N. 0170

Gazeta de Matemática

Publicação quadrimestral da SOCIEDADE PORTUGUESA DE MATEMÁTICA | Ano LXXIV | Jul. 2013 | 4,20€

Macacos me Mordam

NA LINHA DE FRENTE FABIO CHALUB

Yerkes National Primate Research Center

Combinatória, Zonogonos e Zonoedros

ILDA PEREZ

Números Inteiros: Alguns Critérios de Divisibilidade

ANDRÉ FONSECA E TERESA ALMADA

United Nations Educational, Scientific and Cultural Organization

Comissão Nacional da UNESCO - Portugal
Portuguese National Commission for UNESCO

Math 2013

2013 ESCOLA DE VERÃO DE MATEMÁTICA

Matemática do Planeta Terra

5 a 7 setembro
MUHNAC Lisboa
(Museu Nacional de História Natural e da Ciência da Universidade de Lisboa)

CONFERÊNCIAS

Decisões individuais e mercados competitivos
Alberto Pinto

Matemática no Planeta Terra
Eduardo Marques de Sá

Estrutura e dinâmica da população portuguesa
Edviges Coelho, Maria da Graça Magalhães e Jorge Bravo

Seria a Terra redonda no Renascimento? Navegação e cartografia no tempo das descobertas
Joaquim Alves Gaspar

Aspetos matemáticos do Planeta Terra
José Francisco Rodrigues

Entre ordem e desordem: da célula ao Sol
Paula de Oliveira

Ondas harmónicas, análise de Fourier e vibrações sísmicas
Sérgio Oliveira

Matemática dos recursos biológicos: crescimento e colapso
Tiago Domingos

MINI CURSOS

Simetrias nas equações diferenciais
Alexandre Rodrigues

Matemática e Google Earth
Jaime Carvalho e Silva

O GPS e a Teoria da Relatividade
José Natário

O efeito da rotação da Terra na circulação atmosférica e oceânica
Juha Videman e Aires dos Santos

Fogos florestais em Portugal: caracterização e modelação
Manuela Oliveira, Susete Marques e José Borges

Influência de decisões individuais num mercado competitivo
Renato Soeiro

http://evspm2013.spm.pt/
evspm2013@spm.pt

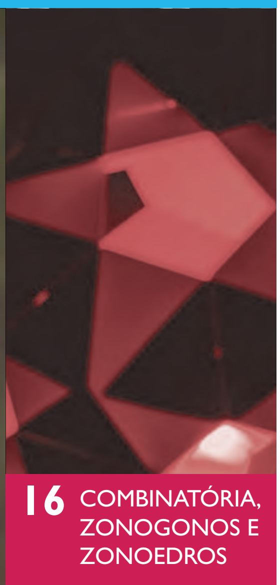
spm SOCIEDADE PORTUGUESA DE MATEMÁTICA

ORGANIZADORES

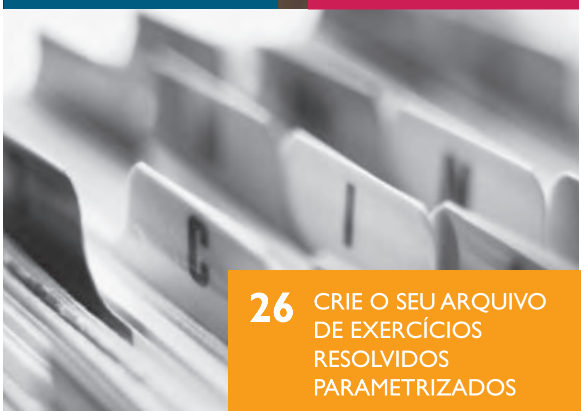
Carla Martinho | Fernando Pestana da Costa | João Teixeira Pinto | Jorge Buescu

36 NÚMEROS INTEIROS: ALGUNS CRITÉRIOS DE DIVISIBILIDADE

13 NA LINHA DE FRENTE | **MACACOS ME MORDAM!**



16 COMBINATÓRIA, ZONOGONOS E ZONOEDROS



26 CRIE O SEU ARQUIVO DE EXERCÍCIOS RESOLVIDOS PARAMETRIZADOS

03 ATRACTOR | **CORTESIA EM JOGO**

ÍNDICE

EDITORIAL

ROGÉRIO MARTINS
Universidade Nova
de Lisboa
roma@fct.unl.pt

SOBRE A **IMPORTÂNCIA** DE **ENTRAR** COM O **PÉ DIREITO**

A matemática tende a ser vista pela sociedade como uma medida da nossa inteligência. Infelizmente isso tem um custo...

No editorial do número 168 desmontei um pouco este mito. De facto, não me parece que a matemática seja uma medida fiel da nossa inteligência, independentemente do que a inteligência possa significar. Gostaria agora de falar sobre os problemas que esta imagem acarreta.

Independentemente do que entendermos por inteligência, a verdade é que ninguém gosta de assumir que não a tem em quantidade razoável. É comum ouvir alguém dizer que não é suficientemente alto para jogar basquetebol, que não tem queda para a bricolage, ou que não tem jeito para arrumar a louça na máquina... No entanto, algo que nunca ouvimos dizer é: "Eu não sou lá muito inteligente!..." Por alguma razão que me escapa, ninguém gosta que coloquem em causa as suas capacidades de inteligência. A verdade é que nos sentimos feridos quando a nossa inteligência é posta em causa.

Sendo o sucesso em matemática (certa ou erradamente) normalmente associado às nossas capacidades de inteligência, é espectável que o sucesso em matemática acabe por ser um assunto sensível para os estudantes. Por um lado, quem por alguma razão tende a entrar com o pé direito na matemática, recebe um reforço positivo e tipicamente diz: "Eu tenho jeito para a matemática." Por outro lado, quem entra com o pé esquerdo recebe um beliscão na sua auto-estima e tende a dizer: "Eu não gosto de matemática." Reparem que não é inocente a escolha nos verbos: "tenho jeito" *versus* "não gosto". No primeiro caso, o interlocutor deixa claro que tem essa capacidade e, no segundo caso, prefere assumir que o insucesso é essencialmente uma opção, protegendo, desta forma, a sua auto-estima.

No caso em que há sucesso, há um reforço positivo para o estudante, que tende a manter ou até mesmo a melhorar os seus resultados. No caso de insucesso, há uma tendência para piorar os resultados e reforçar a posição de desinteresse pela disciplina, protegendo a auto-estima, como vimos antes. Na verdade, é bem conhecida uma certa tendência para a bipolarização dos resultados em matemática, e, na minha opinião, esta é uma das causas.

Por outro lado, a entrada, ou não, de um estudante com o pé direito na matemática não depende de forma essencial de capacidades cognitivas especiais, mas sim de uma série de outros factores, na maior parte das vezes não controláveis pelo próprio estudante. Muitos estudantes entram no círculo vicioso do "não gosto de matemática" por razões que, em geral, não são fáceis de identificar...

ATRACTOR

No âmbito de uma colaboração entre a Gazeta e o Atractor, este é um espaço da responsabilidade do Atractor, relacionado com conteúdos interactivos do seu site *www.atractor.pt* . Quaisquer reacções ou sugestões serão bem-vindas para *atractor@atractor.pt*

CORTESIA EM JOGO

O presente texto gira em torno da pergunta seguinte: *num conjunto de dados diferentes, qual é o melhor?*

Esta pergunta, que é natural formular, levanta uma questão matematicamente interessante que tem uma resposta algo inesperada. E foram estes dois aspetos que ditaram a escolha, pelo Atractor, de um módulo para a exposição "Matemática Viva"[1], que permitia precisamente pôr em evidência um comportamento aparentemente estranho.

Antes de descrevermos esse módulo, tornemos claro o que entendemos por um dado ser melhor do que outro. Os dados *normais* são cubos e têm, em cada uma das seis faces, um número diferente de pintas, entre um e seis. Nenhum dado é melhor do que o outro, no sentido de que dois jogadores, cada um com um dos dois dados, têm iguais probabilidades de ganhar, podendo ainda empatar. Se em vez de considerarmos dois dados normais, admitirmos que em cada face de cada um há um número de pintas entre 0 e 6, podendo duas ou mais faces de um mesmo dado ter igual número de pintas, então os dois dados podem ser diferentes entre si e as probabilidades de cada um ganhar não serem as mesmas, além de que a probabilidade de empate pode ser 0. O dado A é considerado *melhor* do que o dado B, se a probabilidade de A ganhar a B for maior do que a de B ganhar a A. Por exemplo, se as seis faces de A tiverem, respectivamente, 1, 1, 1, 3, 3, 3 pintas e as de B tiverem todas 4 pintas, o jogo nunca empata e a probabilidade de A ganhar é 0, o que equivale a afirmar que a de B ganhar é 1. Se os dados forem iguais, as probabilidades de A e B ganharem são as mesmas, mas o seu valor depende da probabilidade de A e B empatarem. Por exemplo, se A e B forem iguais e além disso todas as faces tiverem o mesmo número de pintas, a probabilidade de empate é 1 e, portanto, a probabilidade de cada um ganhar é 0. O leitor poderá verificar que esta situação extrema só acontece nas condições descritas, também elas extremas.

Figura 1

[1] A exposição "Matemática Viva", que esteve patente no Pavilhão do Conhecimento, em Lisboa, entre novembro de 2000 e agosto de 2010, foi concebida e criada pelo Atractor.

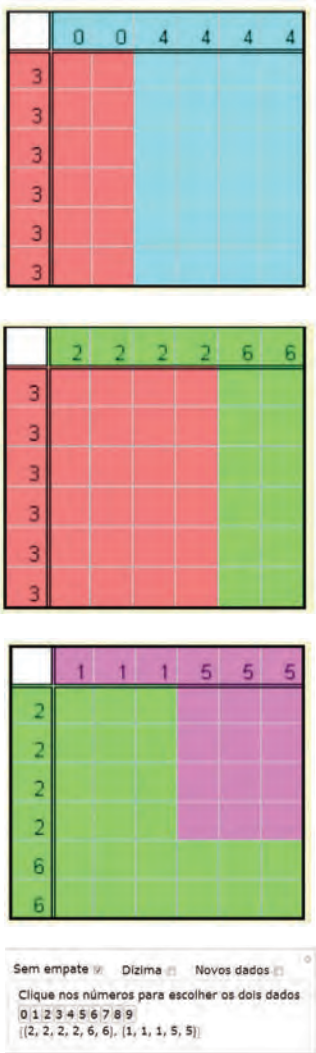


Figura 2

Suponhamos agora que A tem duas faces sem pintas e quatro com 4 pintas, o que convencionamos descrever por $A = (0, 0, 4, 4, 4, 4)$ e, com notação análoga, suponhamos $B = (3, 3, 3, 3, 3, 3)$. Em cada par de lançamentos (de A seguido de B) o jogo nunca empata, e há 36 pares (igualmente prováveis) de faces possíveis (em cada par de lançamentos), mas os pares de números obtidos são apenas dois: (0, 3), em que ganha B e (4, 3), em que ganha A. Ora, dos 36 casos possíveis, 12 correspondem a (0, 3) e 24 a (4, 3). Portanto, a probabilidade de B ganhar é $12/36 = 1/3$ e a de A ganhar é o dobro: $24/36 = 2/3$. Se B jogar com um terceiro dado $C = (2, 2, 2, 2, 6, 6)$, também nunca há empate, B ganha a C em 24 dos 36 casos e C ganha a B nos outros 12: podemos traduzir a situação, dizendo que B é *duas vezes melhor* do que C. Deixamos ao leitor a verificação de que, tomando como quarto dado $D = (1, 1, 1, 5, 5, 5)$, C é duas vezes melhor do que D. (Para controlar ou evitar as contas, pode usar uma calculadora de probabilidades [1], figura 2).

Chegados a este ponto, e encarando apenas as observações feitas, parece que, relativamente à questão formulada no início do artigo, é natural conjeturar que, no caso dos dados A, B, C, D acima definidos, a resposta é clara: o dado A é o melhor dos quatro, uma vez que é melhor do que B, este é melhor do que C e C é melhor do que D. Em particular, se dois jogadores decidirem jogar e, antes de começarem, tiverem a oportunidade de escolher o dado que preferem (entre A, B, C e D), parece que o primeiro parte em vantagem, bastando-lhe escolher o dado A.

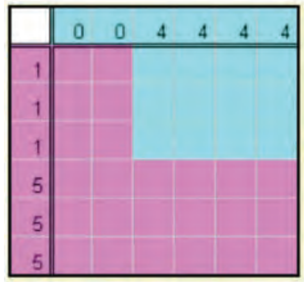


Figura3

O termo "conjecturar" usado acima em vez de "concluir" pode parecer de uma prudência excessiva. Mas, se o leitor fizer a comparação direta entre A e D, poderá verificar que A só ganha nos 12 pares correspondentes a (4,1), perdendo nos restantes 24 (= 6 + 6 + 12) correspondentes a (0,1), (0,5) e (4,5). Quer dizer: o dado D, que *devia* ser muito (? 8 vezes) pior do que A, é na verdade duas vezes melhor do que ele... Voltemos à conjectura: subjacente à sua formulação estava a ideia, que acaba de se verificar ser errada, de que a relação entre dados, traduzida por "melhor do que" seria transitiva.

Figura 4

O quadro ao lado representa bem o ciclo de dados que se considerou: em cada coluna estão indicados os números de pintas das seis faces e em cima a probabilidade de esse dado ganhar ao representado na coluna seguinte (a seguinte à última é a primeira). Na situação atrás referida, se, realmente, o primeiro jogador tivesse escolhido o dado A, bastaria ao segundo escolher D, para ter uma probabilidade de 2 contra 1 de ganhar ao primeiro. Mas se o primeiro jogador tivesse escolhido qualquer outro dado, bastaria ao segundo escolher o *precedente* (na seriação A, B, C, D) para ter uma probabilidade de 2 contra 1 de ganhar ao primeiro. Isto é, o jogador que escolhe o dado em segundo lugar é que parte em grande vantagem, pois pode sempre escolher um dado melhor do que o do outro jogador (a noção de cortesia é invertida neste contexto: ser cortês é aqui "servir-se primeiro" e não "deixar o adversário servir-se"...). Conclusão: a pergunta inicial está mal formulada e induz uma ideia errada; antes de perguntar qual o dado melhor, seria prudente estar certo de que existe **sempre** um dado melhor do que todos os restantes (pelo menos num sentido lato). Ora isso não acontece, como o comprova o exemplo dado. Na exposição "Matemática Viva", havia uma mesa (ver foto da figura 1) e, sobre ela, quatro dados com a composição A, B, C, D indicada acima. Com quatro jogadores à volta da mesa, cada um jogava um número razoável de ve-

Figura5

zes com o seu vizinho da direita e anotava o resultado, depois o da direita jogava com o seguinte (à direita) e assim sucessivamente. Com grande probabilidade[2], cada jogador ganhava ao jogador à sua direita, o que acabava por "sugerir" que não havia nenhum dado melhor do que todos os outros[3].

