Do Pequeno Teorema de Fermat às Famílias Gerais de Congruências

Cristina Serpa
Universidade de Lisboa
mcserpa@gmail.com

Neste artigo mostra-se como a congruência associada ao Pequeno Teorema de Fermat admite versões muito mais gerais, que se podem demonstrar por métodos de sistemas dinâmicos e de combinatória. Ilustram-se também as contribuições mais importantes para a obtenção destes resultados.

Pierre de Fermat (1601-1665) deu um contributo valioso para o desenvolvimento da matemática. Não deu, no entanto, grande relevância à publicação do seu trabalho, pelo que a maior parte dos resultados a que chegou foram tornados públicos ou através de correspondência que mantinha com outros matemáticos ou pelas suas anotações, que vieram a ser reveladas postumamente. As demonstrações dos seus resultados e conjeturas foram matéria de muito estudo por parte de matemáticos mesmo até aos dias de hoje. De facto, só no final do século XX é que foi provado o seu último teorema, prova essa que envolve ferramentas matemáticas ainda não conhecidas à época de Fermat. Existe, pois, alguma especulação à volta da eventualidade de Fermat não ter conseguido provar os seus resultados ou de que as suas provas não fossem suficientemente rigorosas. O que é facto é que, de uma forma ou de outra, Fermat chegou a resultados surpreendentes e tinha um gosto por fazer conjeturas.

1. O PEQUENO TEOREMA DE FERMAT

De entre as áreas da matemática em que Fermat se empenhou, a teoria dos números terá sido a que mais o envolveu. Foi nesta área que ele descobriu um resultado que ficou conhecido como Pequeno Teorema de Fermat. Apesar de hoje serem conhecidas várias provas, foi necessário quase um século para que fosse conhecida uma prova (através de Euler, em 1736). Apesar disso, terá sido Leibniz a prová-lo em primeiro lugar, num trabalho que não publicou. Este teorema foi escrito numa carta de Fermat para um seu correspondente, Bernhard Frénicle de Bessy, em 1640, na qual referiu que não enviava a demonstração por recear ser demasiado longa (ver [1], [2]).

Teorema 1.1. (Pequeno Teorema de Fermat). *Se p é um número primo e a é um inteiro arbitrário não divisível por p, então p divide $a^{p-1}-1$.*

Este teorema pode ser demonstrado recorrendo a várias técnicas matemáticas e de várias áreas da matemática. Sendo um resultado de teoria de números, a prova mais natural é a que surge da manipulação da divisibilidade de números.

A primeira demonstração publicada é da autoria de Euler (ver [3]).

Demonstração. Do teorema binomial resulta

$$(a+1)^p \equiv a^p + 1 \pmod{p}, \tag{1}$$

pois, de facto,

$$\binom{p}{k} \equiv 0 \pmod{p}, \tag{2}$$

para $0 < k < p$. Subtraindo $a+1$ de ambos os membros da congruência (1),

$$(a+1)^p - (a+1) \equiv a^p - a \pmod{p}. \tag{3}$$

Por indução, verifica-se, em primeiro lugar, que $1^p - 1$ é divisível por p.

Suponha-se que $a^p - a$ é divisível por p. Logo por (3), $(a+1)^p - (a+1)$ é divisível por p. Isto completa a prova por indução de

$$a^p \equiv a \pmod{p}. \tag{4}$$

Assim, multiplicando esta última congruência pelo inverso multiplicativo de a (mod$p$), obtém-se o resultado na forma clássica

$$a^{p-1} \equiv 1 \pmod{p}, \tag{5}$$

onde a e p são primos entre si.

Observação 1.2. Note-se que a formulação (4) é um pouco mais geral do que a original (5), pois neste caso não é necessário que a e p sejam primos entre si, isto é, pode considerar-se um $a \in \mathbb{N}$ qualquer. No entanto, não deixam de ser duas formulações equivalentes, pelo que por vezes o Pequeno Teorema de Fermat é enunciado da forma (4).

