Alfredo Costa
Universidade
de Coimbra
amgc@mat.uc.pt

A FÓRMULA DE LEGENDRE PARA FATORIAIS

Neste *Canto Délfico*, abordamos a fórmula de Legendre para o cálculo dos expoentes da fatorização em primos de um fatorial, tendo em mente a sua aplicação em problemas de Olimpíadas de Matemática.

1. UM PROBLEMA DAS OPM

O seguinte problema foi proposto na final das XIX Olimpíadas Portuguesas de Matemática (OPM), em 2001, e encontra-se, com solução, num dos volumes de compilações de problemas das OPM feitas por Jorge Picado e Paulo Eduardo Oliveira [7].

Problema 1. *Com quantos zeros consecutivos termina o número*

$$2001! = 2001 \times 2000 \times \cdots \times 3 \times 2 \times 1\ ?$$

O autor deste artigo do *Canto Délfico* também encontrou este problema noutras fontes, e.g. num teste de seleção de talentos das Olimpíadas Sul-Africanas, de 2009 (mas com o número 2009 no enunciado, em vez do número 2001). A fórmula de Legendre que é objeto deste *Canto Délfico* sistematiza a resposta a este tipo de problemas.

Comecemos por escrever uma solução direta do problema das OPM. Para tal é conveniente usarmos a notação $\lfloor x \rfloor$, indicando o chão do número real x, ou seja, o maior inteiro menor ou igual a x. Assim, se a e b são inteiros positivos, o número $\lfloor \frac{a}{b} \rfloor$ é o "número de vezes que b cabe em a", ou seja, é o quociente da divisão inteira de a por b.

Uma resolução do problema. Comecemos por observar que o número de zeros com que 2001! termina é o maior inteiro k tal que 2001! é um múltiplo de 10^k. Tendo em conta a fatorização em primos $10 = 2 \times 5$, somos levados a procurar

Figura 1. Adrien-Marie Legendre (1752-1833).[1]

descobrir qual é o maior inteiro r tal que 5^r divide 2001!.

Note-se que r é o número de vezes em que o fator 5 aparece na fatorização de 2001! em primos (contando repetições). Denotando por r_i o expoente de 5 na fatorização em primos de i para cada $i \in \{1, \ldots, 2001\}$, vemos que

$$r = r_1 + r_2 + \cdots + r_{2001}.$$

Para cada inteiro positivo n, consideremos o conjunto

$$S_n = \{i : r_i \geq n\},$$

que apenas para um número finito de valores de n é não vazio. Usando a notação $|X|$ para a cardinalidade de um conjunto X, observemos que

$$|S_1| + |S_2| + \cdots = r.$$

Ora $|S_n|$ é o número de múltiplos de 5^n que são menores ou iguais a 2001, ou seja,

$$|S_n| = \left\lfloor \frac{2001}{5^n} \right\rfloor.$$

Assim, temos

$$r = \left\lfloor \frac{2001}{5} \right\rfloor + \left\lfloor \frac{2001}{25} \right\rfloor + \left\lfloor \frac{2001}{125} \right\rfloor + \left\lfloor \frac{2001}{625} \right\rfloor$$
$$= 499.$$

Portanto, 2001! é um múltiplo de 5^{499}, mas não de 5^{500}.

Por outro lado, como existem 1000 números pares menores do que 2001, sabemos em particular que 2001! é um múltiplo de 2^{499}. Logo 2001! é um múltiplo de 10^{499}, mas não de 10^{500}. Concluímos que 2001! termina precisamente com 499 zeros. □

Nas linhas seguintes vamos ver uma sistematização do método aplicado nesta resolução.

2. VALORAÇÕES p-ÁDICAS

Dado um primo p e um inteiro não nulo a, denotemos por $v_p(a)$ o expoente de p na fatorização de a em números primos. Por outras palavras, temos

$$v_p(a) = \max\{k \in \mathbb{N} : p^k | a\},$$

onde a notação $x|y$ significa que x divide y (isto é, que y é um múltiplo de x) e onde se considera 0 como elemento de $\mathbb{N}$. Em particular, $v_p(a) = 0$ se e só se p não divide a. A função v_p é por vezes chamada de *valoração p-ádica*. Esta função já foi alvo de atenção nesta coluna da *Gazeta de Matemática*, num artigo sobre o Teorema de Monsky [3].

