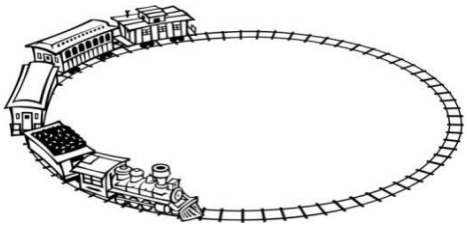
Problema 1 E assim nas calhas da roda…



Resolução *Dedicada a jovens que se encantaram com o universo dos comboios, ou outras máquinas igualmente maravilhosas como aviões ou computadores, que nos deslumbram pela forma como funcionam e que alteram a maneira como vivemos, e que começam a descobrir os encantos e a potência da ciência lógica dedutiva que permitiu estabelecer os princípios em que estas máquinas se baseiam e é decisiva na sua concepção, construção e controle.*

A nossa primeira pergunta

Vamos então designar o número de estações por N e o número de estações até que o comboio para de novo por a e vamos supor que a e N são primos relativos.

Imagina que entras no comboio na estação e; conseguirás chegar a qualquer estação se escolheres o número k de paragens antes de saíres?

Vamos experimentar em dois casos simples designando por s o número da estação de saída e supondo que $e = 1$.

Caso 1: $N = 5 \quad a = 2$

k	1	2	3	4	5
s	3	5	2	4	1

Caso 2: $N = 6 \quad a = 5$

k	1	2	3	4	5	6
s	6	5	4	3	2	1

De facto, em ambos os casos consegues sair em qualquer das estações da linha. E facilmente reconheces que o mesmo se passaria se entrasses numa outra estação e.

Mas agora imagina que a linha tem 968207 estações e que o comboio para de 227 em 227 estações ou que tem 227 estações e o comboio cada 968207 estações: sabemos que estes números são primos relativos pois $968207 = 977 \times 991$ e 977, 991, 227 são primos.

Estás a ver que neste caso a construção de uma tabela análoga é uma tarefa e tanto… impraticável.

E mesmo que o fosse recorrendo por exemplo a um computador, não o conseguiríamos fazer para todos os primos relativos pois todo o número primo é relativo com qualquer outro primo e há primos arbitrariamente grandes.

A demonstração de que há primos arbitrariamente grandes foi feita por Euclides, há mais de 2000 anos, que conseguiu uma demonstração tão bela que o matemático inglês G. H. Hardy a inclui no seu célebre livro "*A apologia de um matemático*"[1] considerando-a simples na ideia e execução mas da mais alta classe. Podes ler essa demonstração no fim no Apêndice I.

Vamos então tentar demonstrar que todas as estações são atingíveis se N e a são primos relativos. E para facilitar a exposição vamos designar a estação N por estação 0.

Repara que, partindo da estação e , e depois de k paragens o comboio está na estação s onde s é o resto da divisão de $e + ka$ por N: $e + ka = \dot{N} + s$.

Ora é fácil reconhecer que se j e k são diferentes e inferiores a N os restos da divisão de $e + ja$ e de $e + ka$ por N são diferentes, ou seja, ao fim de j e k paragens vais sair em estações diferentes.

Vê só:

Se $e + ja = \dot{N} + r$ e $e + ka = \dot{N} + r$ então, e subtraindo membro a membro, chegamos a

$$(j - k)a = \dot{N}$$

Mas como a e N são primos relativos $j - k$ seria um múltiplo de N (*vê o Apêndice II no fim*) o que é impossível pois $j - k \neq 0$ e $|j - k| < N$.

Assim, deixando k variar de 0 a $N - 1$ chegas a N estações diferentes, ou seja, chegas a todas as estações da linha e isto independentemente da estação e onde entraste.

Para chegar à estação e basta-te não partir!... mas se quiseres passear um pouco de comboio deixas passar um número de paragens que seja múltiplo de N e estarás onde partiste… queres verificar?

A nossa segunda pergunta

Se entrares na estação e e, ao fim de k paragens, saíres na estação s então, e como já vimos, s é o resto da divisão de $e + ka$ por N.

O que queremos conhecer são os valores de s quando k varia de 0 até infinito.

Os restos da divisão de ka por N são os números 0, $d, 2d, \ldots, (N' - 1)d$ onde d é o máximo divisor comum de a e N e $N' = \frac{N}{d}$ (*podes ver a prova no Apêndice III*) e obtêm-se para os valores de k de 0 a $N' - 1$. Dois $k's$ que difiram de um múltiplo de N conduzem ao mesmo resto.

Logo os restos da divisão de $e + ka$ por N são os restos da divisão de $e + rd$ por N [2] com r a variar de 0 a $N' - 1$.

[1] Ouvi um dia o neurocirurgião João Lobo Antunes dizer que na sua juventude tinha ficado fascinado com este livro que lhe tinha aberto a janela para a beleza da Matemática. Está publicado pela Gradiva.

[2] O resto da divisão por N da soma é o resto da divisão por N da soma dos restos da divisão das parcelas por N: queres verificar?

Facilmente vês que são todos diferentes e em número de N' : são estas, e só estas, as estações a que consegues chegar quando embarcas em e. E para lá chegar basta-te esperar por 0, 1, 2,…, $N' - 1$ paragens.

Se chegares a uma paragem e quiseres viajar mais um pouco regressando ao mesmo sítio basta-te esperar por um número de paragens que seja múltiplo de N'.

Apêndice I

Teorema

Há uma infinidade de primos.

Prova - *Devida a Euclides e constante do Livro IX dos* *Elementos*

Suponhamos que a sequência dos primos, 2, 3, 5, 7, 11, ... termina em P o maior dos primos.

Ponhamos $Q = 2 \times 3 \times 5 \times 7 \times 11 \times \ldots \times P + 1$, ou seja, Q igual ao produto dos primos mais um.

Então Q não seria divisível por qualquer primo pois qualquer primo divide a primeira parcela, mas não a segunda.

Mas Q não seria primo pois os primos terminam em P.

Logo seria divisível por um primo que não consta na lista de primos e seria, por isso, ser superior a P!

Nota : *Trata-se de uma prova por redução ao absurdo método que Euclides usava com tanto gosto*.

Apêndice II

Cerca de 300 AC Euclides enunciou o que é conhecido como o

Teorema Fundamental da Aritmética

> *Todo o natural maior do que 1 pode escrever-se como produto de naturais primos menores ou iguais a ele. Essa representação é única[3] a menos de rearranjos dos factores.*

Então se a e b são primos e $ac = \dot{b}$ como nenhum dos factores primos de b aparece na decomposição de a em factores primos deve aparecer na decomposição de c e com expoente não inferior logo c é múltiplo de b.

Apêndice III

Como vimos no início da resolução os restos da divisão de ka' por N' são todos os números e 0 a $N' - 1$ e obtêm-se para $k = 0, \ldots, N' - 1$ pois a' e N' são primos relativos. Dois $k's$ que difiram de um múltiplo de N' conduzem ao mesmo resto.

Ou seja $ka' = \dot{N}' + r$ onde r toma todos os valores entre 0 e $N' - 1$ quando k varia de 0 a $N' - 1$.

Multiplicando a igualdade por d obtemos $ka = \dot{N} + rd$.

---

[3] É para garantir esta unicidade que não se considera 1 um número primo.