Recentemente (2008) foi feita uma demonstração, da autoria de Bishop (ver [3]), que aplica técnicas já conhecidas à época de Fermat, mas que é original no sentido em que ainda não tinha sido dada esta abordagem.

Demonstração. Para a prova de (5) considera-se que p é primo e ímpar, pois para o único primo par a prova é trivial. Seja

$$f(x) = x^{p-1} - 1. \tag{6}$$

Fazendo o desenvolvimento em série de Taylor da função em torno de $x = 1$, obtém-se

$$f(x) = (p-1)(x-1) + \frac{1}{2!}(p-1)(p-2)(x-1)^2 + \\ + \cdots + \frac{1}{(p-1)!}(p-1)!(x-1)^{p-1}. \quad (7)$$

Note-se que esta série pode ser obtida aplicando o teorema binomial à expressão

$$(1 + (x-1))^{p-1} - 1. \quad (8)$$

Considerem-se, agora, os valores de x divisíveis por p. Para estes valores de x, $f(x)$ é igual a um múltiplo de p menos 1, logo não é divisível por p.

Considere-se agora $x = kp + c$, com $c \in \mathbb{Z}$ e $0 < c < p$. Então da equação(6) (mod p), resulta

$$f(kp + c) \equiv f(c) \pmod{p}. \quad (9)$$

Logo, é apenas preciso considerar os valores de x tais que $0 < x < p$.

Agora utiliza-se a indução matemática para provar o teorema. O caso base é $x = 1$.. Note-se que $f(1) = 0$ e por isso é divisível por p. Suponha-se que $f(n)$ é divisível por p, com $0 < n < p-1$, isto é, $n^{p-1} - 1$ é divisível por p. Veja-se que $f(n+1)$ é divisível por p.

Tem-se

$$f(n+1) = (p-1)n + \frac{1}{2!}(p-1)(p-2)n^2 + \\ + \cdots + \frac{1}{(p-1)!}(p-1)!n^{p-1}. \quad (10)$$

Como

$$\binom{p-1}{k} = \frac{(p-1)\cdots(p-k)}{k!} \equiv (-1)^k \pmod{p}, \quad (11)$$

resulta que

$$f(n+1) \equiv -n + n^2 - n^3 + \cdots + (-1)^k \pmod{p}. \quad (12)$$

Então, $f(n+1)$ é congruente com a soma duma progressão geométrica de razão $-n$, o que, utilizando a respetiva fórmula da soma, vem

$$f(n+1) \equiv \frac{-n + n^p}{1+n} \pmod{p}. \quad (13)$$

Fatorizando esta última congruência, obtém-se

$$f(n+1) \equiv \frac{n(-1 + n^{p-1})}{1+n} \pmod{p}. \quad (14)$$

Como $0 < n < p-1$, $1+n$ não é divisível por p. Por hipótese, $n^{p-1} - 1$ é divisível por p, o que prova o resultado por indução.

Não obstante estas demonstrações não oferecerem grande dificuldade, existe uma alternativa muito mais intuitiva e acessível (mesmo a não matemáticos) que advém de contagem de objetos. De facto, foi em 1872 que Petersen (ver [4]) apresentou a demonstração que se transcreve.

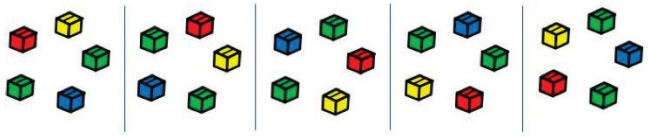

Figura 1: Ilustração da demonstração do Pequeno Teorema de Fermat por contagem de caixas.

Sejam 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. Pelo que, $p | a^p - a$.

