada foi assim adaptada, substituindo o que está na primeira forma para a segunda, agora em termos de conjuntos.

Partindo desta notação define-se

Definição 2.20. Denota-se por $C_j^{\{1,2,\ldots,k\}}$ o conjunto de todos os subconjuntos de $\{1,2,\ldots,k\}$ com j elementos.

Assim, $\delta \in C_j^{\{1,2,\ldots,k\}}$ é um conjunto formado por j elementos distintos de $\{1,2,\ldots,k\}$. Sem perda de generalidade, escrevemos $\delta \in C_j^{\{1,2,\ldots,k\}}$ da forma $\delta = \{\delta_1, \delta_2, \ldots, \delta_j\}$, onde os δ_i, com $i = 1,\ldots,j$, são os elementos de δ.

Teorema 2.21. *Sejam a e n inteiros positivos cuja factorização em números primos de n é $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ e seja $P = p_1 p_2 \cdots p_k$. Então*

$$\sum_{j=0}^{k} (-1)^{k+j} \sum_{\delta \in C_j^{\{p_1,p_2,\ldots,p_k\}}} a^{\frac{n}{P}\delta_1\delta_2\cdots\delta_j} \equiv 0 \ (mod\ n). \tag{2.27}$$

Demonstração. O duplo somatório é simplesmente uma soma sobre todos os divisores de P. Notando ainda que $(-1)^k = \mu(P)$ e que $(-1)^j = \mu(\delta_1\delta_2\cdots\delta_j)$, este toma a forma de

$$\sum_{d|P} \mu(dP)\, a^{\frac{n}{P}d}. \tag{2.28}$$

Substituindo d por P/d obtém-se o seguinte

$$\sum_{d|P} \mu(d)\, a^{\frac{n}{d}}. \tag{2.29}$$

No entanto, como $\mu(d) = 0$ se $d|n$ e $d \nmid P$ este somatório é igual a

$$\sum_{d|n} \mu(d)\, a^{\frac{n}{d}}, \tag{2.30}$$

e pelo teorema 2.15 obtém-se o resultado pretendido. □

Exemplo 2.22. Para $n = 14$ o teorema 2.21 conduz à seguinte congruência

$$a^{14} - a^7 - a^2 + a \equiv 0 \pmod{14}, \tag{2.31}$$

válida para todo o $a \geq 1$.

Exemplo 2.23. Para $n = 360$ o teorema 2.21 conduz à seguinte congruência

$$a^{360} - a^{180} - a^{120} - a^{72} + a^{60} + a^{36} + a^{24} - a^{12} \equiv 0 \pmod{360}, \tag{2.32}$$

válida para todo o $a \geq 1$.

Note-se que, apesar da expressão da congruência (2.27) não ser tão compacta como a apresentada por Gegenbauer (2.19), a primeira tem uma vantagem relativamente à segunda. Assim, para a fórmula (2.27), basta identificar os divisores de P, ao passo que na fórmula (2.19) é necessário identificar todos os divisores de n. Assim, de acordo com (2.27), para exprimir uma congruência (mod n) basta, relativamente ao primeiro membro, seguir os passos:

1. Todas as parcelas têm o factor $a^{\frac{n}{P}}$. Isto corresponde a diminuir em uma unidade o expoente de cada factor primo;

2. o expoente de cada parcela multiplica-se por um divisor de P. Existem tantas parcelas quantos os divisores de P;

3. o sinal da parcela depende do número de factores primos que foram multiplicados no passo 2. Para a parcela cujo divisor de P é o próprio

P fica com sinal positivo. Com menos um factor primo troca-se o sinal. Por cada factor primo a menos faz-se uma troca de sinal.

Exemplo 2.24. Para a construção da congruência do exemplo anterior, isto é, para $n = 360 = 2^3 \cdot 3^2 \cdot 5$ e $a \geq 1$, tem-se

$$a^{2^2\cdot 3(2\cdot 3\cdot 5)} - a^{2^2\cdot 3(3\cdot 5)} - a^{2^2\cdot 3(2\cdot 5)} - a^{2^2\cdot 3(2\cdot 3)} + a^{2^2\cdot 3(5)} + a^{2^2\cdot 3(3)} + a^{2^2\cdot 3(2)} - a^{2^2\cdot 3} \equiv 0 \pmod{2^3 \cdot 3^2 \cdot 5}. \tag{2.33}$$

As generalizações apresentadas do pequeno teorema de Fermat não se esgotam por aqui. De facto, como Dickson referiu no seu livro da história da teoria dos números (veja-se [8]), existem inúmeras generalizações do mesmo. No entanto, a última generalização apresentada é a que interessa para este trabalho.

3

Linguagens formais - colares e palavras

3.1 Conceitos e exemplos

Neste capítulo introduzem-se alguns conceitos de linguagens formais e combinatória de palavras tal como definidos em [3] e [21]. Os exemplos são, fundamentalmente, os apresentados no *Recreational Mathematics Colloquium II* e no respectivo artigo para *Proceedings* (ver [22]).

Definição 3.1. Um *alfabeto* é um conjunto finito não vazio de símbolos.

Vejam-se alguns exemplos.

Exemplo 3.2. O alfabeto binário $\{0, 1\}$.

Exemplo 3.3. O alfabeto de 10 dígitos $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Exemplo 3.4. O alfabeto da língua inglesa $\{a, b, c, \ldots, x, y, z\}$, bem como os de outras línguas.

Exemplo 3.5. O alfabeto alfa-numérico $\{0, 1, \ldots, 8, 9, a, b, c, \ldots, x, y, z\}$.

Exemplo 3.6. O alfabeto hexadecimal $\{0, 1, \ldots, 8, 9, a, b, c, d, e, f\}$.

Exemplificam-se outros possíveis alfabetos, numa perspectiva mais lúdica.

Exemplo 3.7. O alfabeto dos naipes de cartas $\{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$.

Exemplo 3.8. Um alfabeto de 3 formas geométricas $\{\square, \triangle, \bigcirc\}$.

Exemplo 3.9. O alfabeto de 7 cores {■, ■, ■, ■, ■, ■, ■}.

Exemplo 3.10. O alfabeto do Zodíaco que inclui os símbolos de Carneiro, Touro, Gémeos, Caranguejo, Leão, Virgem, Balança, Escorpião, Sagitário, Capricórnio, Aquário e Peixes.

Definição 3.11. Uma *palavra* de um alfabeto A é uma sequência finita de símbolos de A. A *concatenação* de palavras é a nova palavra formada justapondo as palavras originais, isto é, escrevendo a primeira palavra imediatamente seguida da segunda, etc., sem espaço de separação. Uma *factorização* de uma palavra u é qualquer sequência $u_1, \ldots, u_t$ tal que $u = u_1 \ldots u_t$. Diz-se que uma palavra u é uma *potência* n de v se $u = \underbrace{vv \cdots v}_{n \text{ vezes}}$, isto é, é a concatenação de n palavras iguais a v e denota-se por $u = v^n$.

Para um par de palavras (u, v) define-se:

(i) u é um *prefixo* de v se existir uma palavra z tal que $v = uz$ e $\text{pref}_k(v)$ é o prefixo de v de comprimento k;

(ii) v é um *sufixo* de v se existir uma palavra z tal que $v = zu$ e $\text{suf}_k(v)$ é o sufixo de v de comprimento k;

(iii) u é um factor de v se existirem palavras z e z' tais que $v = zuz'$;

(iv) Se $v = uz$ escreve-se $u = vz^{-1}$ ou $z = u^{-1}v$ e diz-se que u é o quociente direito de v por z e que z é o quociente esquerdo de v por u.

Observação 3.12. Se for considerada como palavra a sequência vazia, então dadas duas palavras u e v existe sempre e é único o *prefixo maximal comum* de u e v que se denota por $u \wedge v$.

Introduzindo uma relação de ordem total (designada por $\prec$) num alfabeto A fica definida uma ordenação dos seus símbolos: dados $x, y \in A$, $x \prec y$ significa que x é menor do que y em relação a $(A, \prec)$.

A partir de agora, supõe-se introduzida em A esta relação de ordem, utilizando-a quando for relevante.

Definição 3.13. Diz-se que u é *lexicograficamente menor* que v, e denota-se por $u \prec_l v$, se, ou u é um prefixo próprio de v, ou o primeiro símbolo após $u \wedge v$ de u é menor $(\prec)$ do que o de v.

Considerando que os alfabetos são conjuntos finitos, é natural identificar cada alfabeto de cardinalidade n por um conjunto finito de números naturais.

Definição 3.14. Designa-se o conjunto $\{0, 1, 2, \ldots, n-1\}$ por *alfabeto base*.

Assim, para um determinado alfabeto pode fazer-se uma correspondência biunívoca com o alfabeto base de modo a que a ordem obtida (nos números naturais) respeite a ordem lexicográfica dos símbolos originais.

Definição 3.15. Considere-se a permutação cíclica $c : A \to A$ definida por

$$c(u) = \mathrm{pref}_1(u)^{-1} \, u \, \mathrm{pref}_1(u) \tag{3.1}$$

para $u \in A$. Diz-se que duas palavras u e v são *conjugadas* se e só se existir um $k \in \mathbb{N}$ tal que $v = c^k(u)$.

Observação 3.16. Facilmente se prova que a relação de conjugação é uma relação de equivalência.

Definição 3.17. A uma classe de equivalência da relação de conjugação chama-se *colar*.

Seja $u = a_1 \ldots a_n$, com $a_i \in A$. Um *período* de u é um inteiro p tal que

$$a_{p+i} = a_i \text{ para } i = 1, \ldots, n-p. \tag{3.2}$$

O menor p que verifica (3.2) chama-se *o período* de u e é designado por $p(u)$. As palavras do colar $\left[\mathrm{pref}_{p(u)}(u)\right]$ são chamadas *raízes cíclicas* de u. Diz-se que uma palavra é *primitiva* se não é uma potência própria de nenhuma das suas raízes cíclicas. Uma *palavra de Lyndon* é uma palavra primitiva que, de entre as palavras do mesmo colar, é a menor no que se refere à ordem lexicográfica.

Existe uma página na internet[1] que perante a especificação da cardinalidade do alfabeto A e do comprimento k da palavra fornece a listagem de todas as palavras de Lyndon de comprimento k em A. O resultado é apresentado considerando o alfabeto base e, se o utilizador o pretender, também em cores.

Exemplo 3.18. Considere-se o alfabeto dos naipes de cartas, com a ordenação ♠ ≺ ♣ ≺ ♡ ≺ ♢. A figura 3.1 representa 4 possíveis colares.

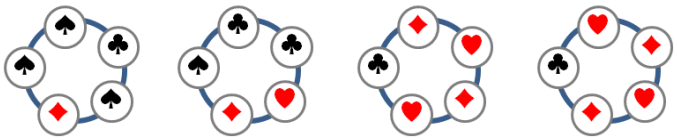

Figura 3.1: Colares cujas palavras de Lyndon são ♠♠♣♠♢, ♠♣♣♡♢, ♣♢♡♢♡ e ♣♡♢♡♢.

Note-se que uma condição equivalente de primitividade é

$$\forall z \in A : u = z^n \Rightarrow n = 1 \text{ (i.e., } u = z). \tag{3.3}$$

Neste sentido, pode dizer-se que uma palavra é primitiva se e só se for aperiódica, pois as palavras periódicas u caracterizam-se por

$$u = z^n, \text{ com } n > 1. \tag{3.4}$$

Observação 3.19. As raízes cíclicas são, necessariamente, palavras primitivas.

[1] http://theory.cs.uvic.ca/gen/neck.html, acedido em 23/09/2011.

3.2 Teoremas de contagem

Tal como em [18] designa-se por $S(a,n)$ o número de palavras aperiódicas de comprimento n de um alfabeto A contendo a letras e por $M(a,n)$ o correspondente número de colares. Analogamente, designa-se por $L(a,n)$ o correspondente número de palavras de Lyndon. Denotam-se os conjuntos correspondentes pelas respectivas letras caligráficas, isto é, respectivamente, por $\mathcal{S}(a,n)$, $\mathcal{M}(a,n)$ e $\mathcal{L}(a,n)$.