Um ciclo de quatro dados como (A, B, C, D) atrás considerado diz-se *não-transitivo*. E é natural agora levantar a questão de saber se haveria outras escolhas possíveis para os números de pintas nas faces dos seis dados, escolhas essas que fossem igualmente adequadas para pôr em evidência esta inesperada propriedade. Se quisermos escolher quatro dados de forma a que, tal como acontece naqueles dados, nunca haja empate em qualquer das jogadas entre dois deles, teremos de os escolher de modo a que nenhuma face de cada um deles tenha o mesmo número de pintas de qualquer face do outro. Ora, se permitirmos de 0 a 6 pintas, estas sete possibilidades não chegam para que todos os quatro dados tenham dois tipos de faces ($4 \times 2 = 8 > 7$ alternativas), portanto, pelo menos um dado terá necessariamente todas as faces com o mesmo número de pintas. Usando um programa feito no *Mathematica* com esse propósito, selecionámos todos os ciclos não-transitivos, isto é, em que as probabilidades de cada dado ganhar ao seguinte são todas maiores do que 1/2. Encontrámos 37 ciclos não-transitivos (ver [1]), dos quais os 12 primeiros estão representados na figura 5.

Calculando, para cada ciclo, o mínimo das probabilidades referidas, todas elas maiores do que 1/2, obtivemos para esses mínimos apenas três valores: 5/9, 7/12 e 2/3, mas apenas um ciclo, o indicado acima, tem mínimo 2/3, que é o valor (comum) da probabilidade de cada dado ganhar ao seguinte no ciclo. Dos restantes 36 ciclos, três (do 2.º ao 4.º, na figura) têm 7/12 como probabilidade mínima e 33 têm 5/9. Ora, 5/9 é muito próximo de 1/2, isto é, a probabilidade de um dado ganhar ao outro é só ligeiramente maior do que a de perder. E essa pequena diferença torna a escolha desinteressante: com um pequeno número de jogadas, não se consegue pôr em evidência de modo significativo a diferença entre os resultados dos dois dados. Além disso, um ciclo que corresponda a 7/12, embora em grau ligeiramente menor do que no caso 5/9, também tem um inconveniente análogo e não é uma boa escolha. Em conclusão: o ciclo da "Matemática Viva" era a única escolha ótima!

Para uma versão virtual deste módulo, interessa dispor de vários ciclos não-transitivos diferentes, todos *ótimos* (no sentido de a probabilidade mínima ser a maior possível[4]). Isso não é viável para dados com 0 a 6 pintas nas faces, pois já vimos que só há um ciclo ótimo, o acima indicado. Mas recorrendo a dados com faces podendo ter maior número de pintas e mantendo as outras características (em particular, ser 2 o número máximo de faces diferentes em cada dado),

[2] Suponhamos que, para cada par de jogadores, há um lançamento dos dois dados, não apenas uma vez, mas sim um número n (ímpar) de vezes. Se se considerar ganhador aquele que mais vezes obtiver um número maior do que o do oponente, então a probabilidade de A ganhar a B neste jogo aumenta relativamente à de A ganhar a B com apenas um lançamento de A e outro de B (suposta > 0.5). É esta a razão pela qual se preconizava no módulo da "Matemática Viva" que os visitantes repetissem várias vezes os lançamentos. O leitor pode verificar que essa probabilidade é dada pela seguinte fórmula

$$\sum_{j=k}^{n} \binom{n}{j} p^j q^{n-j}, \text{ em que } n = 2k-1 \text{ e } \binom{n}{j} = \frac{n!}{(j!(n-j)!)}.$$

Os primeiros vinte valores, para n=1,3,...,39 são aproximadamente: 0.667, 0.741, 0.790, 0.827, 0.855, 0.878, 0.896, 0.912, 0.925, 0.935, 0.944, 0.952, 0.958, 0.964, 0.969, 0.973, 0.977, 0.980, 0.982, 0.984.

[3] Refira-se como curiosidade que, se B jogasse com D, a probabilidade de lhe ganhar seria 1/2, e, se A jogasse com C, a probabilidade de A ganhar seria 4/9.

[4] Trybula e Steinhaus provaram que essa probabilidade mínima não pode exceder o valor encontrado naquele ciclo: 2/3. Ver [2] e [3].

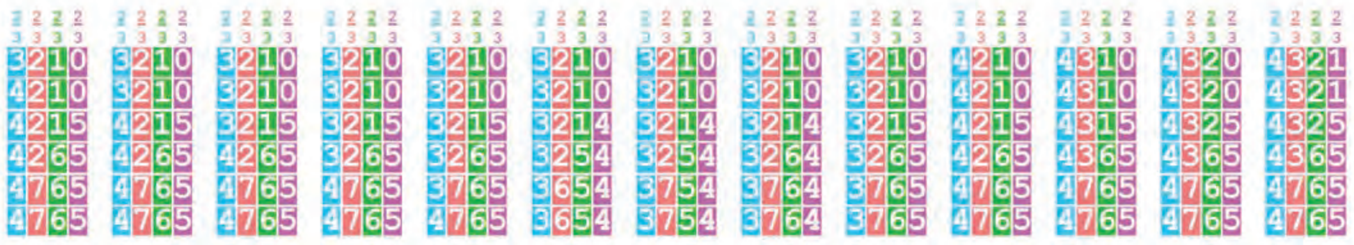


Figura 6

é possível obter mais ciclos *ótimos*. Com o *Mathematica* foi possível localizar 13 ciclos *ótimos* para 0 a 7 pintas e 81 para 0 a 8 pintas (num total, respetivamente, de 527 e 3495 ciclos não-transitivos). Na figura 6, eis os ciclos ótimos com 0 a 7 pintas.[5]

Se, em vez de ciclos de quatro dados, nos limitarmos a ciclos de três, digamos com uma a seis pintas, haverá algo interessante a referir? Vamos desistir da impossibilidade de ocorrerem empates, mas acordamos que, quando num par de lançamentos houver um empate, ele é ignorado e o lançamento é repetido até à vitória de um dos lados.

Analisando a situação com um programa feito no *Mathematica*, foi possível recolher alguma informação: há 462 dados diferentes e com eles podemos construir 40666 ciclos não-transitivos. Mas 68 dados não intervêm nestes ciclos e, dos restantes 394, a frequência com que surgem é muito variável: desde dois dados ({1,1,2,2,2,4} e {3,5,5,5,6,6}) que aparecem, cada um, em apenas um ciclo, respetivamente {{1, 1, 1, 2, 4, 4}, {1, 1, 1, 3, 3, 4}, {1, 1, 2, 2, 2, 4}} e {{3, 3, 5, 6, 6, 6}, {3, 5, 5, 5, 6, 6}, {3, 4, 4, 6, 6, 6}}, até dois outros dados ({1,1,1,5,6,6} e {1,1,2,6,6,6}) que aparecem, cada um, em 1897 ciclos distintos.

A figura 7 contém um gráfico de barras mostrando a frequência com que intervém cada dado nos diferentes ciclos não-transitivos. Em [1] é possível ver a figura numa maior resolução e uma análise mais fina permite observar que as barras desse gráfico aparecem aos pares com a mesma altura. Na base da figura estão representados os dados por colunas, cada uma com os números de pintas das faces do dado. E os dados de cada par, que aparecem, pois, ambos com a mesma frequência, estão relacionados pela forma seguinte: se $(n_1 \leq n_2 \leq \ldots \leq n_5 \leq n_6)$ são os números de pintas das faces de um dado, os números das pintas das faces do outro dado são $(m_1 \geq m_2 \geq \ldots \geq m_5 \geq m_6)$, sendo, para cada $i = 1, \ldots, 6$, $n_i + m_i = 7$. No site [1] há mais informação sobre a relação entre os 3-ciclos não-transitivos em que cada dado do par intervém.

Os valores dos mínimos das probabilidades dos ciclos não-transitivos são {18/35, 17/33, 16/31, 15/29, 14/27, 13/25,

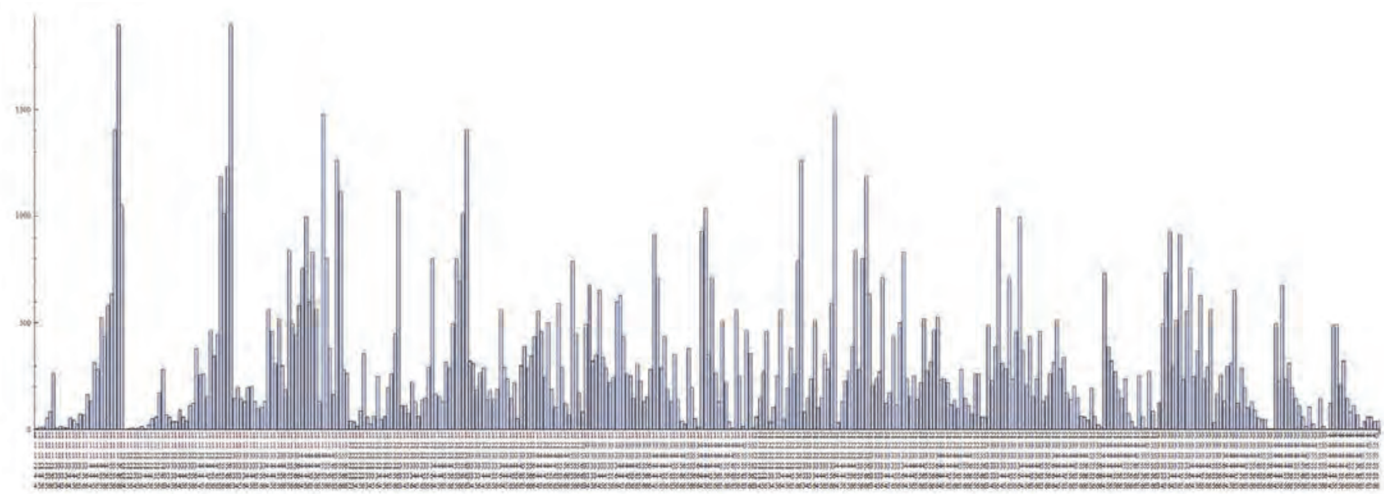


Figura 7

12/23, 11/21, 10/19, 19/36, 9/17, 17/32, 8/15, 15/28, 7/13, 13/24, 19/35, 6/11, 17/31, 16/29, 5/9, 19/34, 9/16, 17/30, 4/7, 15/26, 7/12} e oscilam, pois, entre 18/35 e 7/12, aparecendo com desigual frequência, como mostra o gráfico de barras (Figura 8). Para se ter uma ideia, não só do mínimo das probabilidades para cada ciclo não-transitivo mas também do próprio terno das probabilidades (de cada dado ganhar ao seguinte), o melhor é fazer uma representação gráfica desses ternos. Note-se que, para cada ciclo, associar-lhe um terno de probabilidades pressupõe a escolha (arbitrária) de um elemento inicial do ciclo. As outras escolhas correspondem a rodar a figura anterior por ângulos de 120º e 240º, em torno da reta passando pela origem e com direção determinada pelo vetor (1,1,1). Esses três conjuntos de pontos estão representados a cores diferentes na Figura 9. E o par estereoscópico representa um conjunto análogo mas correspondente aos 3-ciclos de dados com apenas 1 a 4 pintas nas faces (Figura 10).

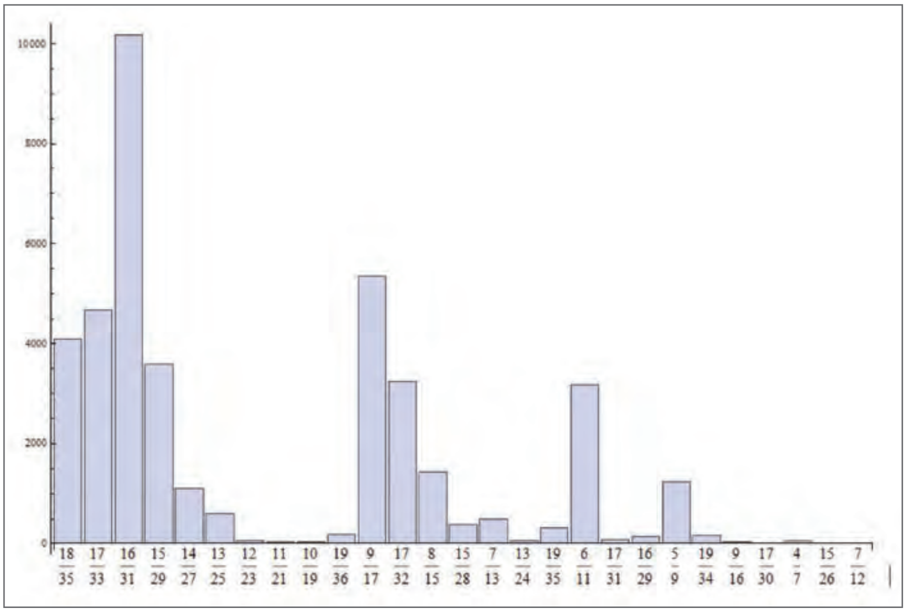


Figura 8

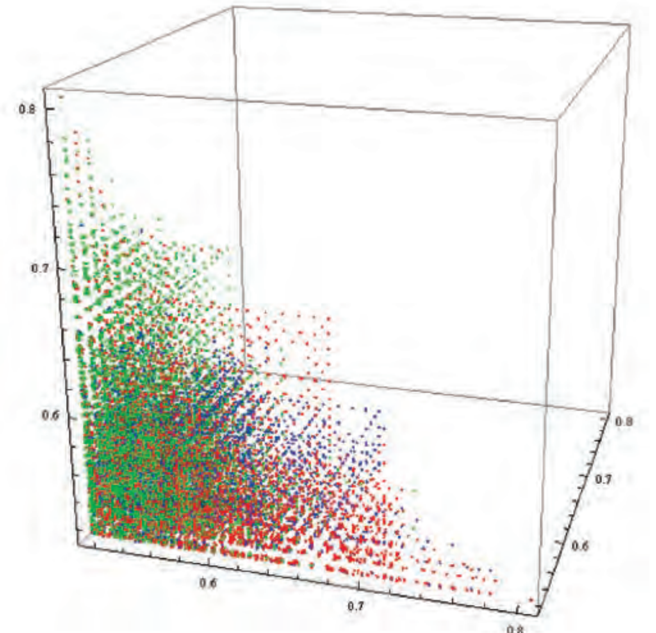


Figura 9

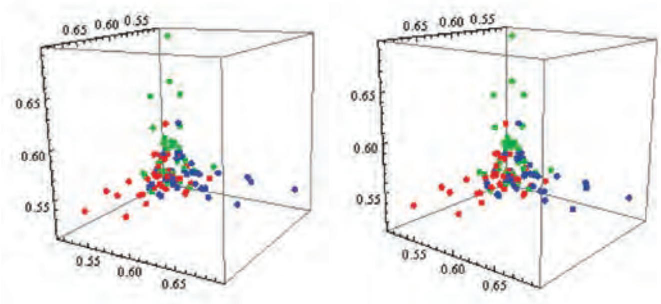


Figura 10

REFERÊNCIAS

[1] *http://www.atractor.pt/mat/JogoDados*

[2] H. Steinhaus, S. Trybula. "On a paradox in applied probabilities", *Bulletin of the Polish Academy of Sciences 7* (1959), 67-69

[3] Usiskin, "Max-min probabilities in the voting paradox", *Annals of Mathematical Statistics* Vol. 35, 2 (1964), 857-862

[5] Ver mais informações no *site* do Atractor [1].