Esta demonstração recorre a conceitos que hoje em dia são estudados de forma mais sistemática, com terminologia já estabelecida. Assim, os conceitos envolvidos são colares e palavras formadas por letras de um alfabeto. Aqui os colares representam classes de equivalência (rotações), as palavras representam formas de coloração e as letras são as cores disponíveis na paleta (alfabeto). A noção precisa de colar apareceu explicitamente num artigo de MacMahon em 1892 (ver [5]). Estes objetos matemáticos surgem numa área da matemática relativamente recente, a combinatórica de palavras. Uma contribuição decisiva nesta área veio dos volumes escritos sob o pseudónimo Lothaire, o primeiro dos quais [6] de 1983 e cujo terceiro volume [7] foi publicado em 2005. No entanto, como precursores desta temática estão os trabalhos de investigação de padrões de repetições em palavras feitos por Axel Thue (artigos [8] e [9] de 1906 e 1912). Para mais detalhes na história deste ramo da matemática ver [10].

Recentemente tem sido apresentada uma forma alternativa de demonstração recorrendo a sistemas dinâmicos (ver, por exemplo, [11], [12] e [13]). Em termos esquemáticos, a prova dinâmica é a seguinte.

1. Pierre de Fermat (1601-1665)

2. Leonhard Euler (1707-1783)

3. Julius Petersen (1839-1910)

Demonstração. Considere-se a aplicação $T_a : [0,1] \to [0,1]$ definida por

$$\begin{cases} ax \pmod 1 & \text{se } x \neq 1 \\ 1 & \text{se } x = 1. \end{cases} \tag{15}$$

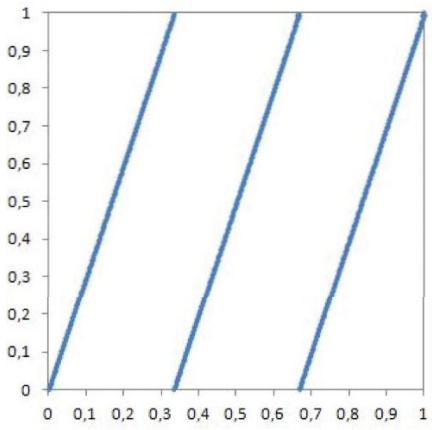

Figura 2: Gráfico da aplicação T_3.

É fácil verificar que sendo a um número inteiro positivo, T_a tem a pontos fixos, por exemplo, por observação do gráfico da aplicação (figura 2).

Também não é difícil mostrar que $\forall a, b \in \mathbb{N}, T_a(T_b) = T_{ab}$, e em especial que $\forall a, n \in \mathbb{N}, T_a^n = T_{a^n}$.

Por outro lado, verifica-se que os pontos periódicos de período p são os pontos fixos de $T_a^p = T_{a^p}$. Daqui resulta que existem exatamente $a^p - a$ pontos periódicos de T_a cujo período mínimo é p. E isto implica que $p \mid (a^p - a)$ como pretendido.

Outra demonstração possível vem da teoria de grupos em álgebra. Fundamentalmente, a ideia é análoga à demonstração acima, no sentido em que a ordem de um elemento de um grupo finito divide a ordem do grupo (ver, por exemplo, [14]).

Em síntese, estas três últimas demonstrações exploram uma forma de contagem de objetos matemáticos que podem ser agrupados em conjuntos de p elementos, onde p é um número primo. Destas três, a prova elaborada por Petersen é a mais trivial e intuitiva possível.

2. GENERALIZAÇÕES

Euler, autor da primeira demonstração do Pequeno Teorema de Fermat, também foi o autor da primeira e mais conhecida generalização, a qual é também usualmente referida como Teorema de Euler (ver, por exemplo, [1] e [15]). Nesse resultado é usada a função de Euler (apresentada por volta de 1760).

Definição 2.1. Chama-se *função* de Euler à função $\phi(m)$ que conta o número de inteiros positivos $\leq m$, que são primos com m, isto é, m.d.c. $(n, m) = 1$.