Através da cardinalidade destes conjuntos é possível demonstrar o pequeno teorema de Fermat e algumas das suas generalizações. Uma primeira ilustração deste facto é a demonstração feita por Petersen, em 1872, conforme referido por Smyth (veja-se [24]) e que, no fundo, espelha a ideia colar, apesar de não lhe ter sido atribuída essa designação.

> Suponham-se p caixas, dispostas em círculo, para serem coloridas com a cores. Existem, ao todo, a^p formas de coloração possíveis, e a formas de coloração se todas as caixas ficarem da mesma cor. As restantes possibilidades de coloração $a^p - a$ podem ser agrupadas em conjuntos de p elementos, uma vez que as p rotações possíveis destas colorações são todas distintas. Consequentemente, $p|a^p - a$.

Em termos da notação introduzida, um círculo de p caixas é um colar de comprimento p sobre um alfabeto A composto por a letras (i.e., a cores).

Com o mesmo raciocínio Thue, em 1910 (veja-se [8]), apresentou uma generalização do pequeno teorema de Fermat, onde desta vez são n lugares e a diferentes tipos de objectos a representar - na notação aqui utilizada, respectivamente, o comprimento dos colares e a cardinalidade do alfabeto. Veja-se como Dickson o descreveu ([8]).

> Observe-se que a diferentes tipos de objectos podem ser colocados em n lugares distintos de a^n diferentes maneiras. Destes, seja U_a^n o número de colocações tais que cada uma é convertida em si própria por não menos do que n aplicações da operação que substitui cada um pelo próximo e o último pelo primeiro. Então, U_a^n é divisível

por n. Se n é primo $U_a^n = a^n - a$, o que conduz ao teorema de Fermat. De seguida, $a^n = \sum U_a^d$, onde d varia entre os divisores de n. Finalmente, se p, q, ..., r são os diferentes factores primos de n,

$$U_a^n = \sum (-1)^\theta \, a^{n/D} \equiv 0 \pmod{n},$$

onde D varia entre todos os divisores de $pq \ldots r$, ao passo que θ é o número de factores primos de D.

Esta congruência não é mais do que uma outra forma de apresentar a generalização do pequeno teorema de Fermat do capítulo precedente, conforme descrita por (2.19) e (2.27).

A ideia fundamental aqui presente é a contagem de colares aperiódicos.

Teorema 3.20. *Sejam a, n inteiros positivos. Então*

$$S(a,n) = \sum_{d|n} \mu(d) \, a^{\frac{n}{d}}. \tag{3.5}$$

Demonstração. Considere-se um alfabeto A com a letras. Existem a^n palavras diferentes de comprimento n que se podem escrever com este alfabeto. Por outro lado, considerando que qualquer palavra de comprimento n é uma potência d de uma sua raiz cíclica, com $d|n$, então

$$a^n = \sum_{d|n} S(a,d). \tag{3.6}$$

Aplicando a fórmula de inversão de Möbius (2.9) obtém-se o resultado enunciado. □

Teorema 3.21. *Sejam a, n inteiros positivos. Então tem-se*

$$M(a,n) = \frac{1}{n} \sum_{d|n} \mu(d) \, a^{\frac{n}{d}}. \tag{3.7}$$

Demonstração. Considere-se um colar aperiódico de comprimento n. Este é uma classe de equivalência com n palavras, correspondendo a n permuta-

ções cíclicas. Existem, por isso, exactamente n palavras por cada colar, logo $S(a,n) = nM(a,n)$. □

Teorema 3.22. *Sejam a, n inteiros positivos. Então*

$$L(a,n) = \frac{1}{n}\sum_{d|n}\mu(d)\, a^{\frac{n}{d}}. \tag{3.8}$$

Demonstração. Por definição, a cada colar corresponde uma e uma só palavra de Lyndon, logo $L(a,n) = M(a,n)$. □

Exemplo 3.23. Para $n = 4$ e $a = 2$, a figura 3.2 ilustra todas os possíveis colares e palavras.

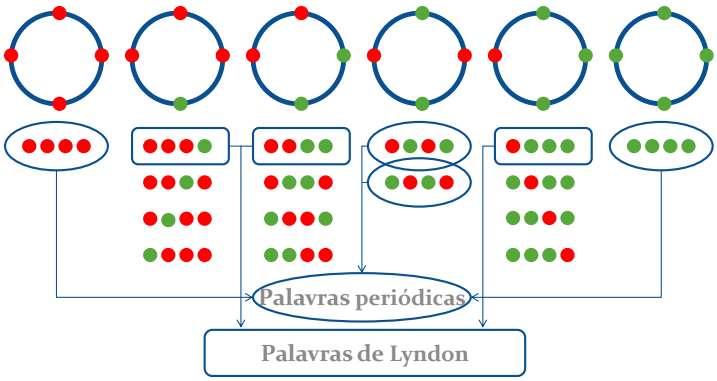

Figura 3.2: Todas as possibilidades de colares e palavras de comprimento 4 de um alfabeto com 2 letras.

Observação 3.24. Da fórmula (3.7) obtêm-se directamente as congruências que generalizam o pequeno teorema de Fermat (2.19). Como se pode constatar, o recurso a colares é uma forma alternativa de provar este resultado de teoria de números de forma relativamente simples. Mais adiante será possível verificar que existem outros métodos para o demonstrar.

4

Perspectiva dinâmica

4.1 Conceitos e resultados de sistemas dinâmicos

Neste capítulo, em primeiro lugar, apresentam-se definições gerais de sistemas dinâmicos, que podem ser encontradas em qualquer livro sobre este tema e que, em geral, são plenamente conhecidas e uniformizadas, à parte de pequenas diferenças de notação entre autores. Definem-se os conceitos que se seguem com base em Hasselblatt e Katok [11].

Definição 4.1. Sejam X um espaço topológico e $f : X \to X$ uma aplicação. Dado um ponto $x \in X$, a sucessão $(x, f(x), f(f(x)), \ldots, f^n(x), \ldots)$ é chamada de *órbita* de x por f. Um *ponto fixo* de f é um ponto tal que $f(x) = x$. O *conjunto dos pontos fixos* de f é denotado por $\mathrm{Fix}(f)$. Um *ponto periódico* é um ponto x tal que $f^n(x) = x$ para algum $n \in \mathbb{N}$, isto é, um ponto de $\mathrm{Fix}(f^n)$. Um tal n diz-se ser um *período* de x e a sua órbita é uma órbita *n-periódica*. Ao menor destes n chama-se *período mínimo* de x. O número de

pontos periódicos de f de período n é denotado por $\mathrm{Per}_n(f)$, isto é, o número de pontos fixos de f^n.

Milnor e Thurston (veja-se [19]) fizeram um estudo sobre aplicações do intervalo, isto é, sobre aplicações que aplicam um intervalo real nele mesmo, desenvolvendo uma abordagem baseada na dinâmica simbólica. Vão ser usadas e adaptadas algumas das notações aí utilizadas.

Definição 4.2. Seja $J \subset \mathbb{R}$ um intervalo compacto. Uma aplicação $f : J \to J$ diz-se *monótona por troços* se J pode ser subdividido num número finito de intervalos $J_1, J_2, \ldots, J_a$, nos quais f é estritamente crescente ou estritamente decrescente. A cada intervalo maximal no qual f é monótona dá-se o nome de *ramo* de f. Aqui $J = [c_0, c_a]$, $J_j = [c_j, c_{j+1}]$ $\forall j \in \{0, 1, \cdots, a-1\}$ e $c_0 < c_1 < \cdots < c_a$. Os pontos interiores de separação $c_1, \cdots, c_{a-1}$ nos quais f é um mínimo ou máximo local são chamados de *pontos de viragem* de f.

Observação 4.3. A definição original exige continuidade, que neste caso não será imposta.

Definição 4.4. Define-se *endereço* $A(x)$ de um ponto $x \in J$ ao símbolo formal J_j se x pertencer ao ramo J_j e não é um ponto de viragem, ou o símbolo formal c_j se x é precisamente igual ao ponto de viragem c_j. Chama-se *itinerário* $I(x)$ à sucessão de endereços $\left(A(x), A(f(x)), A\left(f^2(x)\right), \cdots\right)$ das imagens sucessivas de x. Denota-se por $I_m(x)$ a sequência de comprimento m que corresponde à truncatura de $I(x)$ no símbolo m, e designa-se de *itinerário truncado de ordem* m.

Observação 4.5. Uma órbita periódica de período n pode ser representada de n formas diferentes, dependendo do ponto a partir do qual é identificada. Uma representação difere de outra através de uma permutação cíclica. Assim, por este motivo, uma órbita periódica de período n denota-se por $[(x, f(x), f(f(x)), \ldots, f^n(x))]$.

Para a contagem de pontos periódicos de sistemas dinâmicos utiliza-se a definição dada por Frame [9].

Definição 4.6. Dada uma aplicação f, designa-se por $N_n(f)$ o número de pontos periódicos de período mínimo n.

Observação 4.7. Para $n = 1$,

$$N_1(f) = \mathrm{Per}_1(f). \tag{4.1}$$

Na definição anterior pode apenas indicar-se N_n se não houver possibilidade de confusão.

Realiza-se uma definição análoga para órbitas periódicas.

Definição 4.8. Dada uma aplicação f, designa-se por $O_n(f)$ o número de órbitas periódicas de período mínimo n.

Tal como no capítulo anterior, os conjuntos correspondentes serão designados pela letra caligráfica correspondente.

Definição 4.9. Diz-se que $\mathcal{N}_n(f)$ e $\mathcal{O}_n(f)$ são, respectivamente, os conjuntos dos pontos e órbitas de período mínimo n.

A questão da divisibilidade é um elemento central para muitos resultados da teoria dos números, de que são exemplo os resultados apresentados no primeiro capítulo deste trabalho. A presença de padrões de divisibilidade em órbitas periódicas e pontos periódicos de sistemas dinâmicos é a chave para poderem ser demonstrados teoremas de teoria de números por via dinâmica. Veja-se o seguinte resultado (apresentado em [9]).

Teorema 4.10. *Dado um sistema dinâmico que tenha órbitas periódicas,*

(i) Se x é um ponto de período n cujo período mínimo é m, então $m|n$.

(ii) Duas órbitas de período m ou são disjuntas ou coincidem.

(iii) Para todo o $m \geq 1$, $m|N_m$ sempre que N_m é finito.

Demonstração. Seja x_0 um ponto de período mínimo m e considere-se a sua órbita que inclui os seguintes pontos periódicos: $x_0, x_1, \ldots, x_{m-1}$. Sabe-se que todos os pontos $x_i, f(x_i), f^2(x_i), \ldots, f^{m-1}(x_i)$ são completamente determinados por qualquer dos x_i da órbita, pois $f^m(x_i) = x_i$. Por este facto, tem-se necessariamente (ii).

Para provar (i), supõe-se que x é um ponto de período n cujo período mínimo é m. Considerem-se os pontos $x, f(x), \ldots, f^{m-1}(x), \ldots, f^n(x)$. Por hipótese os primeiros m pontos são pontos da órbita periódica de período mínimo m. Como $f^m(x) = x$, os pontos repetem-se em cada m iterações. Como se tem $f^n(x) = x$, então necessariamente $m|n$.

A prova de (iii) advém do facto que os pontos de período mínimo m estarem particionados em órbitas de período m, que por (ii) são disjuntos. Como cada órbita de período mínimo m contém exactamente m pontos e o número de órbitas é um inteiro, tem-se $m|N_m$. □

Este resultado tem como consequência a seguinte relação entre contagens de pontos periódicos.

Teorema 4.11. *Dado um sistema dinâmico definido por uma aplicação f que tenha órbitas periódicas, então*

$$Per_n(f) = \sum_{m|n} N_m(f). \tag{4.2}$$

Demonstração. Pela alínea (i) do teorema 4.10, os pontos de período n são os que têm período mínimo m igual a n ou inferior desde que $m|n$. □

4.2 Aplicações do círculo e generalização do pequeno teorema de Fermat

Para estabelecer os resultados principais desta tese serão estudadas especificamente as aplicações do círculo e, em particular, as aplicações do tipo linear. W. E. Briggs e William L. Briggs fizeram uma caracterização deste tipo de

aplicações. A definição 4.14 é adaptada do artigo por eles publicado (veja-se [4]).

