PRIMOS QUE EVITAM DÍGITOS

Pedro J. Freitas
Universidade de Lisboa
pjfreitas@fc.ul.pt

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

O matemático inglês James Maynard mostrou recentemente que existem infinitos números primos que na sua expansão decimal evitam um dígito à escolha. Existem, por exemplo, infinitos primos que evitam o dígito 7!

1. INTRODUÇÃO

Os números primos são os inteiros positivos que têm exatamente dois divisores. Sabemos da importância do estudo dos primos, a qual resulta em parte do facto de todo o número natural poder ser escrito, de modo único, como produto de fatores primos. Euclides demonstrou que os números primos nunca se esgotam, existem primos tão grandes como se queira, ou seja, o conjunto dos números primos é infinito. A noção de número primo é tão natural que deve sido descoberta ainda antes do período clássico grego.

Até ao século XVII pouco ou nada se acrescentou ao estudo dos números primos. Pierre de Fermat, Carl Friedrich Gauss, Pafnuty Chebyshev e Bernhard Riemann fizeram do estudo dos números primos um problema central da matemática. Em particular, a distribuição dos números primos está relacionada com uma famosa conjetura de Riemann sobre a localização dos zeros de uma certa função zeta.

Nos últimos anos têm surgido diversos resultados novos sobre a estrutura dos números primos. Podemos afirmar que esta é uma época áurea para os números primos! Claro que temos de começar por formular as questões mais simples e avançar passo a passo. A maioria dos problemas permanece naturalmente ainda sem resposta, o comportamento selvagem dos números primos resiste teimosamente às nossas tentativas de domesticação.

2. PRIMOS COM PROPRIEDADES ESTRANHAS

Recordemos que uma capicua, ou número palíndromo, é um número inteiro que coincide com o seu reverso, i.e., pode ser lido da mesma forma da esquerda para a direita ou da direita para a esquerda. A noção de palíndromo depende naturalmente da base em que escrevemos o número, para simplificar a discussão vamos considerar quase sempre a base 10. Haverá alguma relação entre capicuas e números primos? A maioria dos números primos não é certamente uma capicua, do mesmo modo que, a maioria das capicuas nao é número primo. Podemos mesmo afirmar que todas as capicuas com um número par de dígitos são múltiplos de 11. A procura restringe-se às capicuas com um número ímpar de dígitos. Ser um número primo e ser uma capicua são dois conceitos completamente distintos e sem qualquer relação aparente.

Se eu decidir gostar muito de números primos e de capicuas, então gostaria certamente de encontrar capicuas que fossem também números primos. A lista dos números primos que são simultaneamente capicuas começa assim:

$$2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353,$$
$$373, 383, 727, 757, 787, 797, 919, 929\ldots$$

Será que existem infinitos números primos palíndromos na base 10? E na base 2? O nosso conhecimento atual não nos permite ainda responder a estas questões. Podemos duvidar do interesse em saber se existem números primos que satisfazem estas, ou outras, estranhas propriedades. O objetivo central é sempre perceber um pouco mais da subtil estrutura subjacente aos números primos, da qual sabemos ainda tão pouco. Para saber é preciso fazer perguntas, por mais inúteis que estas possam parecer inicialmente.

Existem números primos com outras propriedades igualmente estranhas. Por exemplo, existem primos cuja expansão decimal contém apenas uns 11 e 1111111111111111111 (19 dígitos) são exemplos de números primos contendo apenas o dígito 1. Para produzir um número primo deste tipo, devemos usar o dígito 1 exatamente: 2, 19, 23, 317, 1031, 49081, 86453, 109297 ou 270343 vezes (*https://oeis.org/A004023*). Esta lista está certamente incompleta e ninguém sabe se a sequência é infinita. Sabemos apenas que o número de dígitos tem de ser ele próprio um número primo. Caso contrário, encontramos facilmente pelo menos, um fator próprio, por exemplo: $111111111 = 1001001 \times 111$. Mais uma vez, não parecem existir ferramentas adequadas para abordar este tipo de problema, que também pode ser formulado numa base qualquer diferente da base 10.

Em vez de repetir sempre o mesmo dígito, talvez seja possível, em alternativa, excluir um determinado dígito na expansão decimal dos números primos. O matemático inglês James Maynard mostrou recentemente que existem infinitos números primos que na sua expansão decimal evitam um dígito à escolha. Existem, por exemplo, infinitos primos que evitam o dígito 7! Um resultado fantástico para quem não gosta do dígito 7 e adora números primos. James Maynard tem apenas 29 anos e tem colecionado prémios nos últimos anos: SASTRA Ramanujan (2014), Whitehead (2015) e European Mathematical Society (2016).