Jorge Nuno Silva
Universidade de Lisboa
jnsilva@cal.berkeley.edu

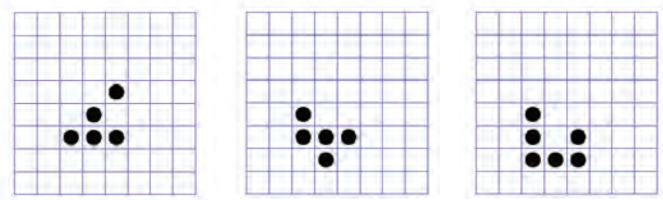
VIDA A ANDAR PARA TRÁS

O Jogo da Vida foi inventado por John H. Conway no começo da década de 70 do século passado. Numa visita a Martin Gardner, entre "outros 50 assuntos de que queria falar", mostrou como, no tabuleiro de Go, se pode implementar este jogo. Gardner ficou maravilhado e popularizou o Jogo da Vida nas páginas do *Scientific American* e em alguns dos seus livros. O volume de trabalhos de investigação a que deu origem é incalculável!

A Mathematical Association of America publicou mais uma homenagem ao maior divulgador de sempre, *Martin Gardner in the Twenty First Century*, editado por M. Henle e B. Hopkins. Aqui se recolhem textos do próprio Gardner, bem como de outros, inspirados em temas caros ao homenageado. Desta obra retiramos uma variante do jogo de Conway introduzida por Yossi Elran: Vida a Andar para Trás.

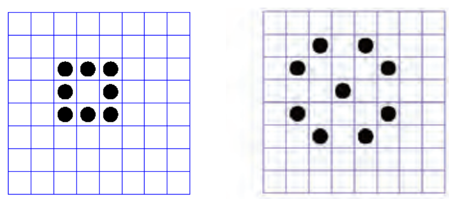
Num tabuleiro quadriculado, cada célula pode estar viva (ocupada) ou morta (vazia). Na geração seguinte, permanecem vivas as células que tiverem duas ou três casas vivas entre as oito células vizinhas. Nasce vida numa célula vazia com exatamente três vizinhos vivos. Morrem todas as células vivas que tenham menos de dois ou mais de três vizinhos vivos.

Vejamos duas gerações a partir de uma configuração inicial.

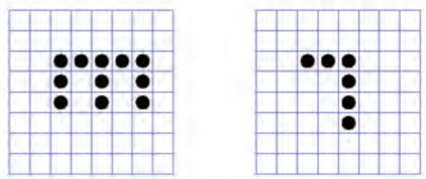


Dada uma configuração, a geração seguinte determina-se sem ambiguidade. Contudo, há muitas possibilidades para o antepassado direto de cada geração. Youssi Elran propõe alguns *puzzles* em que, dada uma configuração, se pretende obter um antepassado direto, satisfazendo algumas restrições.

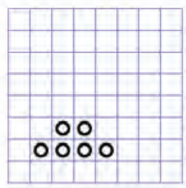
Vejamos um exemplo de Vida a Andar para Trás em que se exige que as casas vivas estejam mortas na geração anterior. Note-se que agora o diagrama da esquerda representa o futuro, o da direita, o passado imediato.



Propomos o exercício de encontrar paternidade para mais duas configurações, com a mesma restrição.



Um quebra-cabeças um pouco diferente: na configuração seguinte acrescente peças negras ao tabuleiro de forma a que somente as brancas tenham exatamente três peças vizinhas (os vizinhos podem ser peças brancas ou negras) e mais nenhuma casa do tabuleiro tenha exatamente três vizinhos. Nenhuma das peças negras pode ter dois ou três vizinhos (brancos ou negros).



Algumas notas sobre os problemas do último número.

1. *Dois homens metem-se a caminho para um longo passeio. Em cada dia o primeiro percorre 20 milhas, o segundo, uma no primeiro, duas no segundo, três no terceiro, etc. Quando é que o segundo apanha o primeiro?*

Trata-se de resolver $20x = x(x+1)/2$, que dá $x = 39$.

2. *Um homem é encarregado de transportar 90 maças entre Borgo e Perugia, que distam 30 milhas entre si. Ele só consegue carregar 30 e come uma por cada milha percorrida. Como maximizar o número de maças que chegam a Perugia?*

Por lapso faltava, no número anterior, a menção ao número de maças inicial, 90. A solução de Luca Pacioli consiste em efetuar uma paragem após 20 km, no local para onde se levam tantas maças quanto possível (em três viagens): 30. Depois, uma última caminhada, de 10 km permite chegar ao destino com 20 maças. Contudo, fazendo duas paragens, uma após 15 km, num local onde se acumula 45 maças, e outra depois de percorrer mais 5 km, para onde se desloca 35 maças, permite chegar ao fim com 25 maças.

3. *O Sr. Atikin vai de Labutes a Latrum e regressa a Labutes. A sua velocidade é de 4 km/h em terreno plano, 3 km/h nas subidas e 6 km/h nas descidas. Partiu às 9:00 e regressou a casa às 13:00. Será que pode deduzir-se a distância entre Latrum e Labutes?*

Como o percurso é de ida e volta, cada subida e cada descida são percorridas uma vez a subir e outra a descer. A velocidade média de uma viagem cujas metades se vencem a 3 km/h e a 6 km/h é... 4 km/h (4 é a média harmónica de 3 e 6). Assim, temos a velocidade média da viagem e o tempo que ela durou (4 horas). A distância entre Labutes e Latrum é metade de 4x4 km, isto é, 8 km.

Eduardo Marques de Sá
Universidade de Coimbra
emsa@mat.uc.pt

MIGALHAS DE XADREZ E MATEMÁTICA

A matemática e o jogo do xadrez têm afinidades profundas: pensamento estratégico, avaliação posicional, arte combinatória, problemas tantalizantes, dificuldades inesperadas...

Não são raros os matemáticos que se dedicaram com sucesso ao xadrez. O exemplo mais notável é o de Emanuel Lasker (1868-1941) que conseguiu conjugar 27 anos de campeão mundial de xadrez com um desempenho notável como matemático; os manuais de álgebra comutativa referem os *anéis de Lasker* e um importante teorema com o seu nome, sobre anéis de polinómios, que foi 16 anos mais tarde suplantado por Emmy Nöther, a famosa filha do orientador de tese de Lasker.

No xadrez existe a possibilidade de empate, aliás, o empate é mesmo o resultado da maioria absoluta das partidas jogadas entre grandes mestres. Com base apenas nas regras básicas de movimentação das pedras, o xadrez é um jogo *infinito*, explicando melhor: há apenas um número finito de posições possíveis, mas existem sequências infinitas de jogadas de que, obviamente, nenhum dos jogadores sai vitorioso. Sendo desejável que o jogo se torne finito, desde há muito tempo se vêm aperfeiçoando leis que determinem objetivamente o empate. Um caso curioso ocorreu em 1929. Até essa altura, em alguns países do centro europeu vigorou a seguinte regra:

(*) *Uma partida está empatada se uma determinada sequência de jogadas ocorre pela terceira vez consecutiva.*

Aparentemente, muitos xadrezistas desse tempo acreditavam que isto assegurava a finitude do jogo. Mas Max Euwe (1901-1981), também ele matemático e campeão mundial (em 1935-37), provou que não era assim, construindo partidas infinitas que não violam essa regra. Vejamos uma receita para a construção duma partida desse tipo. Olhamos apenas para os dois reis, branco e negro, sozinhos no tabuleiro, como nas figuras mais abaixo. O rei negro decalca as suas jogadas da seguinte sequência de zeros-e-uns:

01101001100101101001011001101001100101100110100101...

dita da *paridade binária*, cujo n-ésimo termo, para $n \geqslant 0$, é por definição a soma binária dos *bits* da representação binária de n. Eis como se move o rei negro: na sua n-ésima vez de jogar, se o termo n da sequência é **0**, ele desloca-se uma casa para a esquerda daquela em que se encontra, se é **1** ele desloca-se uma casa para a direita. A peça negra parece dançar num ritmo indecifrável: toca apenas em três casas e de modo aperiódico... *Porquê?* O rei branco pode dançar qualquer dança, como o *passo doble*, ou deambular preguiçosamente pelo tabuleiro, à toa, mas sem interferir no movimento preciso do outro. O facto interessante é que este *pas de deux* real não viola a regra (*). De facto, a sequência da paridade binária não possui secção nenhuma que ocorra três vezes consecutivas!

Em 1929, ano de publicação do artigo de Euwe, a Federação Internacional de Xadrez propôs a primeira versão oficial das regras do jogo, onde o empate vigora sempre que certa posição do jogo ocorre pela terceira vez. A partir daí, o jogo passou a ser burocraticamente finito! Acrescente-se que existem outras regras tendentes a abreviar a ocorrência dum empate, como a impossibilidade material duma vitória, providências cautelares contra longas sequências "inócuas", acordo entre os contendores, etc..

Em abono da verdade, diga-se que Euwe reinventou a sucessão acima referida. Os nomes a ela associados são: Eugéne Prouhet, que a encontrou, em 1851, na teoria dos números; Axel Thue, em 1906, numa questão combinatória; Marston Morse, em 1921, em geometria diferencial; e Max Euwe, a propósito das regras do xadrez, como vimos. Trata-se dum daqueles objetos matemáticos multifacetados, com muitas definições alternativas retiradas de áreas bem distintas que vale a pena revisitar. Por exemplo, tem uma estrutura fractal, por ser igual a uma subsucessão sua, a dos termos de ordem par, sendo por isso igual a uma infinidade de subsucessões suas... *Porquê?* Por outro lado, ela é uma concatenação de cópias das secções A=0110 e B=1001 e, se nela substituirmos cada 0 por uma secção A e cada 1 por B, reobtemo-la de volta... *Porquê?*

Os problemas seguintes são vagas reminiscências do xadrez. No tabuleiro vão estar apenas os dois reis, o que no xadrez real não interessa. Como um rei não pode encostar-se a outro rei,[1] o resultado xadrezístico é um empate, a não ser que se mudem as regras, o que vai ser o caso.

Introduzamos a seguinte restrição aos movimentos permitidos ao rei no xadrez tradicional:

Lei da Reincidência. *Em cada partida perde o rei que ocupe uma casa já por si ocupada em alguma jogada anterior.*

Nestas condições, cada partida termina ao cabo de não mais de 64 movimentos de cada rei, com a vitória dum deles. Em jogos deste tipo – finitos, sem empates, de informação completa e sem intervenção de fatores aleatórios – sabe-se, desde a posição inicial, que um dos jogadores tem uma estratégia para vencer. Os problemas matemáticos são determinar qual deles detém essa estratégia e como deve jogar para vencer.

No diagrama da figura ao lado, a linha quebrada separa duas partidas distintas de rei contra rei sob a lei de reincidência. A chave para resolver alguns destes problemas é bem conhecida no xadrez: diz-se que os reis estão em *oposição* se ocupam casas da mesma cor e na mesma fila (linha ou coluna); o rei que tem de jogar está, em geral, em maus lençóis; diz-se então que o outro *detém a oposição*.

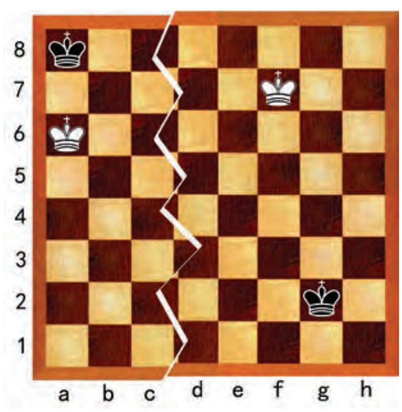
Na partida do lado esquerdo, cabe às negras jogar, pelo que o rei branco detém a oposição. O negro só pode jogar para b8, o que possibilita ao branco deter de novo a oposição, jogando b6; depois o negro é forçado a ir a c8, o branco joga c6 e assim sucessivamente até ao afogamento do rei negro. Coloca-se agora a questão, que fica a seu cargo: *se for o rei branco a jogar, quem tem a estratégia vencedora?*

Na partida da parte direita, os reis não estão em oposição, mas o primeiro a jogar pode detê-la logo na abertura. Abrindo as negras, o rei passa a deter a oposição jogando para f3 e ganhará cumprindo sem falhas duas cláusulas estratégicas: deter sistematicamente a oposição e nunca jogar para sul. O rei branco acaba por ter de recuar até á linha 8 e por lá dar os seus últimos passos. Para o negro, manter a oposição recuando para sul – *e.g.*, indo para f1 na jogada de abertura – pode ser-lhe fatal... *Porquê?*

Propõe-se de seguida uma nova regra de desempate das batalhas reais:

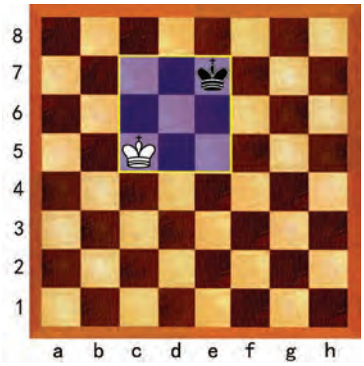
Lei da Terra Queimada. *Em cada partida nenhum rei pode ocupar uma casa que ele ou o seu adversário tenham ocupado anteriormente.*

Na partida do lado esquerdo do diagrama abaixo, a lei da reincidência dá a vitória a quem detém a oposição mas, com a lei da terra queimada vence o rei branco, independentemente de quem joga primeiro; para ganhar, ele pode limitar-se a queimar toda a linha 6 e recuar calmamente para sul, deixando o rei negro a rabiar no reduzido espaço a norte da linha de fogo. Fica a seu cargo, leitor, a discussão da posição acima, à direita.