Definição 4.12. Uma *aplicação do círculo* f é definida por

$$f : S^1 \to S^1. \tag{4.3}$$

Estas aplicações podem, desta forma, ser representadas como aplicações do intervalo

$$\widetilde{f} : [0,1] \to [0,1] \tag{4.4}$$

com a identificação dos pontos $x = 0$ e $x = 1$.

Para estudar a dinâmica de uma aplicação deste tipo é usual fazer um levantamento da aplicação para $\mathbb{R}$ (veja-se [7]). Para isso, é definida a aplicação $\pi : \mathbb{R} \to S^1$ tal que

$$\pi(x) = e^{2\pi i x}. \tag{4.5}$$

Definição 4.13. Uma aplicação $F : \mathbb{R} \to \mathbb{R}$ é um *levantamento* de $f : S^1 \to S^1$ se

$$\pi \circ F = f \circ \pi. \tag{4.6}$$

Neste trabalho as aplicações do círculo serão estudadas na formulação (4.4), sem recorrer a levantamentos.

Definição 4.14. Para $a \in \mathbb{N}$, $b \in [0,1[$, define-se a seguinte família de aplicações lineares do círculo, $\widetilde{g}_{a,b} : [0,1[\to [0,1[$:

$$\widetilde{g}_{a,b}(x) = ax + b \pmod 1. \tag{4.7}$$

Exemplo 4.15. A figura 4.1 ilustra exemplos destas aplicações do círculo com $a = 3$ e, respectivamente, $b = 0,25$ e $b = 0$.

O facto de o parâmetro a ser inteiro permite simplificar alguns cálculos, nomeadamente, permitindo que a operação (mod 1) possa ser realizada em último lugar na obtenção de várias iterações.

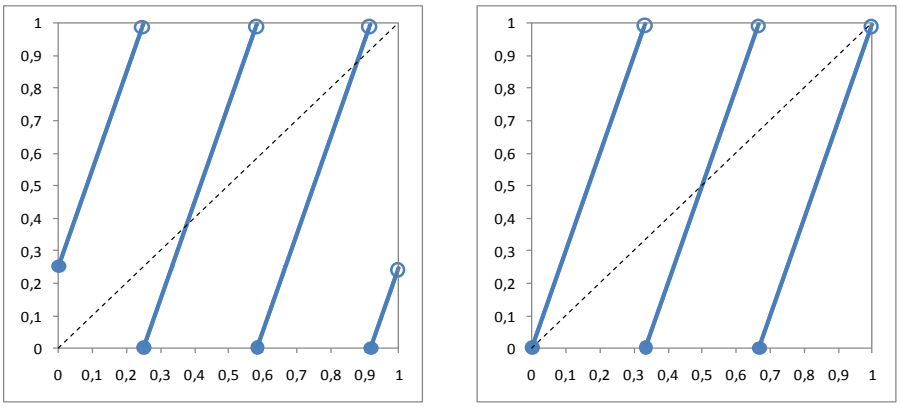

Figura 4.1: Aplicações lineares do círculo $g_{3;0,25}$ e $g_{3,0}$.

Lema 4.16. Para $a, n \in \mathbb{N}$, $b \in [0, 1[$, tem-se

$$\widetilde{g}_{a,b}^{n}(x) = a^n x + a^{n-1}b + \cdots + ab + b \pmod 1. \tag{4.8}$$

Demonstração. A prova faz-se por indução em n.

Para $n = 1$ não há nada a provar.

Suponha-se que $\widetilde{g}_{a,b}^{n}(x) = a^n x + a^{n-1}b + \cdots + ab + b \pmod 1$. Então

$$\begin{aligned}
\widetilde{g}_{a,b}^{n+1}(x) &= \widetilde{g}\left(\widetilde{g}_{a,b}^{n}(x)\right) \\
&= \widetilde{g}\left(a^n x + a^{n-1}b + \cdots + ab + b \pmod 1\right) \\
&= \left(a^{n+1}x + a^n b + \cdots + a^2 b + ab \pmod 1 + b\right) \pmod 1 \\
&= a^{n+1}x + a^n b + \cdots + a^2 b + ab + b \pmod 1.
\end{aligned}$$

Logo, a expressão é válida para todo o $n \in \mathbb{N}$. □

Este resultado pode ser apresentado de forma mais compacta (conforme [4]).

Lema 4.17. Para $a, n \in \mathbb{N}$, $b \in [0, 1[$, tem-se

$$\widetilde{g}_{a,b}^{n}(x) = a^n x + b\frac{a^n - 1}{a - 1} \pmod 1. \tag{4.9}$$

Demonstração. Basta notar que, em (4.8), os termos independentes de x representam os n primeiros termos de uma progressão geométrica de razão a. □

Assim, pode calcular-se exactamente a localização dos pontos periódicos.

Teorema 4.18. *Sejam $a, n \in \mathbb{N}$, $b \in [0,1[$. Se $x \in [0,1[$ é um ponto periódico de período p de $\widetilde{g}_{a,b}$, então x é da forma*

$$x = \frac{q}{a^p - 1} - \frac{b}{a-1} \ (mod\, 1) \tag{4.10}$$

onde $q \in \{0, 1, 2, \ldots, a^p - 2\}$.

Demonstração. Por hipótese,

$$\begin{aligned} x &= \widetilde{g}^p(x) \\ &= a^p x + b\frac{a^p - 1}{a-1} \pmod 1. \end{aligned}$$

Então, existe $q \in \mathbb{Z}$ tal que

$$\begin{aligned} x + q &= a^p x + b\frac{a^p - 1}{a-1} \\ a^p x - x &= q - b\frac{a^p - 1}{a-1} \\ x &= \frac{q}{a^p - 1} - \frac{b}{a-1}. \end{aligned}$$

Verifique-se que $q \in \{0, 1, 2, \ldots, a^p - 2\}$.

$$\begin{aligned} \frac{a^p - 1}{a^p - 1} - \frac{b}{a-1} \pmod 1 &= 1 - \frac{b}{a-1} \pmod 1 \\ &= -\frac{b}{a-1} \pmod 1 \\ &= \frac{0}{a^p - 1} - \frac{b}{a-1} \pmod 1, \end{aligned}$$

concluindo a demonstração. □

Corolário 4.19. Sejam $a, n \in \mathbb{N}$. Se $x \in [0,1[$ é um ponto periódico de período

p de $\widetilde{g}_{a,0}$, então x é da forma

$$x = \frac{q}{a^p - 1}, \tag{4.11}$$

onde $q \in \{0, 1, 2, \ldots, a^p - 2\}$.

Demonstração. Basta aplicar o teorema anterior tendo em conta que $x \in [0, 1[$. □

Relativamente ao número de pontos fixos deste tipo de aplicações, em primeiro lugar, note-se que para $a = 1$ os casos são extremos. No caso de $b = 0$, $\widetilde{g}_{a,b}$ resume-se à aplicação identidade, pelo que todos os pontos do seu domínio são pontos fixos. No caso de $b \neq 0$ tem-se uma aplicação sem pontos fixos. O caso $a = 1$ será, contudo, trivial, para o que se segue. No caso geral ($a > 1$), pela observação do gráfico das aplicações (veja-se figura 4.1) pode identificar-se directamente o seguinte resultado.

Lema 4.20. Sejam $a \geq 2$ um inteiro positivo e $b \in [0, 1[$. Então $\widetilde{g}_{a,b}$ tem $a - 1$ pontos fixos, isto é,

$$\mathrm{Per}_1\left(\widetilde{g}_{a,b}\right) = N_1\left(\widetilde{g}_{a,b}\right) = a - 1. \tag{4.12}$$

Analogamente,

Teorema 4.21. *Sejam $a \geq 2$ um inteiro positivo, $n \in \mathbb{N}$ e $b \in [0, 1[$. Então $\widetilde{g}^n_{a,b}$ tem $a^n - 1$ pontos fixos, isto é,*

$$Per_n\left(\widetilde{g}_{a,b}\right) = a^n - 1. \tag{4.13}$$

Demonstração. Pelo lema 4.17 pode dizer-se que

$$\widetilde{g}^n_{a,b}(x) = a^n x + c \pmod 1, \tag{4.14}$$

onde $c = b\frac{a^n - 1}{a - 1}$ é uma constante. Logo,

$$\widetilde{g}^n_{a,b}(x) = \widetilde{g}_{a^n,c}. \tag{4.15}$$

Pelo resultado anterior obtém-se

$$\begin{aligned}\mathrm{Per}_1\left(\widetilde{g}_{a,b}^n\right) &= N_1\left(\widetilde{g}_{a,b}^n\right)\\ &= a^n - 1.\end{aligned}$$

E, por definição, $\mathrm{Per}_n\left(\widetilde{g}_{a,b}\right) = \mathrm{Per}_1\left(\widetilde{g}_{a,b}^n\right)$. □

Teorema 4.22. *Sejam $a \geq 2$ um inteiro positivo, $n \in \mathbb{N}$ e $b \in [0,1[$. Então*

$$a^n - 1 = \sum_{m|n} N_m\left(\widetilde{g}_{a,b}\right). \tag{4.16}$$

Demonstração. Imediato a partir dos teoremas 4.11 e 4.21. □

Teorema 4.23. *Sejam $a \geq 2$ um inteiro positivo, $n \in \mathbb{N}$ e $b \in [0,1[$. Então*

$$N_n\left(\widetilde{g}_{a,b}\right) = \begin{cases} a-1 & \text{se } n = 1 \\ \sum\limits_{d|n} \mu(d)\, a^{n/d} & \text{se } n > 1 \end{cases} \tag{4.17}$$

Demonstração. Pelo teorema anterior, pela fórmula de inversão de Möbius (2.9) e pelo teorema 2.6, tem-se

$$\begin{aligned} N_n\left(\widetilde{g}_{a,b}\right) &= \sum_{d|n} \mu(d)\left(a^{n/d} - 1\right)\\ &= \sum_{d|n} \mu(d)\, a^{n/d} - \sum_{d|n} \mu(d)\\ &= \begin{cases} \sum\limits_{d|n} \mu(d)\, a^{n/d} - 1 & \text{se } n = 1 \\ \sum\limits_{d|n} \mu(d)\, a^{n/d} & \text{se } n > 1 \end{cases}\\ &= \begin{cases} a-1 & \text{se } n = 1 \\ \sum\limits_{d|n} \mu(d)\, a^{n/d} & \text{se } n > 1, \end{cases} \end{aligned}$$

concluindo a demonstração. □

A partir deste teorema obtém-se directamente a generalização do pequeno teorema de Fermat (2.19), com a condição de que $a, n \geq 2$. No entanto, esta restrição é desnecessária, pois os casos em que $a = 1$ ou $n = 1$ são absolutamente triviais, como acima afirmado.

A demonstração deste resultado que se realizou através de sistemas dinâmicos pode ser feita de forma mais simples e elegante, particularizando a aplicação e fazendo uma pequena alteração, tomando $b = 0$ e realizando o prolongamento por continuidade ao intervalo fechado $[0, 1]$, tal como Iga fez na sua demonstração (veja-se [12]). Note-se que Frame em [9] realizou uma demonstração análoga, com recurso a uma aplicação similar, apenas diferente na definição da aplicação nos seus pontos de viragem.

Definição 4.24. Para cada inteiro $a \geq 2$ define-se a aplicação do círculo $g_a : [0, 1] \to [0, 1]$ por

$$g_a(x) = \begin{cases} a \cdot x \pmod 1 & \text{se } x \neq 1 \\ 1 & \text{se } x = 1 \end{cases}. \tag{4.18}$$

Alternativamente, pode definir-se g_a como uma aplicação monótona por troços. Aplicam-se as definições 4.2 e 4.4 de forma óbvia.