O resultado anterior aparece num *preprint* intitulado *Primes with restricted digits* que apareceu em abril deste ano e que tem a extensão de 44 páginas. A descrição de como podem tantos primos evitar um certo dígito envolve diversas ferramentas, é uma combinação do método do círculo de Hardy-Littlewood, do crivo de Harman (variante moderna do crivo de Eratóstenes), resultados de Geometria dos Números, técnicas de Análise de Fourier e ainda a comparação com um processo de Markov! O equivalente a uma verdadeira prova de decatlo matemático, com a dificuldade extra de todas estas técnicas terem de se ajustar entre si.

O teorema demonstrado por Maynard é bastante mais geral do que o enunciado anteriormente. Na verdade, o resultado é válido para outras bases diferentes da base 10. Podemos também excluir dois ou mais dígitos, em vez de apenas um, desde que a base considerada seja suficientemente grande. Do ponto de vista matemático, não existe nada de especialmente interessante na base 10. Fica certamente mais divertido enunciar o resultado para a representação decimal que usamos habitualmente.

Existem outros exemplos de problemas famosos em Teoria dos Números nos quais se pretende mostrar a existência de um número infinito de primos em conjuntos pouco densos. Aqui é importante saber que existem conjuntos infinitos mais gordos e mais magros. Por exemplo, os seguintes quatro conjuntos são progressivamente mais densos: as potências de 2, os quadrados perfeitos, os números primos e o conjunto dos múltiplos de 13. Isto quer dizer que num dado intervalo $[1, n]$, a partir de certo valor de n existem, por exemplo, mais primos do que quadrados perfeitos. A probabilidade de encontrar um número primo é (muito) maior do que a de encontrar um quadrado perfeito. Podemos dizer que os números primos constituem um conjunto mais denso do que os quadrados perfeitos. De modo mais preciso, existem assintoticamente

$$\frac{n}{\ln(n)}$$

primos entre os primeiros n naturais e apenas $\sqrt{n}$ quadrados perfeitos.

Johann Dirichlet demonstrou em 1837 que existiam infinitos números primos em qualquer progressão aritmética infinita: $\{an + b : n \in \mathbb{N}\}$, com a e b primos entre si. Habitualmente, nos resultados onde se demonstra a existência de um número infinito de primos em conjuntos fixados, esses conjuntos são densos ou possuem algum tipo de estrutura aditiva ou multiplicativa. As progressões aritméticas possuem estrutura aditiva e os números primos possuem estrutura multiplicativa. O conjunto dos números inteiros que evitam algum dígito é um exemplo de um conjunto esparso (pouco denso) e sem nenhum dos dois tipos de estrutura aritmética referida. A importância do resultado mais recente de Maynard reside em ter sido obtido neste contexto adverso e novo. Certamente outros resultados acerca da estrutura dos números primos irão seguir-se a este num futuro próximo.

Mas será que existem assim tão poucos números que evitam o dígito 7? Se escolhermos um número natural ao acaso, digamos com 100 dígitos, ele irá com forte probabilidade conter o dígito 7 na sua expansão decimal, certo? Não é, por isso, difícil provar que o conjunto dos números que contêm algum 7 é muito mais denso do que o conjunto dos inteiros que evitam o dígito 7. O resultado de Maynard é interessante porque mostra a existência de infinitos primos num conjunto pouco denso.

A estrutura subjacente aos números primos, embora sejam um conjunto muito fácil de definir, permanece em grande medida misteriosa. O estudo dos números primos tem importância simultaneamente teoria e prática. Sabemos que os métodos de encriptação normalmente usados na Internet dependem da dificuldade em encontrar os fatores primos de um número (grande) dado. A utilidade dos números primos ficaria comprometida se alguém descobrisse um método simples para fatorizar um número natural.

Por vezes parece que os números primos se comportam de um modo aleatório ou imprevisível. Se observarmos os restos da divisão por 3 dos números na sequência de primos:

$$5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

iremos obter dois valores possíveis, 1 ou 2, sendo que estes valores parecem ter sido obtidos através do lançamento de uma moeda ao ar. Esta imprevisibilidade dos números primos está certamente relacionada com o seu poder de encriptação. Um outro problema famoso de um conjunto de inteiros com eventualmente infinitos números primos é o conjunto $A = \{n^2 + 1 : n \in \mathbb{N}\}$. O conjunto dos quadrados perfeitos não pode obviamente conter nenhum número primo. Mas o que é que acontece se considerarmos o conjunto dos inteiros obtidos, a partir dos quadrados perfeitos, por translação de uma unidade? Não parece neste caso existir nenhuma obstrução para que alguns dos elementos do conjunto A possam ser números primos. Se acreditarmos que os primos se comportam de modo aleatório, devemos talvez apostar na existência de infinitos números primos da forma $n^2 + 1$. Será necessário conhecer um pouco mais da estrutura dos números primos para atacar este e outros problemas do mesmo tipo.

REFERÊNCIAS

[1] J. Maynard, *Primes with restricted digits* arXiv:1604.01041.