Deixo para o fim o trabalho mais difícil: tratar posições iniciais em que a oposição não é imediatamente acessível. O diagrama à direita mostra o caso simples de oposição dita "diagonal". A análise é trivial quando a ação decorre no tabuleiro 3×3 marcado na figura: as brancas, aqui com a obrigação de jogar primeiro, perdem (com qualquer das leis de desempate propostas) se o rei negro se limitar a percorrer os bordos do tabuleiro em movimento "giratório"... Por jogarem primeiro, as brancas também se afogam primeiro. Será que esta desvantagem também se faz sentir no tabuleiro 8×8? Do acima dito apenas se extrai a conclusão de que as jogadas de abertura b6 ou d4 serão fatais para as brancas... *Porquê?*

O caso canónico de quando os reis ocupam cantos opostos do tabuleiro fica também em aberto para qualquer das regras de desempate. Num tabuleiro 4×4, por exaustão e força muito bruta, concluí que a lei da terra queimada faz perder quem começa se o outro agir como deve. Mas a lei da reincidência, que dá mais liberdade aos dois reis, ficou de fora. Haja um leitor que ajude!



NOTA BIBLIOGRÁFICA

O leitor pode ver mais sobre a sucessão de Prouhet-Thue-Morse-Euwe na fabulosa "The On-Line Encyclopedia of Integer Sequences", *http://oeis.org/A010060* (visto em 25 de abril de 2013).

[1] Para quem não conhece: o rei é obrigado, em cada jogada, a mover-se para uma das casas adjacentes àquela em que se encontra, mas é-lhe interdito colocar-se numa casa adjacente à que o rei adversário ocupa.

Fabio Chalub
Universidade Nova de Lisboa
chalub@fct.unl.pt

MACACOS ME MORDAM!

Um recente experimento mostra que os sentimentos de equidade e de justiça não são exclusivo dos seres humanos. Experimentos com macacos servem, por um lado, para compreendermos nossas origens — afinal são os nossos primos, e não estão tão distantes assim; por outro lado, serão a motivação de hoje para discutir alguns conceitos centrais de Teoria de Jogos.

Temos, nós e os chimpanzés, uma longa história comum. Nas escalas de tempo da evolução, a separação das duas linhagens foi anteontem. Assim, é natural supor que estudando os primatas em geral podemos ter algumas indicações das nossas origens e, por extensão, de quem, de facto, nós somos. Uma questão central quando olhamos para nós mesmos é o sentido de igualdade na nossa relação com os nossos semelhantes. Para podermos quantificá-lo, seguiremos uma estratégia simples: primeiro, devemos estimar o comportamento na ausência deste sentido, e, a seguir, devemos verificar experimentalmente (e de forma quantitativa) se é isso que efetivamente ocorre. Em caso negativo, é importante perceber o que é que exatamente faz com que nos desviemos do comportamento estimado. Assim compreendemos um pouco da nossa própria origem, aquilo que nos faz humanos.

A Teoria de Jogos modela o comportamento quando são necessárias decisões estratégias. Um jogo é constituído por três elementos: um conjunto de jogadores, um conjunto de estratégias acessíveis a cada jogador e o prémio que cada um obtém após as suas decisões serem anunciadas. O resultado do jogo (ou seja, o prémio) pode depender de forma complexa das decisões de todos os jogadores envolvidos. É disto que vem toda a sua sofisticação matemática. De facto, a Teoria dos Jogos foi criada por um dos maiores matemáticos do século XX, o húngaro-americano John von Neumann (fig. 1), que queria modelar o comportamento humano em jogos de cartas, como, por exemplo, o póquer. Neste caso, cada um tem uma mão de cartas e deve decidir se as troca, no todo ou em parte, sem saber as mãos dos adversários. O resultado dependerá de todas as mãos restantes (e, portanto, de todas as decisões estratégicas possíveis). Evidentemente, há um enorme fator aleatório envolvido, mas isto não é problema para a sua descrição, que neste caso leva em conta as diferentes probabilidades.

Após os trabalhos pioneiros de von Neumann, a Teoria de Jogos foi aplicada ao estudo do comportamento económico, num trabalho famoso do mesmo matemático com o economista austríaco Oskar Morgenstern. Mas a grande viragem conceptual aconteceu na tese de doutoramento do matemático norte-americano John Nash (ver fig. 1). Considerou este que cada um dos jogadores age somente motivado pelo seu autointeresse. Assim, dadas as estratégias dos outros jogadores, cada jogador escolhe a estratégia que maximiza para si o resultado do jogo (chamado *ganho*), sem nenhuma preocupação com as consequências desta decisão para os outros. Esta hipótese é conhecida como *racionalidade* (uma má escolha de nome, sem dúvida). Usando teorias de ponto fixo (um ramo ainda muito ativo da matemática), foi capaz de provar que, em condições muito gerais, há sempre um conjunto de estratégias (uma para cada interveniente) tal que *cada um maximiza o seu ganho, na hipótese de que todos os outros fazem o mesmo*.

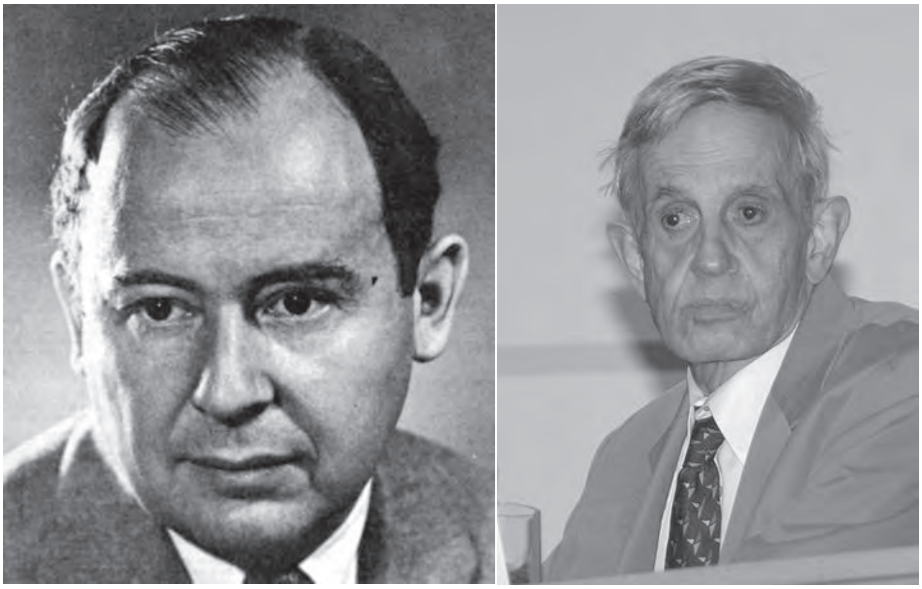


Figura 1: John von Neumann, à esquerda, e John Nash, à direita: duas figuras centrais na Teoria de Jogos. O primeiro criou a Teoria de Jogos; o segundo introduziu o conceito de racionalidade na teoria, dando-lhe uma forma moderna. Fonte: Wikimedia Commons.

Este conjunto de estratégias é conhecido como "o equilíbrio de Nash" e é o que podemos esperar quando agentes racionais interagem entre si.

Assim, já temos um modelo matemático que nos diz o que é podemos esperar quando ninguém pensa em nada a não ser em si próprio. Pensando em várias situações que cada um de nós já viveu, é claro que nem toda a interação humana é desta forma. Existem desvios do equilíbrio de Nash; isto é uma forte evidência de que a preocupação com o próximo é importante naquilo que fazemos. É claro que o nível de preocupação depende da "proximidade do próximo". Preocupamo-nos mais com os filhos, os pais e os irmãos do que com quem nunca vimos antes.

O próximo passo é desenhar jogos, no sentido acima, que nos permitam quantificar o desvio do equilíbrio de Nash. Um dos mais famosos é conhecido como o *jogo do ultimato*: dois jogadores, um na função de proponente, outro com poderes de aceitar ou não a proposta, têm de entrar em acordo sobre a divisão de 10 euros (em números inteiros). O primeiro propõe uma divisão, que o outro aceita ou não. Supondo um segundo jogador racional, então este há de aceitar qualquer oferta não nula (qualquer oferta é melhor do que nada); sabedor disto, o primeiro jogador oferece o mínimo possível. O resultado esperado (que é um dos possíveis equilíbrios de Nash do jogo) é uma oferta mínima do primeiro jogador que é aceite pelo segundo.

Não é isto que ocorre quando este jogo é feito com seres humanos reais. Mesmo em situação de anonímia (ou seja, não se sabe quem fez a oferta e quem a recusou ou não), as ofertas são muito superiores ao mínimo. Isto é verdade em todas as culturas investigadas, apesar de os valores precisos dependerem muito fortemente dos grupos estudados.

Há um interveniente importante nestes jogos: não sabemos se o outro é efetivamente um jogador racional ou se gosta de acender charutos com notas de 100 euros. Portanto, por medo da recusa, é natural que sejam feitas ofertas mais generosas.

Uma variante do jogo do ultimato lida com esta situação. É conhecida como o *jogo do ditador*: o primeiro participante faz a divisão e pronto! O segundo não tem nada a dizer sobre isso. Neste caso, o equilíbrio de Nash é dado pelo primeiro jogador, ficando com os dez euros para si. Mais uma vez, não é isto que ocorre, sendo as ofertas típicas da ordem de 20% a 30% do dinheiro envolvido.

Há alguma coisa que nos faz desviar da racionalidade. Há uma preocupação efetiva em não ser forreta. Será isto exclusivamente humano?

É isto que uma equipa interdisciplinar sedeado nos Estados Unidos, liderada pelo famoso primatologista Frans de Waal, investigou, fazendo com que chimpanzés jogassem o jogo do ultimato e do ditador [1]. Foram colocados dois macacos e um deles deveria escolher um de dois bastonetes. Na primeira escolha, uma divisão de comida equitativa era oferecida; caso fosse

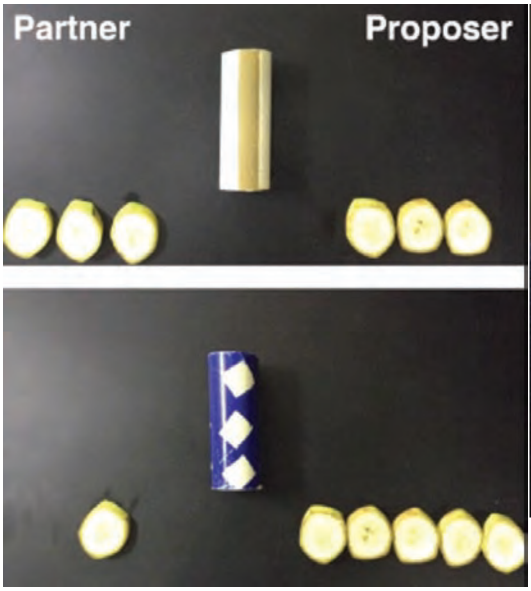


Figura 2: À esquerda, as duas divisões possíveis da comida (bananas, é claro!), em cima, um dos chimpanzés participantes. Imagens gentilmente cedidas por Yerkes National Primate Research Center (*http://www.yerkes.emory.edu/*) e pela equipa de autores.

escolhida a segunda opção, então duas porções de fruta profundamente desiguais eram colocadas à disposição dos símios, sendo que o primeiro ficava com a maior porção. No jogo do ultimato, para que ambos tivessem acesso a comida, qualquer que fosse a divisão escolhida, era necessário que o segundo macaco pressionasse uma alavanca. Se isto não fosse feito em 30 segundos, interpretava-se como uma rejeição àquela divisão. No jogo do ditador, esta última parte era suprimida. Veja a figura 2 e veja também um interessante video em *http://www.emory.edu/LIVING_LINKS/av/ug_2013_narration.mov*.

Há algumas diferenças óbvias em relação aos jogos com pessoas. Para começar, para o *homo sapiens*, o ato de rejeitar é ativo (diz-se "não"). Por outro lado, a reação de um macaco ao estímulo visual da comida é muito intensa, muito maior do que o usual em experimentos com humanos, onde é usado dinheiro (valores que podem oscilar entre o simbólico e o equivalente a alguns meses de rendimentos mensais, sem grande impacto nos resultados). Mas a grande questão técnica é a de saber se as regras do jogo foram compreendidas. Para isso é comum nestes experimentos fazer aquilo a que se chama "pré-testes", selecionando noutros experimentos quais os macacos que conseguem perceber o funcionamento da máquina e o significado dos bastonetes. Muitos chumbam nesta fase e não participam no jogo a sério. De facto, apenas quatro foram selecionados para participar no experimento.

E o que é que a equipa de Waal encontrou? Em primeiro lugar, que as ofertas nos jogos do ultimato são consistentemente mais altas do que as ofertas no jogo do ditador. Este é exatamente o padrão dos seres humanos, mostra que o medo da recusa da outra parte em cooperar pela obtenção de comida é um importante motivador do comportamento. No entanto, em nenhum experimento houve recusa, mostrando que o comportamento, pelo menos do segundo jogador, era racional (tal como discutido acima). Nisto, foram diferentes dos humanos.

No entanto, no mesmo trabalho foi feita uma investigação com crianças, usando um aparato semelhante. Neste caso, também um comportamento racional de quem recebe foi encontrado, assim como propostas mais equitativas no jogo do ultimato em relação ao jogo do ditador.

Uma vez mais, o nosso parentesco com os outros primatas parece confirmar-se: desta vez, no sentido de ética e justiça.

REFERÊNCIAS

[1] Darby Proctor, Rebecca A. Williamson, Frans B. M. de Waal, and Sarah F. Brosnan "Chimpanzees Play the Ultimatum Game" *Proc. Natl. Acad. Sciences* 110 (6) 2070-2075 (2013).