Definição 4.25. Para cada inteiro $a \geq 2$ define-se $g_a : [0, 1] \to [0, 1]$ por

$$g_a(x) = \begin{cases} a \cdot x & \text{se } 0 \leq x < \frac{1}{a} \quad (0) \\ a \cdot x - j & \text{se } \frac{j}{a} \leq x < \frac{j+1}{a} \quad (j) \\ 1 & \text{se } x = 1 \end{cases} \tag{4.19}$$

para $j \in \{1, 2, \ldots, a-1\}$.

Exemplo 4.26. Para $a = 3$, ilustra-se o gráfico da aplicação através da figura 4.2.

Observação 4.27. Os pontos fixos de g_a são os pontos de intersecção do gráfico da aplicação com a diagonal, tal como se observa na figura 4.2. Como o ponto $x = 1$ também está na diagonal, o número de pontos fixos desta aplicação é a.

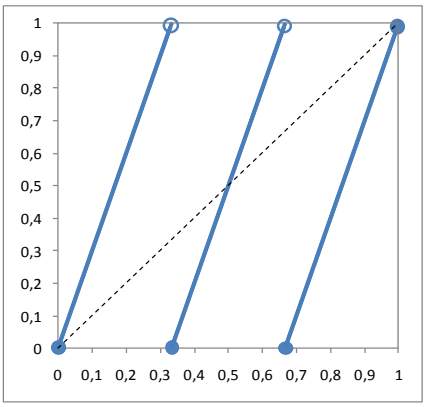

Figura 4.2: Gráfico da aplicação g_3.

Uma primeira propriedade destas aplicações foi mostrada por Iga [12] e adapta-se à notação já definida.

Facto 4.28. Para quaisquer inteiros $a, b \geq 2$ e $x \in [0,1]$, tem-se

$$g_a\left(g_b\left(x\right)\right) = g_{ab}\left(x\right) = g_{ba}\left(x\right). \tag{4.20}$$

Demonstração. Fazendo os cálculos, obtém-se

$$\begin{aligned} g_a\left(g_b\left(x\right)\right) &= g_a\left(b \cdot x \pmod 1\right) \\ &= a \cdot \left(b \cdot x \pmod 1\right) \pmod 1 \\ &= ab \cdot x \pmod 1 \end{aligned}$$

e por comutatividade do produto dos números inteiros, conclui-se a segunda igualdade. □

Teorema 4.29. *Para quaisquer inteiros positivos $a \geq 2$ e n, tem-se*

$$g_{a^n}\left(x\right) = g_a^n\left(x\right). \tag{4.21}$$

Demonstração. Por indução em n. Para $n = 1$, não há nada a provar.

Supondo o resultado verdadeiro para n,

$$\begin{aligned} g_{a^{n+1}}(x) &= g_{a^n}(g_a(x)) \\ &= g_a^n(g_a(x)) \\ &= g_a^{n+1}(x), \end{aligned}$$

o que prova o resultado para todo o $n \in \mathbb{N}$. □

Este último resultado pode ser apresentado da seguinte forma:

$$g_a^n(x) = g_{a^n}(x) = \begin{cases} a^n \cdot x & \text{se } 0 \leq x < \frac{1}{a^n} \\ a^n \cdot x - j & \text{se } \frac{j}{a^n} \leq x < \frac{j+1}{a^n} \\ 1 & \text{se } x = 1 \end{cases}. \tag{4.22}$$

Lema 4.30. Sejam $a \geq 2$ e n inteiros positivos, então g_a tem a^n pontos de período n e

$$a^n = \sum_{m|n} N_m(g_a). \tag{4.23}$$

Demonstração. Pela observação 4.27 g_{a^n} tem a^n pontos fixos. Como g_a^n e g_{a^n} são aplicações idênticas também g_a^n tem a^n pontos fixos. Mas os pontos fixos de g_a^n são precisamente os pontos n-periódicos de g_a, o que mostra a primeira parte do resultado.

Para provar a segunda afirmação basta notar o resultado da alínea (i) do teorema 4.10 que diz que os pontos de período n são os que têm período mínimo m sempre que $m|n$. □

Como consequência, e analogamente ao que foi feito acima, aplicando a fórmula de inversão de Möbius (2.8) obtém-se a expressão para o número de pontos de determinado período mínimo.

Teorema 4.31. *Sejam $a \geq 2$ e n inteiros positivos. Então*

$$N_n(g_a) = \sum_{d|n} \mu\left(\frac{n}{d}\right) a^d. \tag{4.24}$$

Conhecendo o número de pontos periódicos, é imediato calcular quantas órbitas periódicas uma aplicação tem.

Teorema 4.32. *Sejam $a \geq 2$ e n inteiros positivos, então*

$$O_n\left(g_a\right) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)a^d. \tag{4.25}$$

Conjugando o teorema 4.31 com a alínea (iii) do teorema 4.10, obtêm-se as congruências

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)a^d \equiv 0 \pmod{n}, \quad \sum_{d|n}\mu\left(d\right)a^{\frac{n}{d}} \equiv 0 \pmod{n}. \tag{4.26}$$

Esta é precisamente uma das generalizações do pequeno teorema de Fermat apresentadas no primeiro capítulo (teorema 2.15). Como se pode verificar, foi possível demonstrar este resultado da teoria de números, através da contagem de pontos periódicos de aplicações do círculo.

Existem várias aplicações que permitem demonstrar o resultado. Aqui já foram mostrados os casos das que foram designadas por $\widetilde{g}_{a,b}$ e g_a, que essencialmente são aplicações lineares do círculo. Outro exemplo é a aplicação que generaliza a aplicação tenda. Esta foi utilizada para este efeito por Basu, Bose, Sinha e Vishe em [2]. A definição pode ser encontrada, por exemplo, em [1].

Definição 4.33. A aplicação *tenda* é tal que $f_2 : [0,1] \to [0,1]$ e define-se por

$$f_2\left(x\right) = \begin{cases} 2x & \text{se } x \leq \frac{1}{2} \\ 2x-1 & \text{se } x \geq \frac{1}{2} \end{cases} \tag{4.27}$$

e está ilustrada na figura 4.3.

Note-se que das várias aplicações do círculo apresentadas, a contagem de pontos e órbitas periódicas de período mínimo superior a 1 não é influenciado pelos valores nos pontos de viragem e em 0 e 1. Por isso, para o que se vai seguir, não é essencial diferenciar $\widetilde{g}_{a,0}$ de g_a. Assim, nas ilustrações, já não será indicado qual é o valores da aplicação nos seus pontos de viragem.

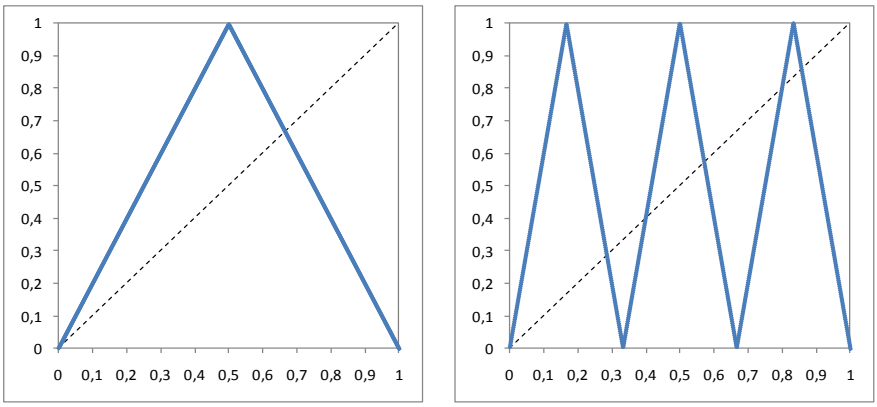

Figura 4.3: Gráfico da aplicação tenda f_2 e uma sua generalização f_6.

Quanto às diferentes abordagens que se podem fazer no que se refere aos pontos e órbitas periódicas, as aplicações do tipo g_a são mais adequadas para o estudo que se fará na próxima secção, pela simplificação de cálculos que permitem. Porém, se para fazer uma análise em termos da teoria de aplicações do intervalo, tal como, por exemplo, o fizeram Milnor e Thurston em [19] e Alsedà em [1], as aplicações que generalizam a aplicação tenda (definição 4.33) são as adequadas, uma vez que esta teoria tem como pressuposto a análise de aplicações que são contínuas no seu domínio.

4.3 Aplicações do círculo e colares

Nesta secção articulam-se conceitos dos capítulos anteriores e quando é referido um alfabeto assume-se que se trata do alfabeto base.

Tendo em atenção os resultados obtidos nos capítulos precedentes, tem-se o seguinte teorema.

Teorema 4.34. *Sejam $a \geq 2$ e n inteiros positivos. Então*

$$S(a,n) = N_n(g_a)\,, \text{ isto é, } \sharp\mathcal{S}(a,n) = \sharp\mathcal{N}_n(g_a)\,; \tag{4.28}$$

$$M(a,n) = O_n(g_a)\,, \text{ isto é, } \sharp\mathcal{M}(a,n) = \sharp\mathcal{O}_n(g_a)\,. \tag{4.29}$$

Demonstração. Imediato a partir dos teoremas 3.20, 3.21, 4.31 e 4.32. □

Este resultado mostra que estes conjuntos finitos de elementos de naturezas distintas têm cardinalidades iguais. Isto é uma evidência da existência de bijecções entre os conjuntos $\mathcal{S}(a,n)$ e $\mathcal{N}_n(g_a)$ e os conjuntos $\mathcal{M}(a,n)$ e $\mathcal{O}_n(g_a)$. Existem várias possibilidades para construir bijecções entre eles; no entanto, investigou-se no sentido de encontrar uma bijecção natural existente entre cada par de conjuntos. O resultado obtido levou à elaboração de um artigo (veja-se [23]), no qual esta secção fundamentalmente se baseia.

A inspiração do caso geral advém da observação de um exemplo.

Exemplo 4.35. Considere-se uma órbita periódica da aplicação g_4, tal como ilustra a figura 4.4.

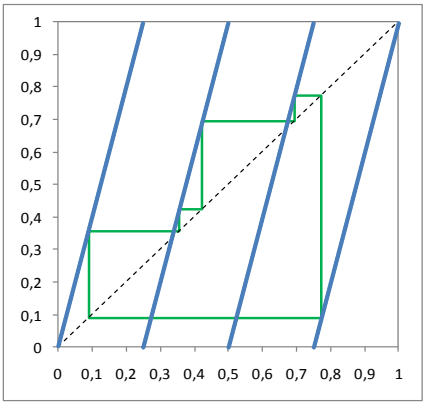

Figura 4.4: Órbita periódica da aplicação g_4.

A cada intervalo de monotonia, $I_0 = \left[0, \frac{1}{4}\right[$, $I_1 = \left[\frac{1}{4}, \frac{1}{2}\right[$, $I_2 = \left[\frac{1}{2}, \frac{3}{4}\right[$ e $I_3 = \left[\frac{3}{4}, 1\right]$ associa-se, respectivamente, o correspondente símbolo do alfabeto $\{0,1,2,3\}$. Assim, à órbita periódica desta figura associa-se a sequência 01123 ou qualquer uma sua permutação cíclica. Isto é, ao itinerário truncado de ordem 5 $(0,1,1,2,3)$ faz-se corresponder o colar aperiódico cuja representante é a palavra de Lyndon 01123.

A partir daqui faz-se a generalização.

Definição 4.36. Para cada $0 \leq j \leq a-1$, denota-se por $g_{a|j}$ a aplicação que é igual a g_a, definida apenas no ramo (intervalo de monotonia) denotado por (j).

Para cada $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, existe uma única sequência $I_n(x) = (j_1, j_2, \cdots, j_n)$ tal que $g_a^n(x) = g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x)$, chamada itinerário truncado de x de ordem n (conforme definição 4.4).

Lema 4.37. Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, tais que $I(x) = (j_1, j_2, \ldots, j_n, \ldots)$. Então tem-se

$$g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) = a^n x - \sum_{k=1}^{n} j_k a^{n-k}. \tag{4.30}$$

Demonstração. A prova faz-se por indução em n.

