PRIMOS ORIGINAIS

JORGE NUNO SILVA
Universidade
de Lisboa
jnsilva@cal.berkeley.edu

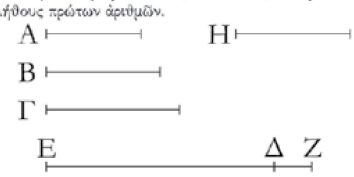
Os números primos, pilares da aritmética, têm apaixonado muitos matemáticos ao longo dos tempos, principalmente pela sua misteriosa distribuição entre os números naturais. Paulo Ribenboim (*The Book of Prime Numbers*, Springer 1989) foi um desses matemáticos. A prova de Euclides, nos *Elementos*, da infinitude dos números primos é um belo exemplo de dedução matemática. Ribenboim exibe outras demonstrações, de mestres como Euler e Kummer, mas também de matemáticos mais obscuros. Hoje trazemos aqui algumas das ideias mais simples.

A prova de Euclides da infinitude dos primos pode ser escrita, essencialmente, mostrando que qualquer coleção finita de primos está incompleta.

Euclides, mestre na utilização do método do exemplo generalizável, começou por considerar uma coleção de três primos.

κ΄.

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.



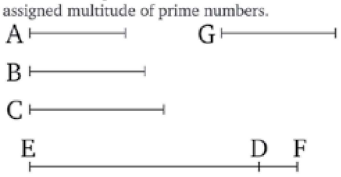
Ἔστωσαν οἱ προτεθέντες πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ· λέγω, ὅτι τῶν Α, Β, Γ πλείους εἰσὶ πρῶτοι ἀριθμοί.

Εἰλήφθω γὰρ ὁ ὑπὸ τῶν Α, Β, Γ ἐλάχιστος μετρούμενος καὶ ἔστω ΔΕ, καὶ προσκείσθω τῷ ΔΕ μονὰς ἡ ΔΖ. ὁ δὴ ΕΖ ἤτοι πρῶτός ἐστιν ἢ οὔ. ἔστω πρότερον πρῶτος· εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ, ΕΖ πλείους τῶν Α, Β, Γ.

Ἀλλὰ δὴ μὴ ἔστω ὁ ΕΖ πρῶτος· ὑπὸ πρώτου ἄρα τινὸς ἀριθμοῦ μετρεῖται. μετρείσθω ὑπὸ πρώτου τοῦ Η· λέγω, ὅτι ὁ Η οὐδενὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. εἰ γὰρ δυνατόν, ἔστω. οἱ δὲ Α, Β, Γ τὸν ΔΕ μετροῦσιν· καὶ ὁ Η ἄρα τὸν ΔΕ μετρήσει. μετρεῖ δὲ καὶ τὸν ΕΖ· καὶ λοιπὴν τὴν ΔΖ μονάδα μετρήσει ὁ Η ἀριθμὸς ὤν· ὅπερ ἄτοπον. οὐκ ἄρα ὁ Η ἑνὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. καὶ ὑπόκειται πρῶτος. εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ πλείους τοῦ προτεθέντος πλήθους τῶν Α, Β, Γ οἱ Α, Β, Γ, Η· ὅπερ ἔδει δεῖξαι.

Proposition 20

The (set of all) prime numbers is more numerous than any assigned multitude of prime numbers.



Let A, B, C be the assigned prime numbers. I say that the (set of all) primes numbers is more numerous than A, B, C.

For let the least number measured by A, B, C have been taken, and let it be DE [Prop. 7.36]. And let the unit DF have been added to DE. So EF is either prime, or not. Let it, first of all, be prime. Thus, the (set of) prime numbers A, B, C, EF, (which is) more numerous than A, B, C, has been found.

And so let EF not be prime. Thus, it is measured by some prime number [Prop. 7.31]. Let it be measured by the prime (number) G. I say that G is not the same as any of A, B, C. For, if possible, let it be (the same). And A, B, C (all) measure DE. Thus, G will also measure DE. And it also measures EF. (So) G will also measure the remainder, unit DF, (despite) being a number [Prop. 7.28]. The very thing (is) absurd. Thus, G is not the same as one of A, B, C. And it was assumed (to be) prime. Thus, the (set of) prime numbers A, B, C, G, (which is) more numerous than the assigned multitude (of prime numbers), A, B, C, has been found. (Which is) the very thing it was required to show.