Exercício 1. *Prove as seguintes propriedades da função v_p, para quaisquer inteiros positivos a, b:*

1. $v_p(ab) = v_p(a) + v_p(b)$.
2. $\min\{v_p(a), v_p(b)\} \leq v_p(a+b)$; se $v_p(a) < v_p(b)$, então $v_p(a) = v_p(a+b)$.
3. $v_p(m.d.c.(a_1, a_2, \ldots, a_n))$ $= \min\{v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\}$
4. $v_p(m.m.c.(a_1, a_2, \ldots, a_n))$ $= \max\{v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\}$.

Se adotarmos a definição razoável de que $v_p(0) = \infty$, com a convenção de que $\infty > x$ e $\infty + x = \infty = x + \infty$ para qualquer número real x, vemos que as propriedades 1 e 2 do exercício anterior se estendem para quaisquer inteiros a, b.

3. A FÓRMULA DE LEGENDRE

A função de Legendre associada ao primo p é a função e_p definida por $e_p(n) = v_p(n!)$, onde n é um número natural. Replicando o argumento usado na secção anterior na resolução do problema das OPM aí apresentado, deduz-se a seguinte Fórmula de Legendre.

Teorema 1. (Fórmula de Legendre). *Para qualquer primo p e para qualquer inteiro positivo n, temos*

$$e_p(n) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Esta fórmula está associada a Adrien-Marie Legendre (1752-1833), devido ao estudo que este dela fez na sua obra *Essai sur la théorie des nombres* [5]. O leitor provavelmente ficará mais bem-impressionado com a elegância do enunciado e a prova da fórmula alternativa para $e_p(n)$, que apresentaremos na secção seguinte, e que Legendre obteve no mesmo livro.

Entretanto, façamos uma pausa para mencionar uma surpreendente curiosidade sobre a figura de Legendre, em que estamos a usar a palavra "figura" num sentido bastante literal. A figura 2 contém a única verdadeira imagem conhecida de Adrien-Marie Legendre. Trata-se de uma caricatura de Legendre e de Fourier, que foi descoberta pela comunidade matemática apenas em 2008. A ampliação na figura 1 foca-se no rosto do primeiro destes dois ilustres matemáticos franceses. Durante mais de um século, até 2005, o matemático Legendre era identificado erradamente, e em livros reputados, com a imagem na figura 3, que sabemos agora retratar o político, seu contemporâneo, Louis Legendre. A interessante história em torno desta confusão e do seu esclarecimento mereceu destaque num número das *Notices of the American Mathematical Society* [4], tendo por capa a referida caricatura.

[1] Ampliação de uma porção da imagem na figura 2.

Figura 2. Caricatura de Adrien-Marie Legendre (esquerda) e Joseph Fourier (direita), da autoria de Julien-Léopold Boilly.[2]

Figura 3. Louis Legendre (1752-1797).[3]

4. VARIANTE DA FÓRMULA

Explorando a igualdade

$$(x-1)(1+x+x^2+x^3+\cdots+x^k)=x^{k+1}-1,$$

válida para quaisquer $x \in \mathbb{R}$ e $k \in \mathbb{N}$, prova-se que a fórmula de Legendre admite a seguinte variante:

Teorema 2. *(Fórmula de Legendre – versão alternativa). Para qualquer primo p e para qualquer inteiro positivo n, seja $S_p(n)$ a soma dos dígitos da expansão de n na base p. Então temos*

$$e_p(n)=\frac{n-S_p(n)}{p-1}.$$

Demonstração. A expansão de n na base p consiste na única decomposição

$$n=a_0+a_1p+\cdots+a_kp^k$$

em que $a_k \neq 0$ e $a_i \in \{0,\ldots,p-1\}$ para qualquer $i \in \{0,\ldots,k\}$. Observemos que

$$\left\lfloor \frac{n}{p^i} \right\rfloor = a_i+a_{i+1}p+\cdots+a_kp^{k-i}$$

para qualquer $i \in \{0,\ldots,k\}$. Atentando no somatório

$$\sum_{i=1}^{k}\left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{k}(a_i+a_{i+1}p+\cdots+a_kp^{k-i})$$

e aí associando, para cada $j \in \{1,\ldots,k\}$, as parcelas da forma $a^j p^r$, obtemos a seguinte cadeia de igualdades:

$$\begin{aligned}(p-1)e_p(n) &= (p-1)\sum_{i=1}^{k}\left\lfloor \frac{n}{p^i} \right\rfloor \\ &= (p-1)\sum_{i=1}^{k}a_i(1+p+\cdots+p^{i-1}) \\ &= \sum_{i=1}^{k}a_i(p^i-1) \\ &= \sum_{i=1}^{k}a_i(p^i-1)+a_0(p^0-1) \\ &= \sum_{i=0}^{k}a_i(p^i-1) \\ &= \sum_{i=0}^{k}a_ip^i-\sum_{i=0}^{k}a_i = n-S_p(n).\end{aligned}$$

Portanto, temos $e_p(n)=\dfrac{n-S_p(n)}{p-1}$.