Teorema 2.2. (Teorema de Euler) *Sejam a, n inteiros tais que m.d.c. $(a, n) = 1$, então*

$$a^{\phi(n)} \equiv 1 \ (mod\ n). \tag{16}$$

Note-se que, no caso particular de n ser primo, (16) é o Pequeno Teorema de Fermat. No entanto, o Teorema de Euler é válido para qualquer inteiro positivo n.

Demonstração (conforme [1]). Primeiro supõe-se que $n = p^k$, com p primo, $p \nmid a$ e $k > 0$ e prova-se, por indução em k, que

$$a^{\phi(p^k)} \equiv 1 \pmod{p^k}. \tag{17}$$

Para $k = 1$, a expressão (17) reduz-se a $a^{\phi(p)} \equiv 1 \pmod{p}$, que é o Pequeno Teorema de Fermat.

Suponha-se que (17) se verifica para certo k. Veja-se que também se verifica para $k+1$.

Por uma propriedade da função de Euler

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

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

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

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

$$a^{\phi\left(p^{k+1}\right)} \equiv 1 \pmod{p^{k+1}} \tag{18}$$

que conclui a prova por indução de (17).

Considere-se m.d.c. $(a,n) = 1$ e a fatorização de n em números primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k}$. Para cada $i \in \{1,2,\ldots,r\}$ aplique-se a congruência (17):

$$a^{\phi\left(p_i^{k_i}\right)} \equiv 1 \pmod{p_i^{k_i}}. \tag{19}$$

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

$$a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}. \tag{20}$$

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

$$a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}} \tag{21}$$

que é o mesmo que (16).

Um grande salto na generalização do Pequeno Teorema de Fermat foi dado por Gauss, que descobriu uma forma de construir congruências quaisquer que sejam os números inteiros positivos a e n. Agora já não é exigido que a e n sejam primos entre si. De acordo com Dickson [16] este resultado foi conhecido 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, para o caso particular de a ser primo. Nos anos 1882 e 1883 foram dadas quatro demonstrações diretas deste resultado por Kantor, Weyr, Lucas e Pellet. Porém, esta forma de apresentação não é nem muito elegante nem muito prática.

Na sua obra magistral *Disquisitiones Arithmeticae*[1], publicada em 1801 (ver [17] e [2]), Gauss é responsável pelo desenvolvimento da linguagem e de notações em teoria de números e, em especial, da álgebra de congruências. Esta obra começa com uma definição:

> Se um número a divide a diferença entre dois números b e c, então diz-se que b e c são congruentes, caso contrário são incongruentes; e a é ele próprio chamado de módulo.

A notação usada por Gauss é a usada nos dias de hoje (neste exemplo, $b \equiv c \pmod{a}$) e possibilitou a construção de uma álgebra com a relação $\equiv$. Nos primeiros capítulos, Gauss introduz uma nova forma de cálculo, a teoria das congruências, que rapidamente ganhou aceitação geral e a sua terminologia foi importante para a atual teoria dos números.

Um dos mais conhecidos alunos de Gauss foi Möbius (ver [18]). Foi seu estudante de astronomia teórica na Universidade de Göttingen. Apesar de os seus principais trabalhos terem sido nas áreas da geometria analítica e da topologia, Möbius deu uma contribuição importante para consolidar a generalização feita por Gauss do Pequeno Teorema de Fermat. De facto, conforme Dickson reporta em [16], foram dois os contributos relevantes (1832): a função de Möbius e a fórmula de inversão de Möbius. A primeira permite escrever o resultado com uma fórmula bastante mais compacta e a segunda foi importante no que se refere à construção de demonstrações que se baseiam na contagem de objetos.

Definição 2.3. Para $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, *a função de Möbius* $\mu(n)$ é definida da seguinte forma:

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

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

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

Observação 2.4. A notação original desta função era a_n.

Teorema 2.5. (Fórmula de inversão de Möbius) *Sejam F e f duas funções aritméticas relacionadas pela fórmula*

$$F(n) = \sum_{d|n} f(d) \tag{22}$$

então,

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d). \tag{23}$$

Com recurso à função de Möbius, o resultado de Gauss pode então ser expresso da forma seguinte (o resultado é válido mesmo que a não seja primo).

