Manuel Silva
Universidade Nova de Lisboa
mnas@fct.unl.pt

Pedro J. Freitas
Universidade de Lisboa
pedro@ptmat.fc.ul.pt

A **ESTRUTURA** DOS **NÚMEROS PRIMOS**

It is evident that the primes are randomly distributed but, unfortunately, we don't know what 'random' means. R. C. Vaughan (1990)

É evidente que os primos se distribuem de forma aleatória, mas infelizmente não sabemos o que é que "aleatório" significa.

UM POUCO DE HISTÓRIA

Hoje voltamos a falar sobre os números primos. O seu estudo interessa aos matemáticos como objeto em si, mas também porque na tentativa de os compreender têm também surgido novas e fecundas teorias.

Historicamente, o primeiro resultado conhecido sobre a estrutura do conjunto dos números primos aparece nos *Elementos* de Euclides (300 a.C.) e diz-nos que estes nunca acabam, i.e., existem infinitos números primos. Euclides demonstrou ainda que todo o número natural admite uma decomposição única como produto de primos. Por exemplo, $2013 = 3 \times 11 \times 61$, não existindo um outro produto de números primos cujo resultado seja 2013. Podemos assim dizer que os primos são os blocos a partir dos quais todos os números podem ser construídos.

Foi preciso esperar cerca de 2000 anos para que um novo resultado importante acerca da distribuicão dos números primos fosse conhecido.

Teorema 1 (Dirichlet, 1837). *Dados inteiros a e b primos entre si, existem infinitos primos na progressão aritmética*

$$\{an + b : n \in \mathbb{N}\}.$$

Assim, por exemplo, existem infinitos primos p tais que $p = 3n + 1$, ou seja, quando divididos por 3 deixam resto 1. Existem também infinitos primos cujo resto da divisão por 3 dá 2. Entre os 3 restos possíveis na divisão por 3 (0, 1 e 2), podemos mostrar que a probabilidade de o resto dar 1 é $1/2$ e a probabilidade de o resto dar 2 é também $1/2$.

Gauss (1777-1855) conjeturou um resultado estatístico sobre a distribuição dos primos: a densidade dos números primos no intervalo $[0, x]$ deveria ser assimptoticamente $\frac{x}{\log x}$. Este resultado foi demonstrado por Hadamard e La Vallée-Poussin (1896) usando métodos analíticos (variável complexa), e mais tarde de modo *elementar* por Selberg e Erdös (1946). A importância de uma demonstração elementar, no sentido de mais direta, é que esta traz consigo uma compreensão mais profunda.

PRIMOS AO ACASO

Os especialistas em teoria dos números acreditam que os números primos se comportam de modo aleatório. Obviamente que não podemos esperar que algures na sequência dos primos apareça um número par maior do que 2. O teorema

de Dirichlet referido acima diz-nos que não havendo nenhuma obstrução óbvia tal como esta, todas as progressões $\{an+b : n \in \mathbb{N}\}$ contêm infinitos números primos, sendo a sua densidade na verdade a esperada para uma sequência aleatória com a mesma densidade dos primos. Podemos dizer que existem propriedades como a de ser um 'número par' que são incompatíveis com ser primo. Por outro lado, muitas outras propriedades naturais são satisfeitas pelos primos como se estes tivessem sido escolhidos ao acaso, respeitando a densidade notada por Gauss.

Será por isso de alguma forma razoável esperar que na sequência dos números primos surjam todo o tipo de estruturas que possamos imaginar. E no entanto, muito poucos resultados sobre padrões de números primos são conhecidos. Não faltando conjeturas plausíveis para desafiar os matemáticos mais corajosos.

Sabemos, por exemplo, que existe necessariamente um número primo em qualquer intervalo $[n, 2n]$ onde n é um número natural. Este resultado foi demonstrado pelo matemático Chebyshev em 1852. Mas não sabemos, por exemplo, se existem infinitos primos da forma n^2+1. Podemos formular questões análogas para qualquer outro polinómio irredutível. Outra questão do mesmo tipo que permanece em aberto é a de saber se existem infinitos pares de primos (pares de Sophie Germain) da forma $(n, 2n+1)$, como por exemplo: 2 e 5; 3 e 7; 5 e 11; 11 e 23; 23 e 47; 29 e 59; 41 e 83.

Não é fácil decidir *a priori* quais as questões matemáticas mais naturais ou fecundas, e por isso dignas de maior atenção. Uma dificuldade do mesmo tipo encontramos nós próprios na escolha que precisamos constantemente de fazer das nossas prioridades. Qual a importância, por exemplo, de saber se existem ou não infinitos pares de primos que distam duas unidades p, $p+2$ (primos gémeos)? Alguns matemáticos chegaram mesmo a dizer com certa maldade que os primos serviam para multiplicar e não para somar. A questão dos primos gémeos seria por isso uma questão artificial e desprovida de interesse. Os resultados recentes obtidos na direção da conjetura dos primos gémeos permitem-nos perceber que se trata na verdade de uma questão natural e importante.

