José Carlos Santos
Universidade
do Porto
jcsantos@fc.up.pt

COMPUTAÇÃO DISTRIBUÍDA E MATEMÁTICA

Sabe como é que o seu computador pode ser empregue para resolver problemas matemáticos em aberto?

INTRODUÇÃO

Uma questão natural para uma rubrica chamada *Apanhados na Rede* é a de saber de que modo é que a Internet interfere com a investigação em matemática. Será que interfere de algum modo? A resposta é afirmativa e, de facto, a interação da Internet com a investigação em matemática dá-se a vários níveis. Eis alguns exemplos:

1. Um grande número de revistas científicas tem os seus artigos acessíveis *online*.
2. A Internet facilita a colaboração entre matemáticos situados fisicamente longe uns dos outros.[1]
3. A Internet permite a utilização de *software* computacional, tanto através de instalação local desse *software* como através do uso diretamente pela Internet.[2]

O tipo de interferência da Internet com a investigação em matemática que vai aqui ser abordada é de outra natureza e tem a ver com computação distribuída, ou seja, com o uso de um grande número de computadores, em muitos casos distribuídos por todo o mundo, para efetuar cálculos que levariam demasiado tempo se fossem feitos por um único computador.

SETI

Um dos mais antigos projetos do género, e talvez o mais famoso de todos, é o SETI@home. SETI são as iniciais de *Search for Extra-Terrestrial Intelligence*, ou seja, Busca de Inteligência Extraterrestre. Foi lançado em maio de 1999 e destina-se, como o nome indica, à busca de sinais de vida inteligente no Universo. Quem quiser participar no projeto, tudo o que tem de fazer é ir à respetiva página de Internet[3], descarregar o *software* e fazer assim com que o seu computador use o seu tempo livre para ajudar a analisar sinais vindos do espaço a ver se contêm vestígios de vida inteligente. Na figura 1 pode-se ver o aspeto de um *screensaver* que vem com o programa em questão.

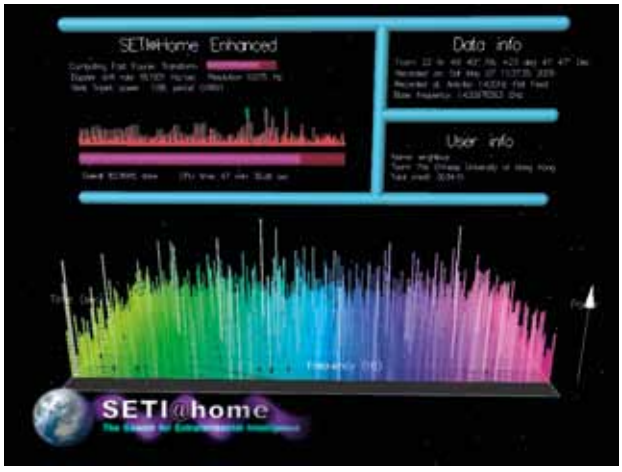

Figura 1. Screensaver do SETI@home

De facto, a busca de vestígios de vida inteligente no Universo não foi o único objetivo da criação deste

projeto. Outro objetivo foi testar a viabilidade de um projeto desta natureza. Constatou-se que era viável e muitos outros projetos semelhantes surgiram.[4] No resto deste artigo, iremos focar-nos nos projetos ligados à matemática.

PRIMOS DE MERSENNE

No século XVII, Marin Mersenne observou que se n for um número natural composto, então $2^n - 1$ também é composto. Com efeito, se $n = pq$, com $1 < p, q < n$,então

$$\begin{aligned} 2^n - 1 &= (2^p)^q - 1^q \\ &= (2^p - 1)(2^{(q-1)p} + 2^{(q-2)p} + \cdots + 2^p + 1), \end{aligned}$$

pelo que $2^n - 1$ é composto. Como, obviamente, $2^1 - 1$ não é primo, resulta desta observação que só quando p for um número primo é que $2^p - 1$ poderá ser primo. Mas será que todos os números desta forma são primos? A resposta é negativa, pois, embora $2^2 - 1(= 3)$, $2^3 - 1(= 7)$, $2^5 - 1(= 31)$ e $2^7 - 1(= 127)$ sejam todos primos, $2^{11} - 1(= 2047)$ é composto, pois é igual a 23×89.

Os números primos da forma $2^p - 1$ designam-se por *primos de Mersenne*. Por vezes, surge uma notícia a dizer que foi descoberto um número primo maior do que qualquer outro número primo conhecido (o recordista atual, descoberto em 2013,[5] é $2^{57.885.161} - 1$, um primo de Mersenne). De facto, há mais de 20 anos que o maior primo conhecido é sempre um primo de Mersenne. Aliás, os dez maiores números primos conhecidos são todos primos de Mersenne. Isto é assim por causa da existência do teste de Lucas-Lehmer, um teste de primalidade feito especificamente para os números de forma $2^p - 1$.

Em 1996 foi lançado o GIMPS (Great Internet Mersenne Prime Search),[6] um projeto de computação distribuída que se destina a descobrir novos primos de Mersenne. Ao todo, conhecem-se atualmente 48 primos de Mersenne, sendo o quadragésimo oitavo o recordista acima referido. A partir do trigésimo quinto (inclusive), foram todos descobertos no âmbito do projeto GIMPS.