Para $n = 1$ tem-se

$$\begin{aligned} g_{a|j_1}(x) &= a^1 x - \sum_{k=1}^{1} j_k a^{1-k} \\ &= ax - j_1. \end{aligned}$$

Suponha-se que $g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) = a^n x - \sum_{k=1}^{n} j_k a^{n-k}$. Então

$$\begin{aligned} g_{a|j_{n+1}} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) &= g_{a|j_{n+1}} \circ g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) \\ &= g_{a|j_{n+1}} \left(a^n x - \sum_{k=1}^{n} j_k a^{n-k} \right) \\ &= a \left(a^n x - \sum_{k=1}^{n} j_k a^{n-k} \right) - j_{n+1} \\ &= a^{n+1} x - \sum_{k=1}^{n+1} j_k a^{n+1-k}, \end{aligned}$$

o que prova o resultado para qualquer $n \in \mathbb{N}$. □

Teorema 4.38. *Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, tais que x é um ponto*

periódico de g_a de período n, com itinerário truncado de ordem n $I_n(x) = (j_1, \cdots, j_n)$. Então

$$x = \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n - 1}. \tag{4.31}$$

Demonstração. Conjugando as hipóteses do teorema com o lema anterior, tem-se

$$\begin{aligned} x &= g_a^n(x) \\ &= g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) \\ &= a^n x - \sum_{k=1}^{n} j_k a^{n-k}. \end{aligned}$$

Daqui, resolvendo a igualdade em ordem a x, o resultado é imediato. □

O inverso também é verdadeiro.

Teorema 4.39. *Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, tais que para $k \in \{1, 2, \ldots, n\}$, $j_k \in \{0, 1, \ldots, a-1\}$ e*

$$x = \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n - 1}. \tag{4.32}$$

Então x é um ponto periódico de g_a de período n, com o itinerário truncado de ordem n $I_n(x) = (j_1, \cdots, j_n)$.

Demonstração. Calcule-se a n-ésima iteração de x através da aplicação g_a pelo itinerário $I(x) = (j_1, \ldots, j_n, \ldots)$. Aplicando o lema 4.37,

$$\begin{aligned} g_{a|j_n} \circ \cdots \circ g_{a|j_1}(x) &= a^n x - \sum_{k=1}^{n} j_k a^{n-k} \\ &= a^n \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n - 1} - \sum_{k=1}^{n} j_k a^{n-k}, \end{aligned}$$

pelo que

$$\begin{aligned} g_{a|j_n} \circ \cdots \circ g_{a|j_1}(x) &= \frac{a^n \sum_{k=1}^{n} j_k a^{n-k} - (a^n - 1) \sum_{k=1}^{n} j_k a^{n-k}}{a^n - 1} \\ &= \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n - 1} \\ &= x \end{aligned}$$

logo, n é período de x. □

O próximo resultado diz que se x é um ponto de período $2n$ de g_a e o seu itinerário truncado de ordem $2n$, $I_n(x)$, é a concatenação de duas sequências iguais de comprimento n, então n é um período de x.

Teorema 4.40. *Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, tais que x é um ponto de período $2n$ de g_a, com o itinerário truncado de ordem $2n$ $I_{2n}(x) = (j_1, \cdots, j_n, j_1, \cdots, j_n)$. Então x é um ponto de período n.*

Demonstração. Utilizando o lema 4.37, tem-se

$$\begin{aligned} g_a^{2n}(x) &= g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1} \circ g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1}(x) \\ &= g_{a|j_n} \circ \cdots \circ g_{a|j_2} \circ g_{a|j_1} \left(a^n x - \sum_{k=1}^{n} j_k a^{n-k} \right) \\ &= a^n \left(a^n x - \sum_{k=1}^{n} j_k a^{n-k} \right) - \sum_{k=1}^{n} j_k a^{n-k} \\ &= a^{2n} x - \sum_{k=1}^{n} j_k \left(a^{2n-k} + a^{n-k} \right). \end{aligned}$$

Como por hipótese x tem período $2n$ é imediato que

$$x = a^{2n} x - \sum_{k=1}^{n} j_k \left(a^{2n-k} + a^{n-k} \right). \tag{4.33}$$

Resolvendo em ordem a x obtém-se

$$\begin{aligned} x &= \frac{\sum_{k=1}^{n} j_k \left(a^{2n-k} + a^{n-k}\right)}{a^{2n}-1} \\ &= \frac{(a^n+1)\sum_{k=1}^{n} j_k a^{n-k}}{(a^n+1)(a^n-1)} \\ &= \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n-1}. \end{aligned}$$

Pelo teorema 4.39 x é um ponto de período n. □

Esta propriedade corresponde à condição de primitividade (3.3) definida para palavras sobre alfabetos. Isto significa que considerando um itinerário truncado de uma órbita periódica de g_a e a sua identificação com uma palavra do alfabeto correspondente, essa palavra será primitiva.

Existem agora em condições de definir as bijecções procuradas.

Definição 4.41. Definem-se as aplicações

$$\begin{array}{rccc} \rho: & \mathcal{S}(a;n) & \to & \mathcal{N}_n(g_a) \\ & u = u_1,\ldots,u_n & \mapsto & \frac{\sum_{k=1}^{n} u_k a^{n-k}}{a^n-1} \end{array} \tag{4.34}$$

$$\begin{array}{rccc} \overrightarrow{\rho}: & \mathcal{L}(a;n) & \to & \mathcal{O}_n(g_a) \\ & u & \mapsto & \left[\left(\rho(u), g_a(\rho(u)), g_a^2(\rho(u)), \ldots, g_a^{n-1}(\rho(u))\right)\right] \end{array}. \tag{4.35}$$

Teorema 4.42. *As aplicações ρ e $\overrightarrow{\rho}$ são bijecções.*

Demonstração. A aplicação ρ é bijectiva pelos teoremas 4.38 e 4.39.

Quanto à aplicação $\overrightarrow{\rho}$, começa-se por demonstrar a injectividade.

Sejam $u = u_1 \cdots u_n$ e $v = v_1 \cdots v_n$ duas palavras de Lyndon diferentes de $\mathcal{L}(a;n)$. Por definição estas representam colares diferentes. Isto é, correspondem a itinerários truncados que não são a permutação cíclica um do outro.

Como ρ é bijectiva, $\rho(u) \neq \rho(v)$. Mais ainda, $\rho(u)$ é diferente de qualquer dos valores $\rho(v), g_a(\rho(v)), g_a^2(\rho(v)), \ldots, g_a^{n-1}(\rho(v))$. Portanto $\overrightarrow{\rho}$ é injectiva.

Veja-se agora a sobrejectividade de $\overrightarrow{\rho}$.

Seja $(x_1, x_2, \ldots, x_n) \in \mathcal{O}_n(g_a)$. Então $x_1, x_2, \ldots, x_n$ são pontos periódicos de g_a de período n, isto é, $x_1, x_2, \ldots, x_n \in \mathcal{N}_n(g_a)$. Como todos os pontos estão sobre a mesma órbita periódica, os respectivos $I_n(x)$ estão relacionados por permutações cíclicas. Considere-se o itinerário que corresponde uma palavra de Lyndon v (o menor de entre eles, relativamente à ordem lexicográfica). Seja $y \in \{x_1, x_2, \ldots, x_n\}$ o ponto que tem este itinerário. Então $\overrightarrow{\rho}(v) = \left[\left(y, g_a(y), g_a^2(y), \ldots, g_a^{n-1}(y)\right)\right]$, que é o mesmo que $[(x_1, x_2, \ldots, x_n)]$. Logo, a aplicação $\overrightarrow{\rho}$ é sobrejectiva. □

Uma bijecção entre os conjuntos $\mathcal{M}(a, n)$ e $\mathcal{O}_n(g_a)$ é consequência da bijecção (4.35).

Definição 4.43. Define-se a aplicação

$$\begin{array}{rccc} \overline{\rho}: & \mathcal{M}(a;n) & \to & \mathcal{O}_n(g_a) \\ & [u] & \mapsto & \left[\left(\rho(u), g_a(\rho(u)), g_a^2(\rho(u)), \ldots, g_a^{n-1}(\rho(u))\right)\right] \end{array} . \quad (4.36)$$

A seguir está ilustrado um exemplo que foi apresentado no *Recreational Mathematics Colloquium II* [22].

Exemplo 4.44. A figura 4.5 ilustra um exemplo das bijecções acima definidas.

No exemplo que se segue ilustram-se todas as órbitas periódicas para o caso $a = 3$ e $n = 4$ e respectivas palavras de Lyndon.

Exemplo 4.45. O conjunto das órbitas periódicas da aplicação g_3 de período 4 e respectivas palavras de Lyndon estão representados através das figuras 4.6 a 4.14.

Verificou-se que é possível obter todas as palavras de Lyndon de comprimento n de um alfabeto de cardinalidade a, através de todas as órbitas periódicas de período mínimo n da aplicação do círculo definida em (4.18), ou simplesmente por $a \cdot x \pmod 1$, se $n > 1$. O procedimento é o seguinte:

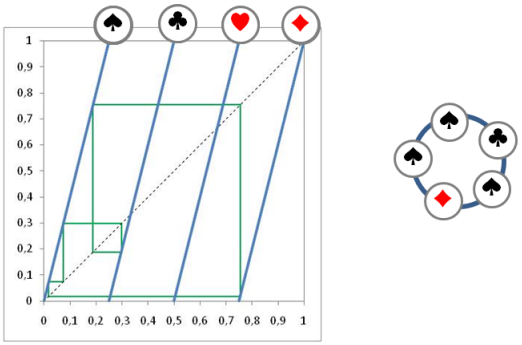

Figura 4.5: Órbita de período 5 de g_4 e o correspondente colar do alfabeto de naipes.

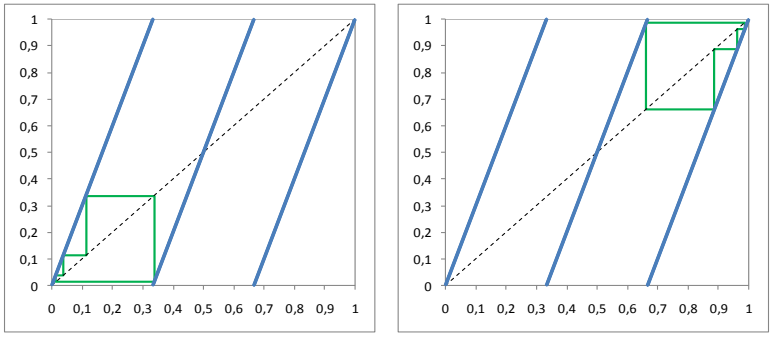

Figura 4.6: Órbitas de g_3 correspondentes às palavras 0001 e 1222.

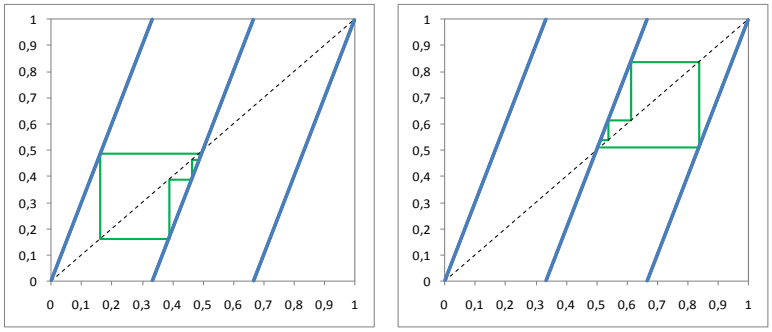

Figura 4.7: Órbitas de g_3 correspondentes às palavras 0111 e 1112.

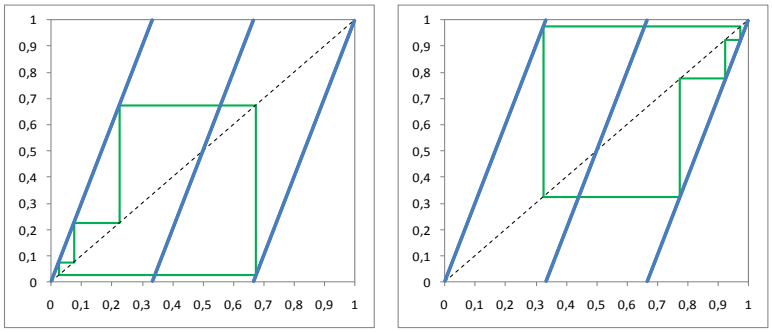

Figura 4.8: Órbitas de g_3 correspondentes às palavras 0002 e 0222.