□

5. EXERCÍCIOS

O leitor pode apreciar a fórmula de Legendre (na formulação que lhe for conveniente) ao resolver os seguintes exercícios.

Exercício 2. *Seja p um primo. Determine o expoente de p na fatorização de $(p^m)!$ em números primos.*

Exercício 3. *Determine todos os inteiros positivos n tais que $n!$ termina em exatamente 1000 zeros.*

Exercício 4. *Mostre que 2^n não divide $n!$, para qualquer inteiro positivo n, e determine todos os inteiros positivos n tais que 2^{n-1} divide $n!$.*

Estes exercícios são exemplos típicos de problemas de matemática olímpica que se atacam facilmente com a fórmula de Legendre. Eles aparecem com solução, por exemplo, num livro de Andreescu e Andrica de introdução à Teoria dos Números na perspetiva da preparação para Olimpíadas de Matemática [2].

6. MAIS PROBLEMAS OLÍMPICOS

Convidamos agora o leitor a ter a satisfação de resolver um problema das Olimpíadas Internacionais de Matemática (OIM). Com efeito, o seguinte problema das OIM de 1972 resolve-se de modo natural com o auxílio da fórmula de Legendre.

Problema 2. *Mostre que, para quaisquer inteiros positivos m, n, o número*

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

também é um inteiro.

O livro de Andreescu e Andrica também inclui uma solução do problema [2]. Este problema serve como exemplo da utilidade da seguinte estratégia para provar que um inteiro a divide um inteiro b: aproveitar o facto de que a divide b se e só se $v_p(a) \leq v_p(b)$ para qualquer primo p.

A dificuldade dos problemas das OIM aumentou dramaticamente desde os primórdios desta prestigiada competição internacional anual para adolescentes, iniciada em 1959. O contraste entre o problema anterior e o seguinte, das OIM de 2019, é eloquente, sendo este exemplo escolhido por também se recorrer à fórmula de Legendre na solução oficial. Esta está disponível, por exemplo, na página *web* da OIM 2019 [1].

Problema 3. *Determine todos os pares de inteiros positivos (k,n) tais que*

$$k! = (2^n-1)(2^n-2)(2^n-4)\cdots(2^n-2^{n-1}).$$

O seguinte problema surgiu num teste de seleção da equipa romena para a OIM de 2010, podendo a sua solução, onde a fórmula de Legendre é aplicada, ser encontrada no texto de Mihet [6]. Sejam n, q inteiros positivos tais que todos os divisores primos de q são maiores do que n. Mostre que $n!$ divide o produto $(q-1)(q^2-1)\cdots(q^{n-1}-1)$.

O leitor com alguns conhecimentos elementares de Teoria dos Números, dentre os que são normalmente usados na matemática olímpica, pode preferir começar por atacar este último problema antes de abordar o problema da OIM de 2019...

REFERÊNCIAS

[1] *https://www.imo2019.uk/wp-content/uploads/2018/07/solutions-r856.pdf.*

[2] Titu Andreescu and Dorin Andrica. *Number Theory. Structures, Examples, and Problems*. Birkhäuser Boston, Ltd., Boston, MA, 2009.

[3] Alfredo Costa. "O Teorema de Monsky". *Gazeta de Matemática*, (195):11-16, 2021.

[4] Peter Duren. "Changing Faces: the Mistaken Portrait of Legendre". *Notices Amer. Math. Soc.*, 56(11):1440-1443, 2009.

[5] Adrien-Marie Legendre. *Essai sur la théorie des nombres*. Cambridge Library Collection. Cambridge University Press, Cambridge, 2009. Reprint of the second (1808) edition.

[6] Dorel Mihet. "Legendre's and Kummer's Theorems Again." *Resonance*, 15:1111-1121, 2010.

[7] Jorge Picado, Paulo Eduardo Oliveira, e Sociedade Portuguesa de Matemática. *Olimpíadas de Matemática*, volume 2. Texto Editores, 2007.

[2] Imagem do domínio público, via Wikimedia Commons, *https://commons.wikimedia.org/wiki/File:Legendre_and_Fourier_(1820).jpg*

[3] Imagem do domínio público, via Wikimedia Commons, *https://upload.wikimedia.org/wikipedia/commons/d/db/Louis_Legendre.jpg*