Combinatória, Zonogonos e Zonoedros

Ilda Perez da Silva
Universidade de Lisboa
isilva@cii.fc.ul.pt

1. INTRODUÇÃO

Neste artigo consideramos uma classe de polígonos e de poliedros convexos, com propriedades de simetria particulares: os zonogonos e os zonoedros. São figuras centralmente simétricas e as suas faces são também centralmente simétricas. Os resultados que veremos a seguir sobre zonogonos e zonoedros, apesar do seu carácter elementar permitem ilustrar diversos resultados, algumas surpresas e até questões em aberto na área da geometria combinatória/topologia.

Zonogonos e zonoedros são os exemplos em dimensão 2 e 3 de poliedros convexos n-dimensionais conhecidos por zonotopos. As propriedades de incidência das faces dos zonotopos estão intimamente relacionadas com certas abstrações combinatórias e topológicas de espaços vectoriais reais – os matroides orientados. A "existência" destes objetos combinatórios foi prevista por J. T. Rockafellar, num artigo de 1969, como a estrutura que permitiria unificar determinados resultados de Teoria de Grafos e de Convexidade.

Cerca de 10 anos mais tarde, em 1978, apareciam, no *Journal of Combinatorial Theory* (série B), os dois artigos fundadores do que hoje é a Teoria de Matroides Orientados: um de Robert Bland e Michel Las Vergnas [3] com axiomaticas motivadas diretamente por trabalhos na Teoria de Grafos e de Convexidade, e o outro de Jon Folkman e Jim Lawrence [6] em que os mesmos objetos são apresentados como objetos topológicos: certo tipo de esferas combinatórias. O livro [2] é uma introdução muito completa aos primeiros 20 anos da teoria, que tem sido explorada recentemente em novas direções e aplicações.

Neste artigo, os matroides orientados são motivados com a necessidade de estender o conceito de zonoedro de modo a poder considerar todas as decomposições de zonogonos em paralelogramos como objetos análogos: algumas destas decomposições, mas não todas, são projeções de zonoedros. Todas são projeções de matroides orientados ou pseudo-zonoedros.

Este ponto de vista é mais recente, apareceu na década de 90 do século passado e tem fortes contributos em [9], [4], [10].

Apresentamos algumas propriedades de polígonos e poliedros com fortes propriedades de simetria central, numa introdução elementar a áreas de investigação atuais: matroides orientados, estudo combinatório e topológico do grupo simétrico.

2. ZONOGONOS E ZONOEDROS

Um zonogono é um polígono convexo com centro de simetria. A simetria central obriga a que cada aresta tenha uma aresta oposta, paralela e com o mesmo comprimento. Em particular, um zonogono tem um número par de lados. Chamamos n-zonogono a um zonogono com $2n$-arestas.

Dos polígonos representados na figura seguinte, apenas o segundo e o quarto são zonogonos. O primeiro não tem simetria central e o terceiro não é convexo.

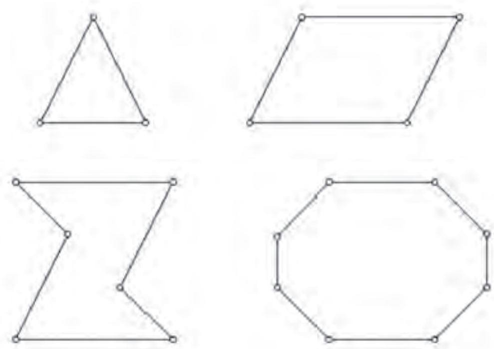


Figura 1: Quais são zonogonos?

A fronteira de um n-zonogono Z é a linha poligonal fechada, $\delta Z = (a_1, \ldots, a_n, a'_1, \ldots, a'_n)$, descrita pela sequência de $2n$ arestas, que vamos encontrando ao percorrer a fronteira δZ começando num vértice e seguindo no sentido dos ponteiros do relógio (ou no sentido contrário!), ver a figura 2. Repare que os pares $\{a_i, a'_i\}$ correspondem a pares de arestas opostas: cada uma das arestas do par é a imagem da outra pela simetria central do zonogono.

Removendo um par de arestas opostas que, sem perda de generalidade, podemos supor ser o par a_n, a'_n, a fronteira do zonogono fica decomposta em duas linhas poligonais disjuntas, cada uma a união de $(n-1)$ arestas do zonogono, $\mathcal{A} = \{a_1, \ldots, a_{n-1}\}$ e $\mathcal{A}' = \{a'_1, \ldots, a'_{n-1}\}$. $\mathcal{A}$ e $\mathcal{A}$ são a imagem uma da outra pela simetria central do zonogono.

Se projetarmos o zonogono Z numa reta r ortogonal à direção definida pelas arestas a_n, a'_n, obtém-se um segmento de reta $[P, P']$ cujos extremos P e P' são as projeções na reta r das arestas a_n e a'_n, respetivamente. As linhas poligonais $\mathcal{A}$ e $\mathcal{A}'$ projetam-se, cada uma, numa decomposição do segmento de reta $[P, P']$ em $(n-1)$ segmentos de reta. O zonogono inicial pode ser reobtido "*levantando*" convenientemente qualquer uma destas decomposições do segmento de reta $[P, P']$.

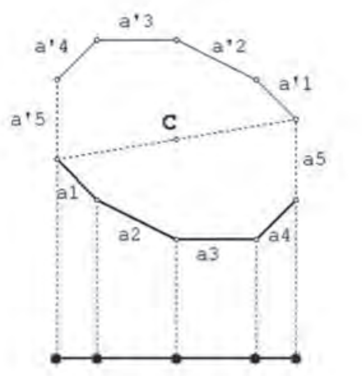


Figura 2: Zonogonos e decomposições de segmentos de reta.

Não é díficil mostrar (descreva um processo geral para o fazer!) que *qualquer que seja a decomposição de um segmento de reta em* $(n-1)$ *segmentos, ela pode ser "ortogonalmente levantada" a um n-zonogono com um par de lados opostos ortogonais ao segmento de reta dado.*

Veremos agora como estas observações sobre zonogonos se generalizam a uma classe particular de poliedros convexos: os zonoedros.

Um zonoedro é um poliedro convexo, centralmente simétrico, cujas faces são polígonos centralmente simétricos, isto é, cujas faces são zonogonos.

Na figura 3 estão representados alguns zonoedros.

Devido às simetrias centrais, quer do poliedro quer das suas faces, as direções de arestas de um zonoedro definem *zonas*. A zona definida por uma aresta a é a união de todas as faces do zonoedro que têm arestas com a direção de a. Esta união de faces constitui uma "passadeira fechada de faces" que divide a superfície do poliedro em dois conjuntos de faces disjuntos: $\mathcal{F}$ e $\mathcal{F}'$ sendo um deles a imagem do outro pela simetria central do zonoedro.

Chamamos n-zonoedro a um zonoedro com n-zonas, que tem arestas em exatamente n-direções.

A projeção de um n-zonoedro $\mathbf{Z}$ num plano ortogonal a uma aresta a é um $(n-1)$-zonogono (ver figura 4). A fronteira desse zonogono é a projeção da zona da aresta a. Qualquer dos conjuntos opostos de faces $\mathcal{F}$ e $\mathcal{F}'$ se projeta numa decomposição desse zonogono em zonogonos.

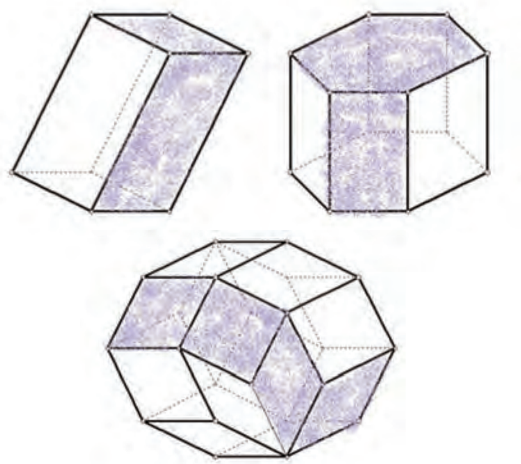


Figura 3: Exemplos de zonoedros com uma zona assinalada.

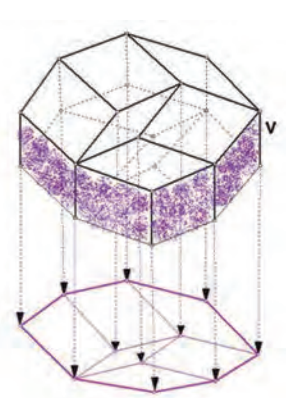


Figura 4: Projetar um zonoedro ortogonalmente a uma zona.

À semelhança do que se passa com as decomposições de um intervalo em n intervalos, é natural pretender descrever um processo geral que permita "levantar a um (n+1)-zonoedro" qualquer decomposição de um n-zonogono em zonogonos. Não vou pedir-lhe que o faça. Não é sempre possível fazê-lo! *Há decomposições de um zonogono com zonogonos que não podem ser levantadas a um zonoedro.* Na figura 5 está representada uma decomposição que não pode ser levantada a um zonoedro.

Havendo, pois, mais decomposições de um zonogono em zonogonos do que aquelas que se obtêm como projeções de zonoedros, que novos objetos são estes que parecem tão próximo de projeções de zonoedros? São projeções de "pseudo-zonoedros" ou matroides orientados de dimensão 3.

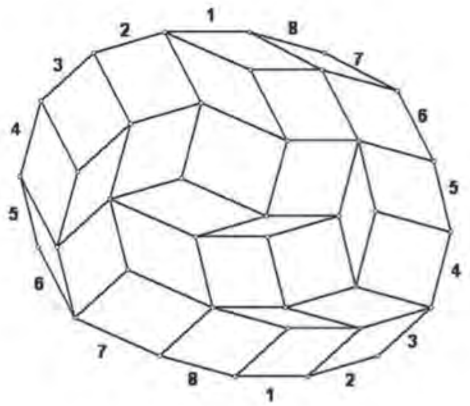


Figura 5: Decomposição que não pode ser "levantada" a um zonoedro.

Estes "pseudo-zonoedros" são objetos combinatórios que podem ser descritos de várias maneiras. Uma delas baseia-se no facto de que os vértices de um n-zonoedro com centro de simetria C se escrevem na forma:

$$V = C + \sum_{i=1}^{n} \epsilon_i v_i,\ \epsilon_i \in \{-1, 1\}$$

onde os vetores v_i definem as direções das arestas. Este facto permite identificar os vértice do zonoedro com um subconjunto $\mathcal{W}$ de n-sequências de $\pm 1's$.

Como saber, dado um conjunto $\mathcal{W} \subseteq \{-1, 1\}^n$ de n-sequências de $\pm 1's$, se ele corresponde, ou não, aos vértices de um zonoedro? As mais fortes condições conhecidas [10] definem matroides orientados – que podem ver-se como pseudo-zonoedros.

Saber se um pseudo-zonoedro é ou não um zonoedro ou se uma decomposição de um zonogono em zonogonos pode ser levantada a um zonoedro são problemas equivalentes, classificados de *NP*-difíceis, isto é, para os quais, embora haja algoritmos de decisão, mesmo o mais poderoso dos computadores poderá não conseguir dar a resposta em tempo útil.

Concluímos esta secção com a descrição de uma família importante de decomposições de um n-zonogono: as decomposições cíclicas, $\mathcal{C}_n$, que correspondem a projeções de um zonoedro, o "zonoedro cíclico com n+1 zonas". São descritas por indução em n: começando num paralegramo (2 zonas) e acrescentando de cada vez uma nova zona, como indicado na figura 6.

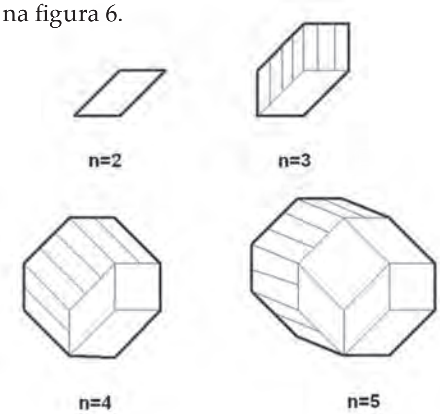


Figura 6: Decomposições cíclicas de n-zonogonos.

Deixamos como exercício ao leitor determinar os números de vértices, arestas e paralelogramos de (um)a decomposição cíclica $\mathcal{C}_n$ de um n-zonogono. Este resultado é fundamental para estimar o número de jogadas do jogo L'OZ, que apresentamos de seguida.

3. DECOMPOSIÇÕES DE ZONOGONOS EM PARALELOGRAMOS

A relação entre matroides e decomposições foi muito explorada na década de 1990, [9], [4] e [10]. Alguns desses resultados podem ser implementados na forma de um jogo/*puzzle* que descrevemos nesta secção.

Em 2007, um grupo de alunos de Engenharia Informática da Faculdade de Ciências de Lisboa implementou um protótipo desse jogo, ainda disponível em *http://labmag.di.fc.ul.pt/virtual/LOZ/*. Para detalhes sobre a implementação propriamente dita deve consultar [5].

O jogo consiste no seguinte:

No ecrã aparecem duas decomposições diferentes de um mesmo zonogono com paralelogramos (LOZangos), como na figura 7.

O objetivo do jogo é transformar a decomposição inicial (da esquerda) na decomposição final (da direita) através de uma sequência apropriada de jogadas. Cada jogada consiste em clicar num vértice interior de grau 3 na decomposição da esquerda, o que muda a posição relativa dos três paralelogramos que contêm o vértice de grau 3 da forma representada na figura 8.

Do ponto de vista matemático, o jogo está completamente estudado. Sabemos responder, e a resposta é afirmativa, às perguntas seguintes:

1. Podem ser escolhidas quaisquer duas decomposições para decomposições inicial e final ou há que ter algum cuidado?
2. Existem estratégias para jogar? E são eficazes?

As respostas a ambas as questões baseiam-se no seguinte resultado:

Teorema *Dados um n-zonogono Z e uma sua decomposição em paralelogramos, $\mathcal{Z}$, fixemos um vértice O da fronteira de Z e seja O' o vértice oposto. Identifiquemos de forma habitual a fronteira de Z: $\delta Z = (a_1, \dots, a_n, a'_1, \dots a'_n)$ e seja $L = (a_{i_1}, \dots, a_{i_n})$ uma qualquer linha poligonal simples (que não repete arestas nem vértices) da decomposição unindo também O a O'. Então:*

1. É sempre possível levar a linha poligonal $L_0 = (a_1, \dots, a_n)$ a coincidir com a linha $L = (a_{i_1}, \dots, a_{i_n})$, ***passando um lozango da decomposição*** $\mathcal{Z}$ ***de cada vez****, ver figura 9.*

2. Seja qual for a decomposição $\mathcal{Z}$, existe uma estratégia para transformar a decomposição cíclica $\mathcal{C}_n$ em $\mathcal{Z}$ usando no máximo $\binom{n}{3}$ jogadas.