Figura 2. Marin Mersenne.

Figura 3. Pierre de Fermat.

PRIMOS DE FERMAT

Pierre de Fermat, que era contemporâneo de Mersenne e que se correspondia com ele, acreditou ter conseguido provar que todos os números da forma $2^{2^n} + 1$ (com $n \in \{0, 1, 2, \ldots\}$) são primos. De facto, isto é verdade para $n \in \{0, 1, 2, 3, 4\}$, mas, no século XVIII, Euler provou que $2^{2^5} + 1$ é múltiplo de 641. Não se conhece mais nenhum número primo da forma $2^{2^n} + 1$para além dos cinco números já referidos. Hoje em dia sabe-se que todos os números da forma $2^{2^n} + 1$ com $5 \leq n \leq 33$ são compostos.

O projeto *Distributed Search for Fermat Number Divisors*[7] destina-se à busca de divisores dos números da forma $2^{2^n} + 1$. Pode provar-se que um tal divisor é necessariamente da forma $k \times 2^m + 1$, com $m \geq n + 2$ (por exemplo, $641 = 5 \times 2^7 + 1$) e este facto, como é natural, ajuda a limitar a busca de novos divisores.

SOMAS DE POTÊNCIAS

Euler conhecia o enunciado do Último Teorema de Fermat: uma potência de grau superior a 2 nunca é soma de duas potências com esse mesmo grau.[8] Embora não tivesse conseguido provar este teorema (isso só seria feito no fim do século XX por Andrew Wiles), Euler conjeturou que, mais geralmente, uma potência de grau n só

---

[1] Um exemplo notável de uma tal colaboração reside no projeto Polymath 8. Em 2013, Yitang Zhang provou que a diferença entre dois números primos consecutivos é menor ou igual a 70.000.000 numa infinidade de casos. Graças ao projeto em questão, este número desceu para 246; veja-se *http://www.ams.org/notices/201506/rnoti-p660.pdf.*

[2] Veja-se, por exemplo o Wolfram|Alpha: *http://www.wolframalpha.com.*

[3] *http://setiathome.ssl.berkeley.edu/*

[4] Veja-se *http://www.distributedcomputing.info*, por exemplo

[5] Veja-se *http://www.mersenne.org/primes/?press=M57885161*

[6] *http://www.mersenne.org*

[7] *http://www.fermatsearch.org*

[8] Neste contexto, "potência" é um número natural elevado a outro número natural.

[9] *http://euler.free.fr/*

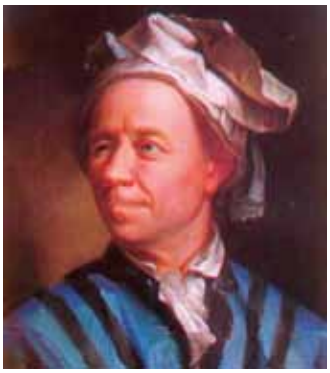
Figura 4. Leonhard Euler.

pode escrever-se como soma de k potências de grau n (com $k > 1$) quando $k \geq n$. Por outras palavras, quando um cubo se pode escrever como soma de vários cubos, são necessários pelo menos três cubos (e, neste caso, a conjetura de Euler não afirma mais do que afirma o Último Teorema de Fermat), quando uma quarta potência pode escrever-se como soma de várias quartas potências, são necessárias pelo menos quatro quartas potências, e assim sucessivamente.

Em 1966, descobriu-se (recorrendo-se a um computador) que a conjetura é falsa, pois

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5. \qquad (1)$$

Vinte anos mais tarde, descobriu-se que a conjetura também é falsa para o expoente 4. Por exemplo,

$$95.800^4 + 217.519^4 + 414.560^4 = 422.481^4.$$

Para estudar este tipo de fenómenos, existe o projeto *Computing Minimal Equal Sums of Like Powers*.[9] Como o nome indica, o projeto é mais geral do que somente procurar contraexemplos da conjetura de Euler. Destina-se também a testar uma conjetura formulada por três matemáticos, L. J. Lander, T. R. Parkin e J. Selfridge (dos quais os dois primeiros foram quem descobriu o exemplo (1), que afirma que, dado um expoente k, se um número natural α puder exprimir-se como soma de m potências de grau k e também puder exprimir-se como soma de n potências de grau k, então $m + n \geq k$ (a menos que $m = n$ e que as duas maneiras de exprimir α como soma de potências de grau k coincidam). A conjetura continua em aberto. Assim, por exemplo, segundo esta conjetura, nenhum número natural pode ser expresso como soma de duas quintas potências de duas maneiras diferentes (pois $2 + 2 \ngeq 5$). Mas a conjetura é compatível com a existência de um número natural que possa ser escrito como soma de duas quintas potências e que também possa ser escrito como soma de três quintas potências. E, de facto,

$$14.132^5 + 220^5 = 14.068^5 + 6.237^5 + 5.027^5.$$

CONCLUSÃO

Há muitos outros projetos de computação distribuída em matemática além destes.[10] Qualquer leitor com um computador pode juntar-se a um deles. E, quem sabe, ajudar a resolver um problema em aberto.

[10] Veja-se em *http://www.distributedcomputing.info/ap-math.html* uma lista de projetos de computação distribuída na área da Matemática.