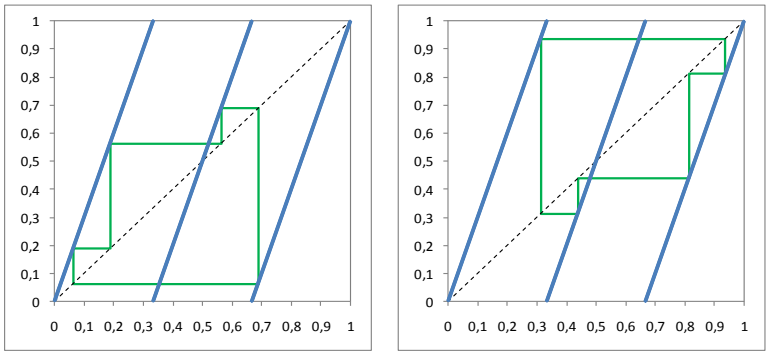

Figura 4.9: Órbitas de g_3 correspondentes às palavras 0012 e 0221.

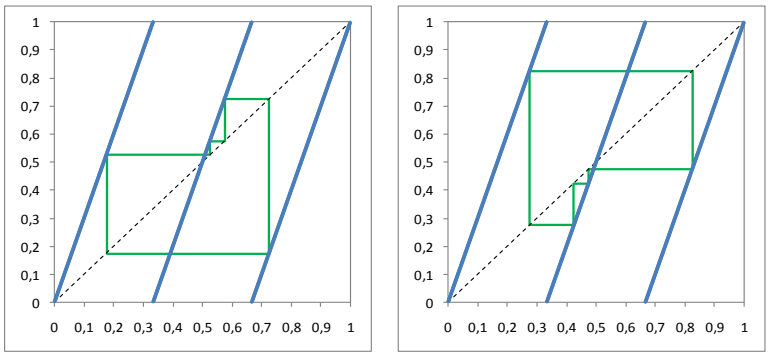

Figura 4.10: Órbitas de g_3 correspondentes às palavras 0112 e 0211.

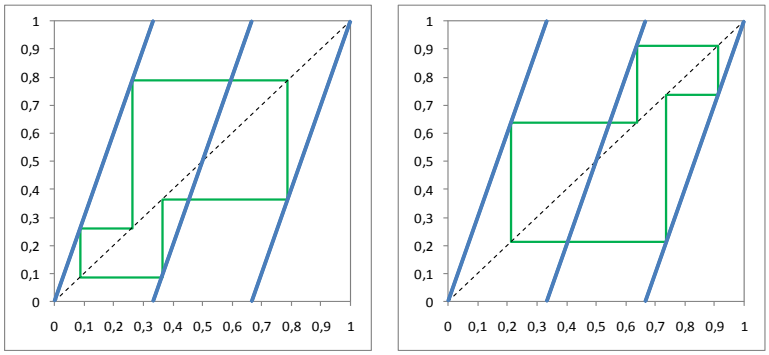

Figura 4.11: Órbitas de g_3 correspondentes às palavras 0021 e 0122.

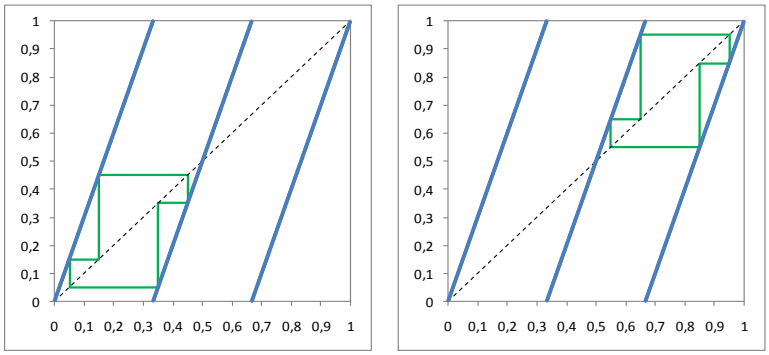

Figura 4.12: Órbitas de g_3 correspondentes às palavras 0011 e 1122.

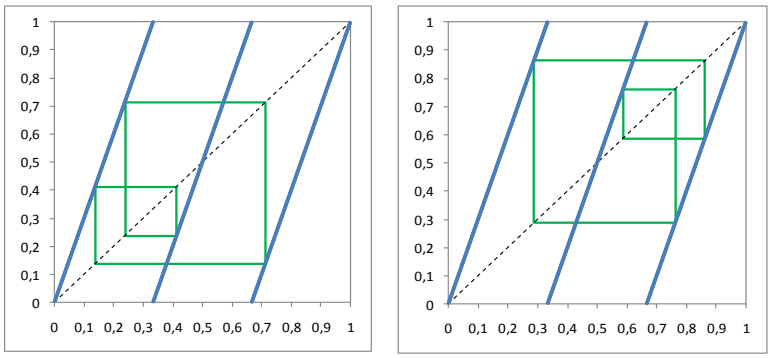

Figura 4.13: Órbitas de g_3 correspondentes às palavras 0102 e 0212.

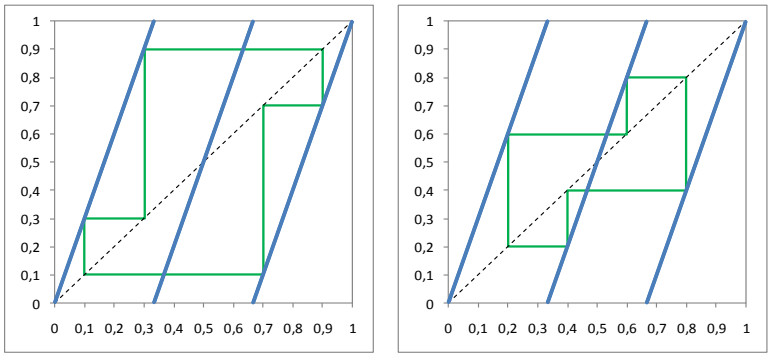

Figura 4.14: Órbitas de g_3 correspondentes às palavras 0022 e 0121.

1. Ao construir uma órbita periódica deve reter-se um seu itinerário. Este itinerário representa uma palavra primitiva.

2. A palavra que representa o colar dessa palavra será a palavra de Lyndon, a menor no que respeita à ordem lexicográfica.

Visualmente, podem identificar-se as aplicações do círculo $a \cdot x \pmod 1$ como aquilo a que se pode chamar "teares" de colares aperiódicos. Considerando um alfabeto de cores, identificar-se-ia cada ramo com uma cor. Colocando um fio a percorrer uma órbita periódica, cada vez que esta toque no gráfico da aplicação irá receber uma peça da cor respectiva, formando assim um colar ao chegar ao ponto inicial.

Inversamente, também foi visto que tendo uma palavra de Lyndon (ou, mais geralmente, uma palavra primitiva) é possível calcular explicitamente os pontos da órbita periódica correspondente (veja-se a fórmula (4.31)).

Após a definição da aplicação ρ que relaciona os elementos de dois conjuntos totalmente ordenados, averigua-se o que acontece às ordenações dos conjuntos envolvidos nesta aplicação. Um primeiro facto, que advém da definição da aplicação g_a, é que para ela se verifica

$$\forall x, y \in [0,1] : x \leq y \Leftrightarrow (A(x) \prec A(y)) \vee (A(x) = A(y)) . \tag{4.37}$$

Esta propriedade refere-se ao endereço de cada ponto periódico. A questão da

ordenação de palavras (itinerários - ordem lexicográfica) em paralelo com a relação usual dos números naturais para os correspondentes pontos periódicos definidos por ρ não é, contudo, tão imediata.

Chegando a este ponto surge naturalmente a seguinte conjectura.

Conjectura 4.46. A aplicação ρ preserva a ordem, isto é, a ordem lexicográfica de $\mathcal{S}(a, n)$ e a ordem dos números reais em $\mathcal{N}_n(g_a)$ mantém-se.

Observação 4.47. Esta conjectura é verificada empiricamente para os vários exemplos estudados.

Uma consequência desta conjectura é:

1. A aplicação ρ aplica uma palavra de Lyndon no menor ponto periódico da órbita que lhe corresponde (no sentido da ordem usual nos reais).
2. Aplicando ρ^{-1} ao menor ponto periódico de uma dada órbita obtém-se uma palavra de Lyndon.

5

Aplicações a linguagens faladas

5.1 Exemplos

Os resultados do capítulo anterior relacionam conceitos matemáticos de combinatória de palavras, em especial os colares, com órbitas de sistemas dinâmicos.

Os conceitos definidos abstractamente podem ser aplicados, naturalmente, aos alfabetos de linguagens faladas. É pois possível representar palavras do nosso dia-a-dia sob a forma de órbitas periódicas, desde que estas sejam primitivas. A sua colecção será assim um dicionário dinâmico de palavras. Note-se que são pouquíssimas as palavras portuguesas que não são primitivas e também o mesmo se passa para as palavras inglesas.

Relativamente à língua inglesa, por exemplo, sabendo que o respectivo alfabeto é constituído por 26 letras, pode utilizar-se a aplicação do círculo (4.18) com $a = 26$. Quanto à língua portuguesa, evitando a sobrecarga de acentos e cedilhas, também é possível utilizar o mesmo alfabeto.

Observação 5.1. As aplicações do círculo do tipo g_a são expansivas para $a > 1$, e sendo lineares o coeficiente de expansividade local é a em todos os pontos. Por esse motivo, para a construção gráfica de uma órbita periódica com $a = 26$ torna-se crítica a localização rigorosa dos pontos periódicos. Se esta não for feita com a devida precisão, ao construí-la através da iteração do primeiro ponto a instabilidade pode desviar a periodicidade da órbita devido a erros de aproximação numérica.

Exemplo 5.2. Com $a = 26$ e $n = 8$, a figura 5.1 ilustra duas palavras com significado linguístico.

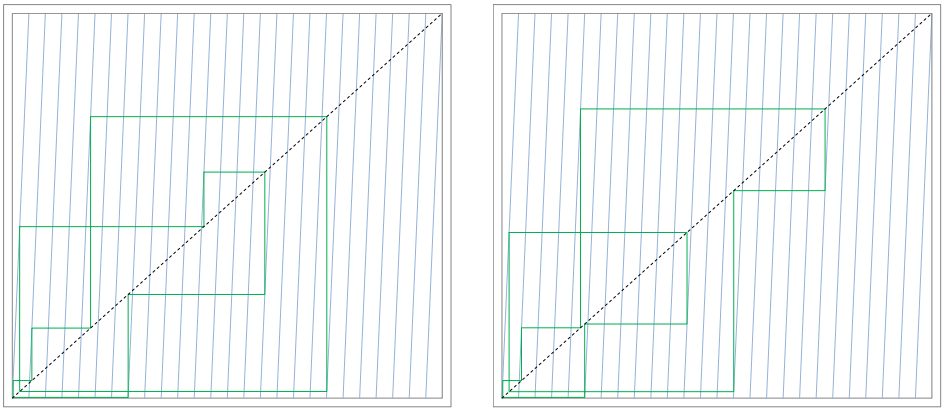

Figura 5.1: Órbitas correspondentes às palavras *alphabet* e *alfabeto*.

Neste exemplo, o primeiro gráfico representa as palavras *alphabet, lphabeta, phabetal, habetalp, abetalph, betalpha, etalphab e talphabe* que formam um colar de $\mathcal{M}(26, 8)$. Destas, as palavras com significado linguístico são:

alphabet - conjunto finito não vazio de símbolos.

phabetal - jogo cujo objectivo é formar sequências de letras ou palavras.[1]

betalpha (Human *Betalpha* Synuclein protein) - recombinante humano b-Synuclein produzido em E.coli.[2]

[1]Fonte: http://www.newgrounds.com/portal/view/240545, acedido em 23/09/2011.