A demonstração de 1) é deixada ao cuidado do leitor mais interessado. Ela foi feita pela primeira vez, noutros termos, por G. Ringel [7] em 1958. A demonstração dada em [9], por indução em n, é construtiva, fornecendo, em simultâneo, uma estratégia para o jogo e uma estimativa para o número máximo de jogadas necessário.

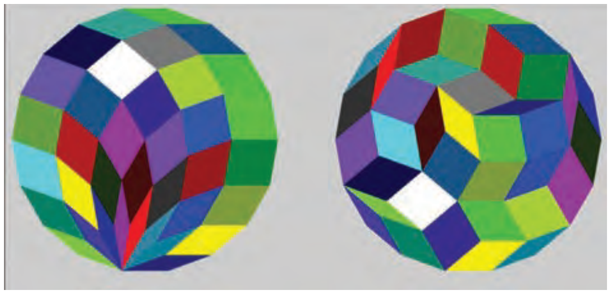
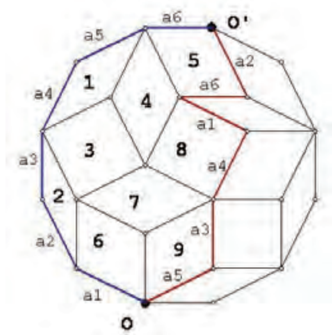


Figura 7: Uma posição inicial de L'OZ.

Figura 8: Uma jogada de L'OZ.



Uma linha "passa um paralelogramo P" quando contém duas arestas de P e essas arestas são substituídas pelas arestas opostas de P.

Pode fazer-se coincidir a linha azul com a encarnada passando os 9 paralelogramos numerados, um de cada vez, pela ordem indicada.

Figura 9

Repare que para $n = 2$, o 2-zonogono é um paralelogramo e a decomposição cíclica $\mathcal{C}_2$ é a única pavimentação.

Para $n = 3$ (ver figura 8) há exatamente duas decomposições em paralelogramos possíveis e uma obtém-se da outra com um clique no único vértice interior.

Exemplificamos agora o passo de indução, mostrando como se joga com $n = 4$, sabendo jogar com $n = 3$.

Considere-se a decomposição cíclica $\mathcal{C}_4$ e uma outra decomposição em paralelogramos, $\mathcal{Z}$, de um 4-zonogono. Ver figura 10.

Removendo a zona 4 de ambas as decomposições. Obtém-se (fig. 10 ao centro) de um lado $\mathcal{C}_3$ e do outro a restrição $\mathcal{Z}_3$, de $\mathcal{Z}$ ao mesmo hexágono regular. Pelo caso anterior, $n = 3$,

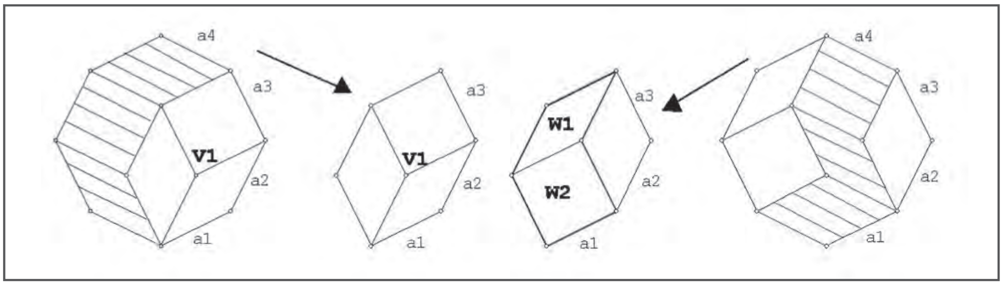


Figura 10

sabemos tranformar (no máximo, com uma jogada) C_3 em $\mathcal{Z}_3$. Seja $\mathcal{C}_4'$ o arranjo obtido de $\mathcal{C}_4$ em que C_3 é substuído por $\mathcal{Z}_3$.

Para levar $\mathcal{C}_4'$ a coincidir com $\mathcal{Z}$, basta levar a zona 4 de $\mathcal{C}_4'$ a coincidir com a zona 4 de $\mathcal{Z}$. Em Z_3 ambas as zonas são representadas por duas linhas quebradas simples unindo o mesmo par de vértices opostos de $\mathcal{Z}_3$ (figura 10 ao centro), e a parte 1 do teorema anterior garante que podemos levar uma a coincidir com a outra passando um paralelogramo de cada vez, isto é, no máximo em três jogadas (no caso da figura 10 em duas jogadas).

Gastaremos assim, no caso geral, para $n = 4$, no total, um máximo $1 + 3 = \binom{4}{3}$ jogadas para transformar $\mathcal{C}_4$ numa qualquer decomposição $\mathcal{Z}$ do mesmo zonogono.

Repare que, se sabemos que $\binom{n}{3}$ jogadas são suficientes para transformar a composição cícica $\mathcal{C}_n$ numa qualquer decomposição $\mathcal{Z}$ do mesmo n-zonogono, então gastaremos no máximo $2 \times \binom{n}{3}$ jogadas para transformar qualquer decomposição $\mathcal{Z}$ numa outra $\mathcal{Z}'$ (passando primeiro de $\mathcal{Z}$ para $\mathcal{C}_n$ e depois de $\mathcal{C}_n$ para $\mathcal{Z}'$). O número máximo de jogadas necessário para concluir qualquer jogo é, pois, polinomial em n (da ordem de n^3). Isto significa que o algoritmo para jogar o jogo tirado da demonstração é eficiente.

4. OBSERVAÇÕES FINAIS

Vimos como os matroides orientados permitem descrever de forma semelhante objetos análogos – as decomposições de zonogonos em zonoedros.

Vimos depois como relacionar através de uma operação simples – clicar num vértice de grau 3 – duas quaisquer decomposições de zonogonos.

A extensão destes resultados a dimensões mais altas não está ainda totalmente percebida.

Para concluir, chamamos a atenção para o facto de que, como consequência do teorema da secção anterior, uma decomposição de um n-zonogono em paralelogramos pode identificar-se (como sugere a figura 9) com uma sequência de permutações que leva de $e = 123\ldots n$ a $e' = n(n-1)\ldots 21$, passando um paralelogramo de cada vez, o que corresponde a dizer invertendo a posição dos números em dois lugares consecutivos de cada vez.

Deste ponto de vista, os matroides orientados aparecem no contexto de estudo das propriedades topológicas e combinatórias do grupo simétrico, e mais geralmente dos Grupos de Coxeter. Para uma introdução recente da investigação nesta área consulte [1].

REFERÊNCIAS

[1] A. Björner, F.Brenti, "Combinatorics of Coxeter Groups", *Graduate Texts in Matehematics* 231, Springer 2005.

[2] A. Björner, M. Las Vergnas, B. Sturmfels, N. White, G. Ziegler, "Oriented Matroids", *Encyclopedia of Mathematics and its Applications* 46, 2nd edition, Cambridge University Press 1999.

[3] R.Bland and M. Las Vergnas, "Orientability of Matroids", *J. Combinatorial Theory*, Ser. B, 24 (1978), 94-123.

[4] J. Bohne, "Eine Kombinatorische Analyse zonotopaler Raumaufteilungen", PhD thesis, Univ. Bielefeld, 1992.

[5] A. P. Cláudio, I. Perez da Silva, N. Pinto, N. Prelhaz, J. Soares, "Implementing L'OZ, Proceedings of Recreational Mathematics" 09, Évora 2009.

[6] J. Folkman, J. Lawrence, "Oriented Matroids", *J. Combinatorial theory*, Ser.B, 25, 199-236.

[7] G. Ringel, "Teilungen der Ebene durch Geraden oder Topologische Geraden", *Math.Z.* 64 (1956), 79-102.

[8] R. T. Rockafellar, "The elementary vectors of a subspace of $\mathbb{R}^n$, Proceedings of the Conference Combinatorial Mathematics and its Applications", Chapel Hill, North Carolina, 1969.

[9] I. P. F. da Silva, "On Fillings of $2n$-gons with Rhombi", *Discrete Math.* 111(1993), 137-144.

[10] I. P. F. da Silva, "Axioms for Maximal Vectors of an Oriented Matroid, a Combinatorial Characterization of the Regions of a Pseudo-hyperplane Arrangement", *Europ. J. Combinatorics* 16 (1995), 125-145.

SOBRE A AUTORA

Ilda Perez da Silva, doutorada pela Universidade de Paris VI, é professora de Matemática na Faculdade de Ciências da Universidade de Lisboa e membro do Centro de Estruturas Lineares Combinatórias. O seu trabalho científico situa-se na área da Combinatória. Interessa-se também por História da Matemática, em particular pelo período dos anos 40 do século XX em Portugal.

António Machiavelo
Universidade do Porto
ajmachia@fc.up.pt

DÍZIMAS PERIÓDICAS E UMA CONJETURA DE EMIL ARTIN

Sabe o leitor que 0,99999999999 ... = 1? E porquê? Supondo, é claro, que as reticências significam que os noves não terminam... E sabe que o período da dízima que representa $\frac{1}{p}$, sendo p um número primo, é um divisor de $p-1$? E que há ainda problemas em aberto sobre as dízimas que representam números racionais?

Quando um número racional é expandido em dízima, três coisas diferentes podem ocorrer, como é ilustrado pelos exemplos seguintes:

$$\frac{1}{8} = 0,125 \quad ;$$

$$\frac{1}{7} = 0,142857\,142857\,142857\ldots \quad ;$$

$$\frac{1}{6} = 0,16666666\ldots .$$

A primeira dízima é finita, ao passo que as outras duas são infinitas periódicas, mas na segunda o período – a parte que se repete *ad infinitum* – tem início imediatamente a seguir à vírgula decimal, enquanto na terceira tal não acontece. Diz-se que a segunda é *periódica pura*, enquanto a terceira é *periódica mista*.

De forma a tornar a representação mais compacta e clara, é usual indicar o período colocando-o entre parêntesis. Por exemplo, $\frac{1}{7} = 0,(142857)$. Aqui ficam mais dez exemplos:

$\frac{1}{11} = 0,(09)\,;$ $\quad\frac{1}{13} = 0,(076923)\,;$

$\frac{1}{17} = 0,(0588235294117647)\,;$ $\quad\frac{1}{101} = 0,(0099)\,;$

$\frac{2}{13} = 0,(153846)\,;$ $\quad\frac{3}{17} = 0,(1764705882352941)\,;$

$\frac{19}{20} = 0,95\,;$ $\quad\frac{19}{27} = 0,(703)\,;$

$\frac{1}{28} = 0,03(571428)\,;$ $\quad\frac{443}{520} = 0,851(923076)\,.$

Não é difícil ver que a expansão em dízima de um número racional é necessariamente periódica (considerando as finitas como tendo período constituído pelo algarismo 0) e que, reciprocamente, todo o número representado por uma dízima periódica é um número racional. A primeira afirmação resulta facilmente do que é feito no algoritmo da divisão, como abaixo veremos, enquanto a segunda resulta de uma simples técnica para converter uma dízima periódica numa fração, que se ilustra aqui com um exemplo, o da dízima 1, 8(43). O primeiro passo é dar um nome ao número correspondente: r, por exemplo. De seguida, multiplica-se a dízima pela potência de 10 que faça com que o período se inicie logo após a vírgula (se tal for já o caso, essa potência é 10^0), e depois pela potência necessária para trazer um período inteiro para a esquerda da vírgula:

$$\begin{aligned} 10\,r &= 18,43\,43\,43\ldots \\ 10^3\,r &= 1843,43\,43\,43\ldots \quad . \end{aligned}$$

Daqui resulta:

$$10^3\,r - 10\,r = 1825,$$

portanto $(10^3-10)\,r = 1825$ ou seja, $r = \frac{1825}{990} = \frac{365}{198}$.

Quando se aborda este assunto da representação em dízima, deve observar-se que tal representação nem sempre é única. Mais precisamente, as dízimas finitas têm também uma representação infinita, que se obtém retirando uma unidade ao dígito mais à direita e acrescentando a seguir a ele uma infinidade de noves. Por exemplo: 1, 25 = 1, 24(9).

Isto pode ser visto aplicando a técnica acabada de descrever à dízima 1,24(9). Já agora, o mesmo procedimento pode ser aplicado para ver que 0, (9) = 1. No entanto, deve o leitor ficar informado de que o porquê exato por detrás destas igualdades passa por saber o que são exatamente os números reais e qual o significado preciso de uma dízima infinita, para o que se recomenda, como ponto de partida, a página *http://en.wikipedia.org/wiki/Construction_of_the_real_numbers* e as referências aí contidas.

Um facto curioso é que o tamanho do período da dízima de uma fração irredutível (em que o máximo divisor comum do numerador e do denominador é 1) depende apenas do denominador. Para ver que assim é, basta perceber o que é feito quando se usa o algoritmo de divisão habitual para expandir uma fração irredutível $\frac{a}{b}$ ($a, b \in \mathbb{Z}$, $b \geq 2$, $\operatorname{mdc}(a, b) = 1$) em dízima. Ora, esse algoritmo é simplesmente um procedimento para determinar os números inteiros $q, q_1, q_2, q_3, \ldots$ tais que:

$$\begin{aligned} a &= b\,q + r_0 \\ 10\,r_0 &= b\,q_1 + r_1 \\ 10\,r_1 &= b\,q_2 + r_2 \\ &\cdots \\ 10\,r_n &= b\,q_{n+1} + r_{n+1} \\ &\cdots \end{aligned} \tag{1}$$

com $0 \leq r_n < b$ para todo $n \in \mathbb{N}_0$. A multiplicação por 10 corresponde a "baixar um zero" no algoritmo que se aprende no ensino básico[1].

Como $0 \leq r_n < b$, tem-se que $0 \leq 10\,r_n < 10\,b$ e, por conseguinte, $0 \leq q_{n+1} < 10$. Ou seja, q_n é um dígito (um número de 0 a 9) para todo $n \geq 1$. De (1) resulta, sucessivamente, que:

$$\frac{a}{b} = q + \frac{r_0}{b}$$
$$\frac{r_0}{b} = \frac{q_1}{10} + \frac{r_1}{10b}$$
$$\frac{r_1}{10b} = \frac{q_2}{10^2} + \frac{r_2}{10^2 b},$$
$$\ldots,$$

o que mostra que

$$\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \cdots = q, q_1 q_2 q_3 \ldots .$$

Ou seja, (1) realmente determina a dízima de $\frac{a}{b}$, como afirmado.