Figura 1. A Proposição VII-20 dos *Elementos* na versão de Richard Fitzpatrick.

Nós usaremos o agora estafado conjunto de n elementos, onde n representa um número natural indeterminado.

Seja $A = \{p_1, \ldots, p_n\}$ um conjunto finito de primos. Seja p um divisor primo de

$$z = p_1 \cdots p_n + 1$$

então $p \notin A$ porque ao dividirmos z por qualquer elemento de A obtemos resto 1.

Em 1878, Kummer propôs uma prova semelhante. Usando a mesma notação, Kummer considera um divisor primo de $w = p_1 \cdots p_n - 1$. Este primo, como está em A, divide também $w + 1$ e, portanto, a diferença destes dois números, o que é impossível.

Pólya sugeriu uma outra abordagem. Para obter a infinitude dos primos, basta exibir uma sucessão de números naturais cujos elementos sejam primos entre si dois a dois. Tomando um divisor primo de cada termo, teríamos uma infinidade de primos. Naturalmente, para obter esta relação entre qualquer par de números da sucessão, não podemos utilizar a infinitude dos números primos...

Pólya usou os números de Fermat

$$F_n = 2^{2^n} + 1 \qquad (n \geqslant 0)$$

Por indução, estabelece-se, sem dificuldade maior, que $F_n - 2 = F_0 \cdots F_{n-1}$, para $n \geqslant 1$. Portanto, se $k < m$, tem-se que F_k divide $F_m - 2$, e qualquer primo que divida F_k e F_m terá de dividir $F_m - 2$ e, por consequência, também terá de dividir 2, o que é absurdo, já que os números de Fermat são todos ímpares.

Aqui deixo o desafio ao leitor: encontrar outras sucessões, para as quais seja possível provar que os respetivos termos são primos entre si dois a dois, sem utilizar a infinitude dos primos. Se o conseguir, terá obtido uma demonstração original do resultado de Euclides!

Outra possibilidade, do agrado geral, mas que não cumpre o último requisito mencionado, consiste em usar os números de Fibonacci

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad (n \geqslant 2) \end{aligned}$$

Os termos da sucessão de Fibonacci gozam de inúmeras propriedades e relações. Uma delas, bem conhecida, é a seguinte:

$$f_{(n,m)} = (f_n, f_m)$$

onde os parênteses representam o máximo divisor comum. Assim, se indexarmos os números de Fibonacci com os termos de uma sucessão cujos termos são primos entre si dois a dois, obtemos outra sucessão com a mesma propriedade. Esta nova sucessão pode agora ser usada para indexar os números de Fibonacci, e assim sucessivamente.

E o leitor, tem outras sugestões para esta questão?

Sobre as questões propostas no número anterior:

- Como o objetivo é 100, a penúltima jogada do vencedor será para 89 (o adversário joga para um número entre 90 e 99.... Este raciocínio de análise retrógrada pode iterar-se e concluímos que o jogador vencedor vai fazer as seguintes jogadas: 1, 12, 23, 34, 45, 56, 67, 78, 89, 100. Assim, o vencedor será o primeiro a jogar, que juntará uma unidade ao total nulo inicial.

- Os filhos vão e um deles regressa, passando o barco ao pai, que atravessa e manda o outro filho de volta. Finalmente, os filhos atravessam juntos. Este procedimento pode iterar-se no caso de um regimento de adultos...

- **A** responde que tem as plantas dos pés vermelhas, quer seja verdadeiro ou mentiroso. Assim, a resposta de **B** mostra que se trata de um indígena mentiroso (plantas brancas). A resposta de **C** denuncia-o também como mentiroso (plantas dos pés brancas).

- $237\,812 = 1025 \times 232 + 12$. A ideia é dividir 237 812 por 1025, porque se o resto de uma divisão for menor do que o quociente e do que o divisor, então estes podem trocar de papéis entre si.