[2]Fonte: http://www.biorbyt.com/human-betalpha-synuclein-protein, acedido em 23/09/2011.

Letra	No alfabeto base	Ponto x	Letra	No alfabeto base	Ponto x
A	0	0,017141	A	0	0,016557
L	11	0,445665	L	11	0,430476
P	15	0,587281	F	5	0,192375
H	7	0,269298	A	0	0,001750
A	0	0,001748	B	1	0,045490
B	1	0,045461	E	4	0,182750
E	4	0,181978	T	19	0,751504
T	19	0,731429	O	14	0,539098

Tabela 5.1: Valores referentes às órbitas das palavras *alphabet* e *alfabeto*.

A palavra de Lyndon que representa este colar é *abetalph*.

Já o colar da palavra *alfabeto* não contém outra palavra com significado linguístico, sendo a palavra de Lyndon que a representa *abetoalf*.

Para a construção deste exemplo foram utilizados os valores que se apresentam na tabela 5.1 (os valores estão apresentados com arredondamentos a 6 casas decimais).

Os cálculos para os pontos das órbitas foram feitos aplicando a fórmula (4.31). Por exemplo, na órbita *alphabet* obtém-se o valor:

$$\begin{aligned} x_1 &= \frac{11 \cdot 26^6 + 15 \cdot 26^5 + 7 \cdot 26^4 + 26^2 + 4 \cdot 26 + 19}{26^8 - 1} \\ &= \frac{3\,579\,493\,807}{208\,827\,064\,575} \\ &\approx 0,017141. \end{aligned}$$

Exemplo 5.3. O nome da autora escrito sob a forma de órbitas periódicas (figura 5.2).

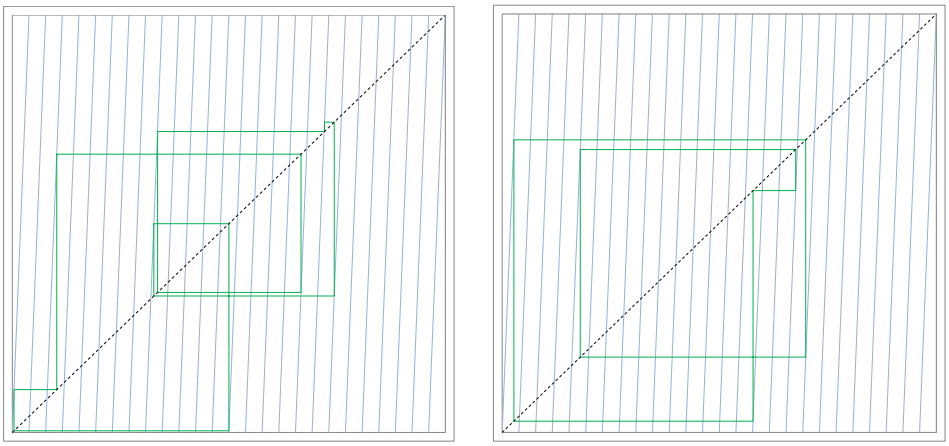

Figura 5.2: Órbitas correspondentes às palavras *Cristina* e *Serpa*.

5.2 Cifras de César e Atbash

Uma vez que existe uma correspondência entre palavras e órbitas periódicas, veja-se o que acontece às órbitas quando a uma palavra inicial são aplicados determinados códigos de cifragem. As cifras utilizadas são regras muito simples e não representam as codificações de mensagens mais usuais hoje em dia. Pertencem a um grupo de cifras chamadas clássicas (conforme descritas em [17]). Algumas destas técnicas de encriptação tornaram-se bastante conhecidas e usadas durante séculos. No entanto, a sua utilização actual não é usual devido à pouca segurança que garantem. A sua reduzida sofisticação permite que a desencriptação seja simples.

Introduzir-se-á, em primeiro lugar, os conceitos base (veja-se, por exemplo [5]).

Definição 5.4. Um *sistema criptográfico* é um 5-tuplo $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \varepsilon, \mathcal{D})$ com as seguintes propriedades:

1. $\mathcal{P}$ é um conjunto chamado *conjunto de textos*.
2. $\mathcal{C}$ é um conjunto chamado *conjunto de criptogramas*.
3. $\mathcal{K}$ é um conjunto chamado *espaço de chaves*.

4. $\varepsilon = \{E_k : k \in \mathcal{K}\}$ é uma família de funções invertíveis $E_k : \mathcal{P} \to \mathcal{C}$ chamadas *funções de cifragem*.

5. $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ é uma família de funções $D_k : \mathcal{C} \to \mathcal{P}$ chamadas *funções de decifragem*, que corresponde à família das funções inversas das funções de ε.

6. Para cada $e \in \mathcal{K}$, existe um $d \in \mathcal{K}$ tal que $D_d(E_e(p)) = p$, para todo o $p \in \mathcal{P}$.

Aqui, $\mathcal{P}$ e $\mathcal{C}$ são alfabetos e considera-se que são iguais.

Uma das variantes das cifras clássicas são as chamadas cifras de substituição (veja-se [17]).

Definição 5.5. Seja A um alfabeto de a letras e T_n o conjunto de todas as palavras de A comprimento n. Seja $\mathcal{K}$ o conjunto de todas as permutações de elementos de A. Seja, para cada $e \in \mathcal{K}$, definida a função de cifragem

$$\begin{aligned} E_e(t) &= (e(t_1)\, e(t_3) \cdots e(t_n)) \\ &= (c_1 c_2 \cdots c_n) \\ &= c, \end{aligned}$$

onde $t = (t_1 t_2 \cdots t_n) \in T_n$. Por outras palavras, substitui-se cada símbolo no n-tuplo, por um símbolo de A de acordo com a permutação e fixada. Para decifrar $c = (c_1 c_2 \cdots c_n)$ calcula-se a permutação inversa $d = e^{-1}$ e

$$\begin{aligned} E_d(c) &= (d(c_1)\, d(c_3) \cdots d(c_n)) \\ &= (t_1 t_2 \cdots t_n) \\ &= t. \end{aligned}$$

A uma função E_e assim definida dá-se o nome de *cifra de substituição simples* ou *cifra de substituição mono-alfabética*.

O número de cifras de substituição simples é $a!$, pois é o número de permutações de elementos de A.

Dentro deste grupo de cifras está a cifra afim.

Definição 5.6. Seja A um alfabeto de a letras. Seja E_e uma cifra de substituição simples tal que

$$e(u) = \alpha u + \beta \pmod{a} \tag{5.1}$$

onde a e a_1 são primos entre si. A uma cifra E_e assim definida dá-se o nome de *cifra afim*.

Ir-se-á designar por $e_{(\alpha,\beta)}$ a cifra definida em (5.1).

Observação 5.7. A função de decifragem de uma cifra afim é

$$d(u) = \alpha'(u - \beta) \pmod{a} \tag{5.2}$$

sendo a_1' a solução da congruência $\alpha\alpha' \equiv 1 \pmod{a}$.

Observação 5.8. Uma cifra afim também é por vezes chamada de *cifra linear* e se $\beta = 0$ ela será uma *cifra de dizimação*.

De seguida apresentam-se dois casos particulares deste tipo de cifra que foram usados na Antiguidade.

Definição 5.9. Chama-se *cifra de César* a uma cifra afim da forma

$$e_{(1,\beta)}(u) = u + \beta \pmod{a}. \tag{5.3}$$

A cifra de César é assim chamada devido ao seu autor Júlio César que a utilizou em cerca de 50 a.c. para escrever, nomeadamente, a Marco Cícero (veja-se [15]), com $a = 26$ e $\beta = 3$ e está representada na tabela 5.2.

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabela 5.2: Cifra de César - função de codificação com $a = 26$, $\beta = 3$.

Definição 5.10. Chama-se *cifra de Atbash* a uma cifra afim da forma

$$e_{(-1,-1)}(u) = -u - 1 \pmod{a}. \tag{5.4}$$

A cifra de Atbash assim definida é a transposição para a terminologia aqui utilizada da descrição dada por Noegel em [20]. Foi originalmente utilizada pelos judeus na sua bíblia em algumas palavras específicas, nomeadamente na palavra *Babilónia*. É uma técnica que substitui a primeira letra do alfabeto pela última, a segunda pela penúltima, a terceira pela ante-penúltima e assim por adiante, como ilustra a tabela 5.3. Note-se que o alfabeto utilizado na bíblia hebraica era o hebraico, que é composto por menos letras.

O curioso desta cifra é que a função de cifragem é exactamente igual à função de decifragem. Esta cifra não é, em geral, referida nos manuais de criptografia.

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Tabela 5.3: Cifra de Atbash - função de codificação para o alfabeto inglês.

Veja-se agora o que acontece aos pontos periódicos se se aplicar uma cifra de substituição simples ao seu itinerário truncado.

Para $a \geq 2$ e x um ponto periódico de g_a de período mínimo n, designa-se por $x_{(\alpha,\beta)}$ o ponto periódico de g_a com o itinerário truncado de ordem n que é o resultado da aplicação de $E_{e_{(\alpha,\beta)}}$ ao itinerário truncado de x de ordem n.

Pela fórmula (4.31), x é da forma $x = \frac{\sum_{k=1}^{n} j_k a^{n-k}}{a^n-1}$, sendo $(j_1, \cdots, j_n)$ o seu itinerário truncado de ordem n. Então, aplicando a cifra $e_{(\alpha,\beta)}$ ao itinerário truncadode x de ordem n obtém-se um novo itinerário truncado de ordem n cujo ponto periódico $x_{(\alpha,\beta)}$ é

$$x_{(\alpha,\beta)} = \frac{\sum_{k=1}^{n} \left(\alpha j_k + \beta \pmod a\right) a^{n-k}}{a^n - 1}. \tag{5.5}$$

Esta é uma fórmula muito geral.

Particularizando para a cifra de César, obtém-se o seguinte resultado.

Facto 5.11. Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0,1]$, tais que x é um ponto periódico de período n de g_a e todos os pontos da sua órbita periódica estão em $\left]\frac{i}{a-1}, \frac{j}{a-1}\right[$,

onde $i < j$, $i, j \in \{0, 1, \ldots, a-1\}$. Então $\forall \beta \in \mathbb{N}$ e $-i \leq \beta \leq a - j - 1$,

$$x_{(1,\beta)} = x + \frac{\beta}{a-1} \tag{5.6}$$

e $x_{(1,\beta)}$ é um ponto periódico com o mesmo período de x e a sua órbita é uma translação ao longo da recta $x = y$ da órbita de x.

Demonstração. Dada a simetria do gráfico de g_a, é claro o resultado. □

Exemplo 5.12. A figura 4.12 mostra um exemplo, com $\beta = 1$, $i = 0$ e $j = 1$.

Exemplo 5.13. A figura 5.3 ilustra este facto com $\beta = 3$.

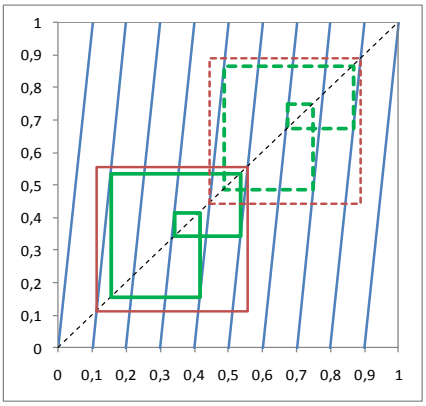

Figura 5.3: Aplicação da cifra de César ao itinerário de uma órbita periódica.

Para o caso da cifra de Atbash, o resultado é o seguinte.

Facto 5.14. Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0, 1]$, tais que x é um ponto periódico de período n de g_a. Então

$$x_{(-1,-1)} = 1 - x \tag{5.7}$$

e $x_{(-1,-1)}$ é um ponto periódico com o mesmo período de x e a sua órbita é uma rotação de ângulo π e centro $\left(\frac{1}{2}, \frac{1}{2}\right)$ da órbita de x.

Demonstração. Dada a simetria do gráfico de g_a, é claro o resultado (visualizar o gráfico de baixo para cima). □

Exemplo 5.15. As figuras 4.6 a 4.13 são exemplificativas deste resultado.