PRIMOS E BEM PRÓXIMOS

Em abril 2013, Yitang Zhang demonstrou que existem infinitos pares de primos que distam no máximo uma dada constante fixa L. A conjetura dos primos gémeos seria equivalente a reduzir o valor para $L = 2$. O valor obtido por Zhang foi $L = 70\,000\,000$. Para tal, Zhang obteve uma nova estimativa para o número de primos em progressões aritméticas com poucos elementos. Em novembro de 2013, motivado pelo surpreendente resultado de Zhang, James Maynard reduziu o valor de L para $L = 600$. Maynard generalizou ainda o resultado de Zhang para k-tuplos de primos. Denotaremos por $p_1, p_2, \cdots$ a sequência dos números primos.

Teorema 2. *Dado $m \in \mathbb{N}$, tem-se*

$$\liminf_n (p_{n+m} - p_n) \ll m^3 e^{4m}.$$

Este resultado diz-nos, por exemplo, que existem infinitos intervalos de comprimento fixo $C = C(k)$ (constante depende apenas de k) contendo, pelo menos, k primos. Isto significa que podemos não só encontrar infinitos pares de primos relativamente próximos (distância não superior a 600), como também que existem k-tuplos de primos não muitos afastados uns dos outros. Os argumentos de Maynard têm ainda a vantagem de ser mais simples, por não usarem resultados da distribuição dos primos em progressão aritmética nem o teorema de Bombieri-Vinogradov, por exemplo.

James Maynard obteve recentemente o seu doutoramento em Oxford (2013). O resultado obtido, ainda mais numa fase inicial da carreira científica, foi surpreendente para os especialistas na área.

O teorema de Maynard foi obtido independentemente pelo omnipresente Terence Tao, usando o mesmo tipo de argumentos. Este fenómeno de obtenção simultânea de progressos científicos é relativamente comum em matemática. De alguma forma, cada momento histórico está preparado para atacar certo tipo de problemas. O desenvolvimento da Física no ínicio do século XX criou condições para o aparecimento de um Einstein.

Foram já obtidos alguns resultados novos como consequência do trabalho de Maynard. Granville mostrou por exemplo que, dados dois inteiros positivos a e b primos entre si e $m > 1$, existem m primos consecutivos $p_n, p_{n+1}, \cdots, p_{n+m-1}$ congruentes com a módulo m (os restos da divisão destes primos quando divididos por b são todos iguais a a). Segundo Granville é também possível demonstrar uma antiga conjetura de Erdös e Turán relacionada com a distância entre dois primos consecutivos $d_n = p_{n+1} - p_n$. Este novo resultado de estrutura

para os primos diz-nos que existem sequências crescentes com um número arbitrário de elementos $d_n < d_{n+1} < \cdots < d_{n+m}$, e também sequências decrescentes $d_n > d_{n+1} > \cdots > d_{n+m}$, ou seja, k-tuplos de primos progressivamente mais próximos e outros progressivamente mais afastados.

Podemos tentar adivinhar qual será o próximo resultado obtido sobre a estrutura dos números primos. Um candidato plausível pode ser uma conjetura formulada por Dickson em 1904, a qual afirma que dados certos conjuntos finitos $S = \{a_1, a_2, \cdots, a_k\} \subset \mathbb{N}$ ditos *admissíveis* existem infinitos valores de n tais que $n + a_1, n + a_2, \cdots, n + a_k$ são todos primos.

Em matemática, e em especial na teoria dos números, quando algum problema importante é resolvido, quase sempre a sua resolução nos sugere novas questões cuja resposta nos escapa. Não parece fazer sentido imaginar um matemático no futuro possuidor de uma *teoria final* para os números primos, capaz de responder a todas as questões que lhe fossem propostas. Os primos são e serão sempre uma fonte inesgotável com novos e importantes desafios. Se fosse possível viajar no tempo e fazer uma pergunta ao matemático futuro (no ano 3000, por exemplo), em vez de lhe perguntar como se demonstra a conjetura dos primos gémeos (fácil para ele certamente), melhor seria perguntar quais eram as grandes questões em aberto do seu tempo relacionadas com os números primos.

REFERÊNCIAS

[1] D. A. Goldston, J. Pintz, and C. Y. Yildirim. "Primes in tuples. I." *Ann. of Math.* (2), 170(2), 819–862, 2009.

[2] J. Maynard, "Small gaps between primes". (Preprint) arXiv:1311.4600, 23pp., 2013.

[3] Polymath, D. H. J. "A new bound for gaps between primes". (Preprint)

[4] Y. Zhang, "Bounded gaps between primes". Aceite para publicação em *Ann. of Math.*

[5] Erica Klarreich, "Together and alone, closing the prime gap", *Quanta Magazine.* Diponível online em *www.simonsfoundation.org/quanta/20131119-together-and-alone-closing-the--prime-gap*