Vê-se agora porque é que toda a dízima correspondente a um número racional é periódica: como só há um número finito de restos r_k possíveis, estes têm de se repetir, portanto, os q_k também se repetem, periodicamente, a menos que terminem, o que acontece quando algum resto é nulo.

Escrevendo $a \equiv b \pmod{m}$ quando a e b deixam o mesmo resto quando divididos por m, de (1) vem que $10\,r_0 \equiv r_1 \pmod{b}$, $10\,r_1 \equiv r_2 \pmod{b}, \ldots, 10\,r_n \equiv r_{n+1} \pmod{b}$ Mas então, para todo $t, n \geq 0$:

$$r_{n+t} \equiv 10\,r_{n+t-1} \equiv 10^2\,r_{n+t-2} \equiv \cdots \equiv 10^t\,r_n \pmod{b}.$$

Note-se que de $\operatorname{mdc}(a, b) = 1$ resulta que $\operatorname{mdc}(b, r_0) = 1$.

Se $\operatorname{mdc}(b, 10) = 1$, então $\operatorname{mdc}(b, r_n) = 1$ para todo $n \in \mathbb{N}$. Em particular, a dízima é infinita. Se r_n for o primeiro resto a repetir-se, sendo pois $r_{n+t} = r_n$ para algum $t \geq 1$, resulta que $r_n = r_{n+t} \equiv 10^t\,r_n \pmod{b}$. Como $\operatorname{mdc}(r_n, b) = 1$, deduz-se que $10^t \equiv 1 \pmod{b}$ e portanto $r_0 \equiv 10^t\,r_0 \equiv r_t \pmod{b}$. Mas como r_0 e r_n são números positivos menores do que b, conclui-se que $r_0 = r_t$, ou seja, o primeiro resto a aparecer repetido é necessariamente r_0. Daqui se conclui que, no caso em consideração, a dízima é periódica pura. Resulta também que o comprimento do período é igual ao menor inteiro positivo d tal que $10^d \equiv 1 \pmod{b}$. Em particular, $d \mid \varphi(b)$, onde φ é a função de Euler[2].

No caso de se ter $b = 2^\alpha 5^\beta$, para alguns $\alpha, \beta \geq 0$, pondo $n = \max\{\alpha, \beta\}$, tem-se que $b \mid 10^n$. Como $r_n \equiv 10^n r_0 \pmod{b}$, resulta que $r_n = 0$, ou seja, a dízima é finita.

Resta o caso em que $b = 2^\alpha 5^\beta c$, com $\alpha, \beta \geq 0$, $\max\{\alpha, \beta\} > 0$, $\operatorname{mdc}(c, 10) = 1$ e $c > 1$. Pondo $n = \max\{\alpha, \beta\} \geq 1$, tem-se

$$\frac{a}{b} = \frac{2^{n-\alpha} 5^{n-\beta} a}{10^n c}.$$

Pelo primeiro caso, sabemos que

$$\frac{2^{n-\alpha} 5^{n-\beta} a}{c}$$

é puramente periódica e que o comprimento do período é independente de a e igual ao menor inteiro positivo d tal que $10^d \equiv 1 \pmod{c}$. Como dividir por 10^n corresponde a deslocar a vírgula n dígitos para a esquerda, resulta que temos neste caso uma dízima periódica mista (que não é pura, resulta de que se tem $\operatorname{mdc}(b, r_0) = 1$ enquanto $\operatorname{mdc}(b, r_n) > 1$, para todo $n \geq 1$).

Resumindo: a dízima de $\frac{a}{b}$ é puramente periódica, mista ou finita consoante se tenha, respetivamente, $\operatorname{mdc}(b, 10) = 1$, $\operatorname{mdc}(b, 10) \neq 1$ e b tem um fator primo $\neq 2, 5$, ou b não tem nenhum fator primo $\neq 2, 5$. Em particular o tipo de dízima e também o comprimento do período não dependem do numerador.

Do que ficou exposto, conclui-se que, no caso particular das frações da forma $\frac{1}{p}$ com p primo, p o comprimento do período é um divisor de $p - 1$. Determinar que divisor é exatamente é que parece ser difícil. Sabemos que é o menor inteiro positivo d tal que $10^d \equiv 1 \pmod p$, mas a nossa ignorância sobre a relação que tal inteiro tem com o primo p é atestada pelo facto de não se saber se há ou não uma infinidade de primos para os quais tal inteiro é $p-1$. Dito de um outro modo, não se sabe se existe ou não uma infinidade de primos p para os quais o comprimento do período da dízima de $\frac{1}{p}$ é $p-1$, como é o caso de $\frac{1}{17}$ dado acima como exemplo.

Esta última questão prende-se com uma conjetura feita por Emil Artin em 1927, ainda em aberto. Para a descrever, é necessário explicar que um número $a \in \mathbb{Z}$ se diz uma *raiz primitiva* de um primo p se o menor inteiro positivo k tal que $a^k \equiv 1 \pmod p$ para $p-1$. A conjetura de Artin em causa afirma que, se a não for -1 nem um quadrado perfeito, então a é raiz primitiva para uma infinidade de primos. A conjetura inclui ainda uma previsão para a percentagem de primos para os quais a é uma raiz primitiva: cerca de 37,4%. O mais surpreendente é que tal percentagem não depende do número a. Para mais detalhes ver *http://www.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/murty.pdf*. A figura 1 dá, para os primeiros 500, 000 primos, o número e as percentagens daqueles em que os períodos da dízima correspondente a $\frac{1}{p}$ são os nela indicados.

Em 1986 Roger Heath-Brown mostrou, com base em trabalhos de Rajiv Gupta and M. Ram Murty, que há no máximo dois números para os quais a conjetura de Artin é falsa. É um resultado fabuloso. Mas, apesar disso, ainda não se conhece nenhum número para o qual a conjetura seja verdadeira! Em particular, não se sabe se 10 é ou não uma raiz primitiva para uma infinidade de primos, o que se prende com a expansão em dízima das frações $\frac{1}{p}$ com p primo. Não é curioso?

[1] O 10 aparece aqui simplesmente por ser essa a base que usamos para representar números. Tudo o que estamos a descrever se aplica a uma outra qualquer base, trocando apenas o número 10 pelo número correspondente.

[2] Ver *http://www.cut-the-knot.org/blue/Euler.shtml*, assim como *http://www.cut-the-knot.org/blue/Modulo.shtml* e *http://www.cut-the-knot.org/blue/Fermat.shtml*. Em alternativa, consultar *http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/modarith.pdf* e *http://www.math.uconn.edu/~kconrad/ blurbs/ugradnumthy/eulerthm.pdf*

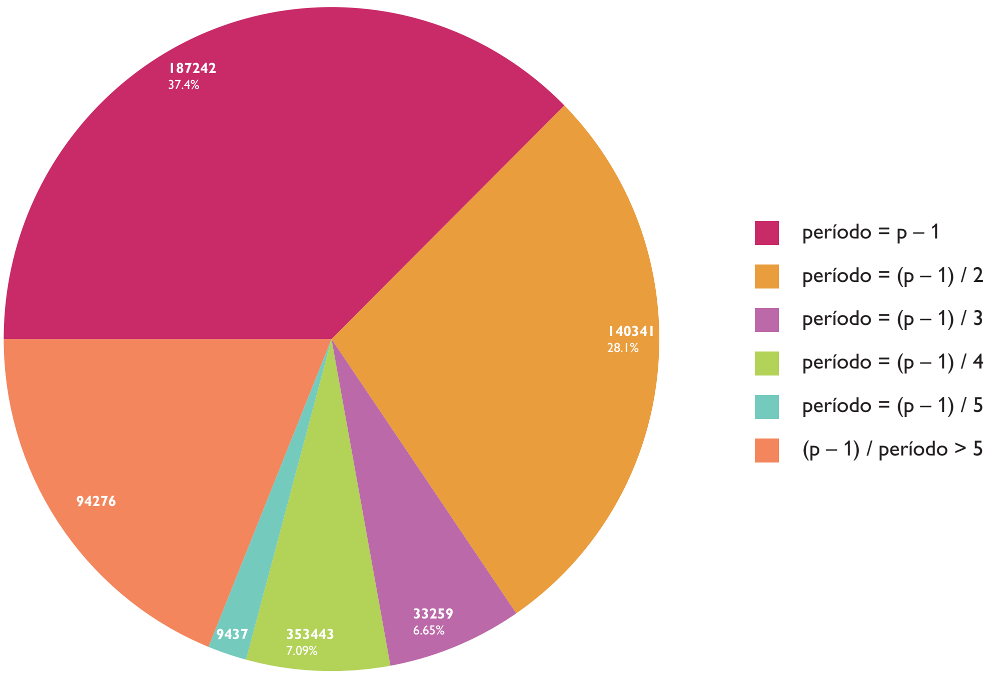


Figura 1: Percentagens de primos tais que a dízima de $\frac{1}{p}$ tem um dado período.

Crie o seu arquivo de exercícios resolvidos parametrizados (Projeto MEGUA)

Pedro Cruz [a], Paula Oliveira [b], Dina Seabra [c]
Universidade de Aveiro
[a] pedrocruz@ua.pt, [b] paula.oliveira@ua.pt, [c] dfcs@ua.pt

INTRODUÇÃO

Muito material, da área da matemática, baseado em ambientes *web* está a ser usado para treino dos alunos, competições ou avaliação, como são exemplos os materiais desenvolvidos nos projetos PMATE [PmatE (2004, 2006, 2010)], AGILMAT [Tomás, A. P et. al. (2008), Costa, R. P. (2003)], e WIMS [Xiao, G. (2004)]. Nestes casos, quando o utilizador gera exercícios, não tem acesso à resolução pormenorizada, tendo nalguns casos acesso à sua solução.

O facto de um aluno poder resolver diferentes exercícios sobre um mesmo tema concreto e, caso deseje, ter acesso à sua resolução, contribui para o seu autoestudo e para a sua autoavaliação.

Já existem vários livros de diferentes áreas de matemática com exercícios resolvidos, mas a construção de bases de dados de exercícios parametrizados vai permitir ao estudante, em diferentes etapas do seu estudo, gerar exercícios de novos tipos, ou do mesmo mas ligeiramente diferentes, e sempre com a respetiva resolução.

Neste artigo apresenta-se o projeto MEGUA, cujo objetivo é a elaboração de bases de dados de exercícios parametrizados e sua resolução, organizadas por classes, usando o *software* Sage Mathematics. Pretende-se que o conjunto de exercícios abranja grande parte dos conteúdos de matemática lecionados nos primeiros anos do ensino superior. O MEGUA pode ser encontrado em *http://code.google.com/p/megua*.

Além disso, a consulta de arquivos de exercícios permite ao docente a rápida elaboração de material didático para apoio às aulas e à avaliação, pois permite gerar diferentes questões sobre o mesmo tópico. Assim, o docente não tem de construir, repetidamente, questões do mesmo tipo.

O QUE É O MEGUA?

MEGUA [MEGUA (2010)] é um sistema que permite a criação de bases de dados de exercícios parametrizados, e respetivas resoluções, em que estes são criados por professores, usando a experiência adquirida ao longo dos anos de lecionação. A geração de novos exercícios ocorre por substituição automática, eventualmente aleatória, de parâmetros por valores numéricos ou funções, extraídos de conjuntos pré-definidos. Este projeto está a ser construído sobre a plataforma Sage Mathematics [Sage Math (2011)].

Anualmente são elaborados exercícios abordando certos tópicos que são resolvidos vezes sem conta por professores e alunos. As dúvidas mantêm-se ao longo dos anos e a questão mais comum é "Como é que se faz?".

Para evitar a repetição sucessiva dos mesmos processos e disponibilizar aos alunos um conjunto de exercícios resolvidos que permita esclarecer as dúvidas comuns foi criado o MEGUA.

O objetivo é o de disponibilizar em rede, quer para professores quer para alunos, um vasto conjunto de exercícios que permita aos alunos aferir os seus conhecimentos e aos professores dê liberdade para investir noutro tipo de problemas e numa preparação de aulas mais eficiente, nomeadamente na criação de mais exercícios ou problemas, textos de apoio e outros meios que implementem o sucesso da aprendizagem.

Cada elemento da base de dados do MEGUA é considerado um "objeto de aprendizagem", que pode ser reutilizado em diversos contextos, como meras folhas de exercícios, jogos, testes, fichas de autodiagnóstico, etc.

Frequentemente, as dificuldades na resolução de um exercício prendem-se não com os conceitos diretamente envolvidos mas com pré-requisitos, como, por exemplo, a manipulação de expressões algébricas.

O detalhe da resolução estará de acordo com o perfil do aluno utilizador, tendo sempre em conta aspetos didáticos do tópico em estudo, contendo justificações dos vários passos dados e referência a alguns dos resultados utilizados para tirar as conclusões adequadas, e aspetos pedagógicos. Por exemplo, um aluno, para aprender a integrar, pode reutilizar exercícios resolvidos do arquivo, relativos à derivação, pois estes funcionam como pré-requisito para a integração.

Atualmente, em Portugal, entram no ensino superior alunos com diferentes percursos académicos, o que leva a que a mesma unidade curricular seja frequentada por alunos com conhecimentos de base bem distintos. Nivelar conhecimentos e ajudar a ultrapassar obstáculos a nível de base de matemática deve ser uma preocupação para os docentes envolvidos em unidades curriculares com este perfil multifacetado.

O facto de acompanhar uma resolução com todos os detalhes explicados ajuda a construir o conhecimento de *baixo para cima*, podendo permitir que uma elevada percentagem de alunos atinja o patamar de aprovação a unidades curriculares para as quais a sua formação anterior era diminuta.

A implementação de um objeto MEGUA passa pela necessidade de três etapas:

- Criação "de autor"
- Programação elementar
- Revisão

Estas etapas devem ser realizadas por pessoas com experiência no ensino, de modo a que a escolha de exercícios e a sua resolução elucidem as dúvidas habituais, permitindo ao estudante prosseguir para exercícios/problemas que exijam um maior grau de conhecimentos.

A experiência permite detetar os problemas comuns dos alunos e, consequentemente, criar conjuntos de exercícios que possam dissipar essas dificuldades.