Teorema 2.6. Para quaisquer a, n inteiros positivos,

$$\sum_{d|n} \mu(d)\, a^{n/d} \equiv 0 \ (mod\ n). \tag{24}$$

Curiosamente, esta formulação não foi realizada nem por Gauss nem por Möbius, mas sim pelo matemático austríaco Gegenbauer (1900).

A seguir apresenta-se uma demonstração (sugerida pelo Prof. Nuno da Costa Pereira).

Demonstração. Suponha-se, em primeiro lugar, que n é divisível por um único número primo p. Sendo $n = p^\alpha$ temos

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

Sabendo que $\phi\left(p^k\right) = p^k - p^{k-1}$, 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

$$a^{p^\alpha} - a^{p^{\alpha-1}} = a^{p^{\alpha-1}} \left(a^{\phi(p^\alpha)} - 1\right). \tag{25}$$

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

$$a^{p^\alpha} - a^{p^{\alpha-1}} \equiv 0 \pmod{p^\alpha}. \tag{26}$$

Passa-se agora ao caso geral em que n se decompõe num produto de fatores 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 divisor d 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

$$b_d^{p_k^{\alpha_k}} - b_d^{p_k^{\alpha_k-1}} \equiv 0 \pmod{p_k^{\alpha_k}} \tag{27}$$

se $d | n_k$.

É pois

$$\sum_{d|n} \mu(d)\, a^{n/d} \equiv 0 \pmod{p_k^{\alpha_k}} \tag{28}$$

e, portanto, também

$$\sum_{d|n} \mu(d)\, a^{n/d} \equiv 0 \pmod{n} \tag{29}$$

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

Johann Gauss
(1777-1855)

August Möbius
(1790-1868)

Leopold
Gegenbauer
(1849-1903)

[1] Foram feitas traduções em francês em 1807 (Paris) e em inglês em 1966 (Yale University Press)

Outras demonstrações conhecidas desta generalização do Pequeno Teorema de Fermat devida a Gauss-Gegenbauer envolvem a fórmula de inversão de Möbius. A ideia consiste em identificar relações entre funções de contagem de objetos com a propriedade (22). Daí, por (23), obtém-se a determinação explícita da fórmula de contagem da cardinalidade de um conjunto de objetos que, à partida, se sabe que é possível agregar em grupos (ou classes de equivalência) de n elementos. Assim resulta a congruência módulo n. Exemplos de demonstrações deste tipo são as que recorrem aos colares e as que resultam do sistema dinâmico (15).

Este resultado também pode ser apresentado sob uma forma combinatórica. Para isso introduz-se a devida terminologia.

Conforme a notação de J. Matoušek e J. Nešetřil [19] e de acordo com o exposto em [20] tem-se o que se segue.

Definição 2.7. Denota-se por $C_j^{\{1,2,\cdots,k\}}$ o conjunto de todos os subconjuntos de $\{1,2,\cdots,k\}$ com j elementos.

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

Teorema 2.8. *Sejam a e n inteiros positivos cuja fatorização 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,*

$$\sum_{j=0}^{k} \sum_{\delta \in C_j^{\{p_1,p_2,\cdots,p_k\}}} (-1)^{k+j} a^{\frac{n}{P}\delta_1\delta_2\cdots\delta_j} \equiv 0 \ (mod\ n) \qquad (30)$$

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

$$\sum_{d|P} \mu(dP)\, a^{\frac{n}{P}d} \qquad (31)$$

Substituindo d por P/d, obtém-se o seguinte

$$\sum_{d|P} \mu(d)\, a^{\frac{n}{d}}. \qquad (32)$$

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

$$\sum_{d|n} \mu(d)\, a^{\frac{n}{d}}. \qquad (33)$$

Por (24) obtém-se o resultado pretendido.