Exemplo 5.16. A figura 5.4 ilustra este facto.

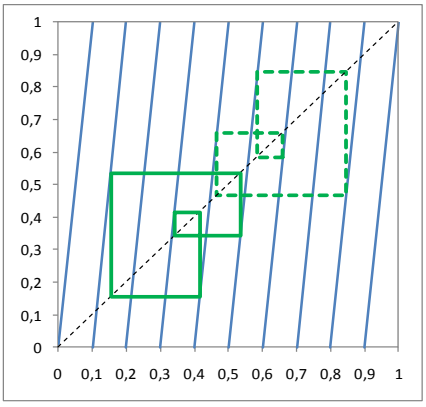

Figura 5.4: Aplicação da cifra Atbash ao itinerário de uma órbita periódica.

Se o alfabeto for restringido é possível generalizar um pouco este último teorema. Isto porque o itinerário truncado de um ponto periódico é composto por letras que são elementos de um subconjunto do alfabeto base $A_{i,j} = \{i, i+1, \ldots, j-1, j\}$, com $i \leq j$, $i, j \in \{0, 1, \ldots, a-1\}$. Para isso, designa-se por $x^{i:j}_{(-1,-1)}$ o ponto periódico de g_a com o itinerário truncado que é o resultado da aplicação de $E_{e_{(-1,-1)}}$ ao itinerário truncado de x, considerando o alfabeto $A_{i,j}$.

Facto 5.17. Sejam $n \in \mathbb{N}$, $a \geq 2$ e $x \in [0, 1]$, tais que x é um ponto periódico de período n de g_a e todos os pontos da sua órbita periódica estão em $\left]\frac{i}{a-1}, \frac{j}{a-1}\right[$, onde $i < j$, $i, j \in \{0, 1, \ldots, a-1\}$. Então,

$$x^{i:j}_{(-1,-1)} = \frac{i+j}{a-1} - x \tag{5.8}$$

e $x^{i:j}_{(-1,-1)}$ é um ponto periódico com o mesmo período de x e a sua órbita é uma rotação de ângulo π e centro $\left(\frac{i+j}{2a-2}, \frac{i+j}{2a-2}\right)$ da órbita de x.

Demonstração. Dada a simetria do gráfico de g_a, é claro o resultado (visualizar o gráfico de baixo para cima, na restrição de $\left]\frac{i}{a-1}, \frac{j}{a-1}\right[$). □

Exemplo 5.18. A figura 5.5 ilustra este último facto, onde o quadrado representa a restrição feita ao alfabeto.

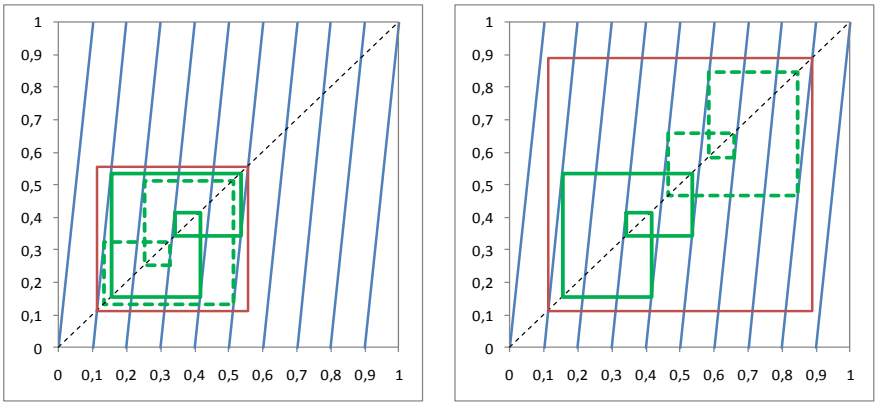

Figura 5.5: Aplicações da cifra Atbash ao itinerário de uma órbita periódica, com restrição do alfabeto.

6

Conclusões

A utilização dos sistemas dinâmicos para demonstrar resultados de outras áreas da Matemática tem tido desenvolvimentos recentes, nomeadamente através da publicação de artigos científicos que provam resultados da teoria dos números. É o caso concreto do pequeno teorema de Fermat e suas generalizações. Conjugando esta metodologia com a dos colares para o mesmo efeito, vai-se mais além construindo bijecções que justificam que ambas as abordagens permitem demonstrar os mesmos resultados. A principal contribuição deste trabalho é pois a de fazer corresponder colares aperiódicos e órbitas periódicas, bem como palavras primitivas e pontos periódicos.

Partindo deste ponto, foi abordada uma ideia de aplicar este tema a palavras que não são apenas formais, mas faladas, chegando a ilustrar o efeito das cifras de César e de Atbash nos objectos trabalhados.

Outra possível aplicação é fazer uma abordagem lúdica e recreativa do tema, recorrendo a simbologias mais apelativas na escolha dos alfabetos a utilizar,

por exemplo, os naipes de cartas, os símbolos do Zodíaco e as cores. Os colares são em si muito ilustrativos de objectos concretos da realidade quotidiana das pessoas e da sua criatividade. Neste âmbito dir-se-ia que as aplicações do círculo apresentadas são "teares" de colares aperiódicos. Foi neste sentido que a autora apresentou uma palestra no *Recreational Mathematics Colloquium II*, na Universidade de Évora, a 27-04-2011 ([22]).

Ainda no capítulo sobre as questões na óptica da teoria dos números, foi apresentada uma fórmula alternativa da generalização de Gauss e Gegenbauer. Apesar da sua expressão ser um pouco mais extensa, tem a vantagem de, na prática, não ser necessário identificar todos os divisores de n. Assim, após a obtenção da decomposição de n em números primos, cada parcela será a potência de base a e expoente que é o produto de n/P pelas possíveis combinações de primos presentes na decomposição, afectada do sinal respectivo que alterna consoante o número de factores primos. Note-se que se $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ então $P = p_1 p_2 \cdots p_k$ e $n/P = p_1^{i_1-1} p_2^{i_2-1} \cdots p_k^{i_k-1}$.

Uma primeira questão que fica em aberto é a se a bijecção ρ preserva a ordenação (ordem lexicográfica e ordem dos números reais). Em termos empíricos verifica-se a esta conjectura.

Outros desenvolvimentos poderiam ser feitos partindo do que aqui se fez. Por exemplo, para a construção das bijecções, em vez de trabalhar com as aplicações do círculo do tipo $ax \pmod 1$, poder-se-ia enveredar pelo estudo das aplicações $ax + b \pmod 1$ ou das aplicações tipo tenda. As fórmulas que se obteriam seriam diferentes e provavelmente com expressões mais exigentes em termos de cálculo. Quanto à opção de aplicações tipo tenda, haveria a vantagem de se poder conjugar esta metodologia com o estudo de aplicações do intervalo contínuas e monótonas por troços tal como feito por Milnor e Thurston [19]. O que falha nas aplicações do tipo $ax \pmod 1$ para não ser possível aplicar directamente o estudo destes autores é a continuidade que não é verificada.

Quanto a mais consequências e futuras investigações que este tema poderá trazer, à partida poderão ser variadas, uma vez que estão envolvidas várias áreas da Matemática e por esse facto cada uma delas poderá vir a beneficiar

de futuros desenvolvimentos que para já não foram identificados.

Para concluir, note-se uma curiosidade sobre primitividade que se encontra neste trabalho. Conforme definido, as palavras primitivas são as palavras aperiódicas e dentro do mesmo colar pode identificar-se aquela primitiva que se caracteriza por ser a menor, em termos lexicográficos e que é uma palavra de Lyndon. Existe um resultado de linguagens formais que nos diz que toda a palavra admite uma factorização única como produto não decrescente de palavras de Lyndon (veja-se, por exemplo, [21]) que de facto são também primitivas. Por outro lado, sabe-se que qualquer número inteiro se decompõe de forma única como produto de números primos. O curioso é que o número de palavras primitivas de comprimento n é obtido por uma fórmula que depende directamente da decomposição em factores primos de n. Analogamente, o número de palavras de Lyndon de comprimento n também depende da decomposição em factores primos de n.

Índice

Bibliografia

[1] Lluís Alsedà, Jaume Llibre, Michał Misiurewicz, *Combinatorial Dynamics an Entropy in Dimension One*, Advances Series in Nonlinear Dynamics, Volume 5, World Scientific, 1993.

[2] Somnath Basu, Anindita Bose, Sumit Sinha e Pankaj Vishe, *Necklaces, Periodic Points and Permutations Representations - Fermat's Little Theorem*, Resonance, pp. 18-26, November 2001.

[3] Jean Berstel e Dominique Perrin, *The origins of combinatorics on words*, European Journal of Combinatorics, 28 (2007) 996-1022.

[4] W. E. Briggs e William L. Briggs, *Anatomy of a Circle Map*, Mathematics Magazine, Vol. 72, No. 2 (Apr. 1999), pp.116-125.

[5] Johannes A. Buchmann, *Introduction to Cryptography*, Second Edition, Springer, 2004.

[6] David M. Burton, *Elementary number theory*, Sixth Edition, McGraw-Hill, 2007.

[7] Robert L. Devaney, *An Introduction to Chaotic Dynamical Systems*, Second Edition, Addison-Wesley Publising Company, 1989.

[8] Leonard Eugene Dickson, *History of the Theory of Numbers, Vol. 1: Divisibility and primality*, Carnegie Institution of Washington, Publication No. 256, 1919.

[9] M. Frame, B. Johnson e J. Sauerberg, *Fixed Points and Fermat: A Dynamical Systems Approach to Number Theory*, The Mathematical Association of America, Monthly 107, May 2000, 422-428.

[10] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Fifth Edition, 1979.

[11] Boris Hasselblatt e Anatole Katok, *A First Course in Dynamics with panorama of recent developments*, Cambridge University Press, 2003.

[12] K. Iga, *A Dynamical Systems Proof of Fermat's Little Theorem*, Mathematics Magazine, Vol. 76, No. 1, February 2003, 48-51.

[13] I. M. Isaacs e M. R. Pournaki, *Generalizations of Fermat's Little Theorem via Group Theory*, The Mathematical Association of America, Monthly, Vol. 112, No. 8, October 2005, 734-740.

[14] L. Levine, *Fermat's Little Theorem: A Proof by Function Iteration*, Mathematics Magazine, Vol. 72, No. 4, October 1999, 308-309.

[15] Dennis Luciano e Gordon Prichett, *From Caesar Ciphers to Public-Key Cryptosystems*, The College Mathematics Journal, Vol. 18, No. 1 (Jan. 1987), pp. 2-17.

[16] J. Matoušek e J. Nešetřil, *Invitation to discrete mathematics*, Second Edition, Oxford University Press, 2009.

[17] Alfred J. Menezes, Paul C. van Oorschot e Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[18] N. Metropolis e Gian-Carlo Rota, *Witt Vectors and the Algebra of Necklaces*, Advances in Mathematics 50, 95-125, 1983.

[19] John Milnor e William Thurston, *On iterated maps of the interval*, Lectures notes on Mathematics, Springer, 1988, Volume 1342/1988, 465-563.

[20] Scott B. Noegel, *Atbash in Jeremiah and Its Literary Significance: Part I*, Jewish Bible Quartely 24/2 (1996), 82-89.

[21] G. Rozenberg e A. Salomaa Eds, *Handbook of Formal Languages*, Vol. 1, Word Language Grammar, Springer, 1997.

[22] Cristina Serpa, *A dynamical approach to necklaces and words*, conference proceedings, submetido para publicação.

[23] Cristina Serpa e Jorge Buescu, *Circle maps and Lyndon words - a dynamical approach to aperiodic necklaces*, submetido para publicação.

[24] C. J. Smyth, *A Coloring Proof of a Generalisation of Fermat´s Little Theorem*, The American Mathematical Monthly, Vol. 93, No. 6 (Jun.-Jul., 1986), pp. 469-471.

[25] Caroline Laroche Turnage, *Selected Proofs of Fermat's Little Theorem and Wilson Theorem*, Thesis submitted to Wake Forest University, Department of Mathematics, May 2008.