Exemplo 2.9. Para $n = 105$ tem-se a seguinte congruência, válida para todo o $a \in \mathbb{N}$

$$a^{105} - a^{35} - a^{21} - a^{15} + a^7 + a^5 + a^3 - a \equiv 0 \pmod{105}. \qquad (34)$$

A vantagem desta última formulação é a de fornecer um algoritmo para construção de congruências. Este consiste nos passos:

1. Todas as parcelas têm o fator $a^{n/p}$. Isto corresponde a diminuir em uma unidade o expoente de cada fator 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 fatores primos que foram multiplicados no passo 2. A parcela cujo divisor de P é o próprio P fica com sinal positivo. Com menos um fator primo troca-se o sinal. Por cada fator primo a menos, faz-se uma troca de sinal.

Como nota final é interessante salientar a diversidade de possíveis generalizações do Pequeno Teorema de Fermat. O livro de Dickson [16] sobre a história da teoria de números é bem ilustrativo. Assim, quando o resultado de Gauss-Gegenbauer parece encerrar a questão da generalização do resultado, surgem também generalizações desta última congruência.

Como exemplo de generalização do Teorema de Gauss-Gegenbauer existe um resultado de Axer, publicado em 1911, que inclui somas de polinómios em vez de somas de potências simples (ver [16]).

AGRADECIMENTOS

A autora agradece a contribuição do Prof. Nuno da Costa Pereira, com sugestões de prova relativamente ao resultado de Gauss-Gegenbauer.

REFERÊNCIAS

[1] David M. Burton, *Elementary Number Theory*, sixth edition, McGraw- Hill, 2007.

[2] Oystein Ore, *Number Theory and its History*, McGraw-Hill Book Company, Inc., 1948.

[3] Robert E. Bishop, *On Fermat's Little Theorem*, julho 2008.

[4] 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.

[5] Percy A. MacMahon, "Application of a Theory of Permutations in Circular Procession to the Theory of Numbers", *Proc. London Math. Soc.* 23, 305-313, 1982.

[6] M. Lothaire, *Combinatorics on Words,* Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1977. Corrected reprint of the 1983 original.

[7] M. Lothaire, *Applied Combinatorics on Words*, Cambridge University Press, 2005.

[8] Axel Thue, *Über unendliche Zeichenreihen*, Norske Vid. Selsk. Skr. I Math- Nat. Kl. Chris. 7, 1-22, 1906.

[9] Axel Thue, *Über die gegenseitige Loge gleicher Teile gewisser Zeichenreihen*, Norske Vid. Selsk. Skr. I Math-Nat. Kl. Chris.

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

[11] 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, maio 2000, 422-428.

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

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

[14] Jenny Momkus, *Introductory Group Theory and Fermat's Little Theorem*, preprint, 2011.

[15] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, fifth edition, 1979.

[16] Leonard Eugene Dickson, *History of the Theory of Numbers, Vol. 1: Divi- sibility and primality*, Carnegie Institution of Washington, N.º 256, 1919.

[17] Carl B. Boyer, *A History of Mathematics*, John Wiley & Sons, Inc., 1968.

[18] "August Ferdinand Möbius." *Encyclopædia Britannica. Encyclopædia Britannica Online*, Encyclopædia Britannica Inc., 2012. Web. 21 Mar. 2012.

[19] J. Matoušek e J. Nešetřil, *Invitation to Discrete Mathematics*, second edition, Oxford University Press, 2009.

[20] Cristina Serpa, Jorge Buescu, "A Combinatorial formulation for a congruence of Gauss-Gegenbauer", artigo para publicação.

BIBLIOGRAFIA

W. W. Rouse Ball, "A Short Account of the History of Mathematics", *The Project Gutenberg Ebook* 2010, 4.ªed., 1908.

SOBRE A AUTORA

Cristina Serpa é monitora na Faculdade de Ciências da Universidade de Lisboa e colaboradora do CMAF – Centro de Matemática e Aplicações Fundamentais. É bolseira de doutoramento financiada pela Fundação para a Ciência e Tecnologia.