DESCRIÇÃO E OBJETIVOS DE UM OBJETO DE APRENDIZAGEM MEGUA

Cada exercício pode ser visto como um conceito, geralmente formado por conceitos de base. Por exemplo, um exercício sobre o conceito abrangente de funções trigonométricas pode referir-se apenas a uma das funções trigonométricas, nomeadamente o cosseno. Mas sobre o cosseno poderemos apenas estar a estudar algumas propriedades, como periodicidade, zeros, domínio, contradomínio, restrições para a existência de inversa, derivada, etc.

O projeto MEGUA pretende que se criem vastas bases de dados de exercícios parametrizados e respetivas resoluções, com fins pedagógicos. A organização de uma base de dados desta natureza pressupõe que os exercícios estejam agrupados em classes, cuja utilização e a pesquisa sejam relativamente simples, quer para professores quer para alunos. Para cumprir esta exigência, cada exercício MEGUA é caracterizado por duas etiquetas fundamentais: um número de identificação único e um código que identifica o autor.

Além disso, cada objeto de aprendizagem é descrito por:

- Um sumário (incluindo a catalogação e palavras-chave)
- O texto do enunciado
- O texto da resposta,

tudo criado originalmente num ficheiro de texto LaTeX ou no *notebook* do "Sage Mathematics".

A catalogação dos exercícios deve seguir a classificação MCS 2010 (Mathematics Subject Classification). Por exemplo, um exercício sobre derivadas de funções reais de variável real será catalogado em

26A24 Differentiation (functions of one variable)
general theory, generalized derivatives, mean-value theorems

Para além disso, o autor do exercício caracteriza-o usando algumas palavras-chave e uma breve descrição. Caso se pretenda alterar um exercício, apenas o seu autor poderá fazê-lo, daí que a cada exercício esteja associado o seu autor. No Anexo A, apresenta-se um exemplo em que são visíveis os parâmetros ('on**x1**' e 'on**a**'), e as diferentes secções 'PROBLEM' e 'ANSWER'.

UM ESTUDO DE CASO

A unidade curricular de matemática em muitas licenciaturas, particularmente nas que não estão tão direcionadas para as áreas das ciências, é usualmente um problema e um dos assuntos mais delicados é a trigonometria.

No presente ano letivo, foram fornecidos aos alunos exercícios-tipo e suas resoluções sobre as inversas das funções trigonométricas, nomeadamente arco-seno, arco-cosseno e arco-tangente, como mostra o exemplo apresentado no Anexo B.

Na unidade curricular em causa, os alunos são frequentemente submetidos a uma questão na aula, a qual faz parte do processo de avaliação. Cada aluno teve de resolver um exercício gerado por parâmetros aleatórios análogo aos que foram feitos na aula. O gráfico ao lado ilustra os resultados obtidos numa questão sobre funções trigonométricas inversas, em que N é a nota do aluno, entre 0 e 20 valores. Atendendo ao tópico em avaliação, os resultados foram substancialmente melhores face a anos anteriores, nos quais raramente os alunos obtinham uma classificação positiva neste tópico.

Dos 45% de negativas (13 num total de 29 alunos) é de observar que 31% foram classificações até 5 valores. No nosso entender, estas notas estão, na sua maior parte, associadas a uma desmotivação pela unidade curricular, enquanto as negativas entre 5 e 9, tendo em conta a natureza do tópico em avaliação e o público em estudo, que não tem conhecimentos prévios de trigonometria, demonstram que algumas das aprendizagens verificáveis foram adquiridas.

CONCLUSÃO

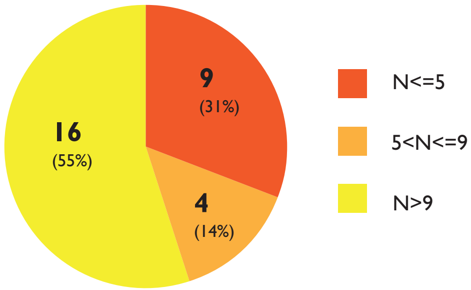
Aprender vendo fazer é uma técnica secular de ensino que tem mostrado ao longo do tempo a sua eficácia. Hoje em dia, com a tecnologia disponível, o aluno pode, ao alcance de um clique, ter uma série de exercícios diferentes e respetivas resoluções, sem necessitar de recorrer sistematicamente ao professor, usando as horas de contacto para questões mais específicas que o impeçam de progredir. O facto de estes exercícios estarem disponíveis permite ao aluno refletir sobre eles e esclarecer efetivamente as dúvidas que ainda persistirem.

No exemplo apresentado, aconteceu por diversas vezes os alunos questionarem na aula apenas algumas passagens da resolução que não entendiam e não a resolução do exercício completo. Esta informação pode ser usada para melhorar a resolução, tentando tornar claras as dúvidas que subsistiram.

Outras situações houve em que o aluno acompanhou a resolução do professor no quadro munido da que lhe tinha sido fornecida, anotando algumas observações que lhe pareceram pertinentes.

O MEGUA, só por si, não constitui uma metodologia de ensino/aprendizagem. É um complemento útil ao autoestudo do aluno e uma ferramenta que permite ao professor investir muito do seu tempo na criação de novos exercícios ou outras iniciativas que promovam uma aprendizagem efetiva dos seus alunos.

RESULTADOS



REFERÊNCIAS

Costa, R. P. (2003) "Geração Automática de Exercícios de Matemática". Tese de Mestrado em Ensino da Matemática. Faculdade de Ciências da Universidade do Porto.

Tomás, A. P., Leal, J. P., Domingues, M. A. (2008) "A Web Application for Mathematics Education". *Springer-Verlag*, LNCS 4823

Xiao, G. (2004). Public-Questions Tests *http://wims.unice.fr/paper/pqt.pdf* (acedido em março de 2011). Exercícios online: *http://wims.unice.fr*

PmatE (2004) "Modelo Gerador de Questões", IADIS Conferência Ibero-Americana WWW-Internet

PmatE (2006) "An Overview of PmatE: developing software for all degrees of teaching", *Proceedings of the International Conference in Mathematics Sciences and Sciences Education*, June 11-14, University of Aveiro.

PmatE (2010) "An old project in education, teaching and learning using new technologies" (aceite para publicação em Proceedings ICERI 2010 International Conference of Education, Research and Innovation), Pages 7249-7253, ISBN: 978-84-614-2439-9.

MEGUA (2010) MEGUA – Mathematics Exercise Generator. Code and documentation can be found at *http://code.google.com/p/megua*.

Sage Math (2011) William A. Stein et al. *Sage Mathematics Software* (Version 4.6.1), The Sage Development Team, 2011, *http://www.sagemath.org*.

ANEXO A-EXEMPLOS DE EXERCÍCIOS PARAMETRIZADOS (versão "MEGUA-01")

O texto ao lado define o enunciado em LaTeX de um exercício parametrizado, no qual consta o texto do exercício, palavras-chave e os parâmetros {ina, inb, onb11,onb21, ona22,ona11} que vão ser substituídos por números, como mostra o exemplo que se apresenta a seguir.

```
#Funções trigonométricas (33B10) Exponen-
tial and trigonometric functions
#Também pode ser 26A09 Elementary functions
# Dada uma função com a*arcsin(b*x), com a
e b positivos determinar a sua inversa, do-
mínio, zeros e contradomínio
#PROBLEM inicia o enunciado
%PROBLEM
Considere a função\[f(x)=ina arcsin{(inb\,x)}\]
 Determine
 \begin{enumerate}
 \item Domínio;
 \item Contradomínio;
 \item Zeros;
 \item $\displaystyle f\left(onb11\right)$;
 \item $\displaystyle  f\left(onb21\right)$;
 \item A solução de
 \begin{enumerate}
 \item $\displaystyle f(x)=ona22$;
 \item $\displaystyle f(x)=ona11$.
 \end{enumerate}
 \item A inversa da função $f$, designando-
 -a por $f^{-1}$.
 \end{enumerate}
Considere a função\[f(x)=ina \,\
arcsin{(inb\,x)}\]
 Determine
 \begin{enumerate}
 \item Domínio;
 \item Contradomínio;
 \item Zeros;
 \item $\displaystyle f\left(onb11\right)$;
 \item $\displaystyle  f\left(onb21\right)$;
 \item A solução de
 \begin{enumerate}
 \item $\displaystyle f(x)=ona22$;
 \item $\displaystyle f(x)=ona11$.
 \end{enumerate}
 \item A inversa da função $f$, designando-
 -a por $f^{-1}$.
 \end{enumerate}
```

`E33B10_invtrigonometricfunction_001`

Sumário

Funções trigonométricas (33B10) Exponential and trigonometric functions Também pode ser 26A09 Elementary functions Dada uma função com a*arcsin(b*x), com a e b positivos determinar a sua inversa, domínio, zeros e contradomínio .

Palavras chave:Funções trigonométricas; arcoseno

Problema ekey=1372425087

Considere a função

$$f(x) = 4\ \text{arcsin}\,(2\,x)$$

Determine

1. Domínio;
2. Contradomínio;
3. Zeros;
4. $f\left(\frac{1}{2}\right)$
5. $f\left(-\frac{1}{2}\right)$
6. A solução de
   (a) $f(x) = \pi$;
   (b) $f(x) = 2\,\pi$.
7. A inversa da função f, designando-a por f^{-1}.

Resolução

1. O domínio da função arcsin é $[-1, 1]$, portanto, $2x$ deve pertencer a este intervalo, isto é,

$$-1 \leq 2x \leq 1 \Leftrightarrow -\frac{1}{2} \leq x \leq \frac{1}{2}$$

e, portanto, o domínio é

$$D_f = \left[-\frac{1}{2}, \frac{1}{2}\right]..$$

2. O contradomínio da função arcsin é $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Assim,

$$-\frac{\pi}{2} \leq \arcsin(2x) \leq \frac{\pi}{2}$$

e, portanto,

$$-\frac{4\pi}{2} \leq 4\arcsin(2x) \leq \frac{4\pi}{2}$$

e o contradomínio de f é

$$CD_f = [-2\,\pi, 2\,\pi]\,.$$

3. A equação $f(x) = 0$ é equivalente a $4\arcsin(2x) = 0$. Como $4 \neq 0$, a equação é equivalente a $\arcsin(2x) = 0$. O único zero da função arcsin é o próprio zero, então

$$\arcsin(2x) = 0 \Leftrightarrow 2x = 0 \Leftrightarrow x = 0$$

Portanto, $f(x) = 0$ tem como solução $x = 0$.

4. Para resolver este exercício basta substituir x pelo valor dado, $x = \frac{1}{2}$: $f(x)$

$$f\left(\frac{1}{2}\right) = 4\arcsin\left(\frac{1}{2}2\right) = 4\arcsin(1) = 2\,\pi.$$

5. Fazendo em $f(x)$, $x = -\frac{1}{2}$, obtém-se +

$$f\left(-\frac{1}{2}\right) = 4\arcsin\left(-\frac{1}{2}2\right) = 4\arcsin(-1) = -2\,\pi.$$

6.

(a) A equação $f(x) = \pi$ é equivalente a

$$4\arcsin(2x) = \pi \Leftrightarrow \arcsin(2x) = \frac{\pi}{4}.$$

Por definição de inversa,

$$\arcsin(2x) = \frac{\pi}{4} \Leftrightarrow 2x = \operatorname{sen}\frac{\pi}{4}$$

Assim, como $\operatorname{sen}\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, vem

$$2x = \frac{\sqrt{2}}{2} \Leftrightarrow x = \frac{\sqrt{2}}{4}.$$

(b) A equação $f(x) = 2\pi$ é equivalente a

$$4\arcsin(2x) = 2\,\pi \Leftrightarrow \arcsin(2x) = \frac{\pi}{2}$$

Por definição de inversa,

$$\arcsin(2x) = \frac{\pi}{2} \Leftrightarrow 2x = \operatorname{sen}\frac{\pi}{2}$$

Assim, como $\operatorname{sen}\frac{\pi}{2} = 1$, vem

$$2x = 1 \Leftrightarrow x = \frac{1}{2}.$$

7. O domínio da inversa é o contradomínio da função e o contradomínio da inversa é o domínio da função. Assim,

$$D_{f^{-1}} = [-2\,\pi, 2\,\pi] \quad \text{e} \quad CD_{f^{-1}} = \left[-\frac{1}{2}, \frac{1}{2}\right].$$

Para determinar a expressão analítica da inversa resolve-se a equação $y = f(x)$ em ordem a x, isto é,

$$y = 4\arcsin(2x) \Leftrightarrow \arcsin(2x) = \frac{1}{4}\,y \Leftrightarrow 2x = \operatorname{sen}\left(\frac{1}{4}\,y\right) \Leftrightarrow$$

$$\Leftrightarrow x = \frac{1}{2}\operatorname{sen}\left(\frac{1}{4}\,y\right).$$

Assim,

$$f^{-1}(x) = \frac{1}{2}\operatorname{sen}\left(\frac{1}{4}\,x\right).$$

ANEXO B – EXEMPLO DE COMANDOS DE UMA SESSÃO

Exemplo a dois passos:

1. sage: from MEGUA.all import *
2. sage: exercicio234.new_exercisefromtext(texto_fonte,key=27)

No passo 1. chamam-se as funções e no passo 2. cria-se um novo exercício do tipo 234, com chave aleatória 27. Esta última permite recriar sempre a mesma concretização dos parâmetros, desde que a *key* se mantenha 27.

SOBRE OS AUTORES

Maria Paula Oliveira é Professora Auxiliar do Departamento de Matemática e coordenadora de conteúdos do Projecto Matemática Ensino da Universidade de Aveiro. Foi várias vezes coordenadora de unidades curriculares com um elevado número de alunos, como Cálculo I e II.

Dina Seabra é Professora Adjunta da Escola Superior de Tecnologia e Gestão de Águeda. Tem experiência no ensino da Matemática em unidades curriculares com alunos com diferentes percursos académicos.

Pedro Cruz é Professor Auxiliar do Departamento de Matemática. Coordenou a unidades curricular "Métodos Numéricos e Estatísticos" com um elevado número de alunos.

PERGUNTAS SIMPLES, RESPOSTAS SURPREENDENTES

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

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

NOVIDADES SOBRE OS PRIMOS

O dia 13 maio de 2013 foi um dia muito especial para os primos. Enquanto o matemático peruano Harald Helfgott anunciava a conclusão da prova da versão ternária da conjetura de Goldbach, nesse mesmo dia o matemático chinês Yitang Zhang apresentava numa palestra o resultado mais importante sobre os números primos dos últimos 100 anos.

A matemática tem a fama, completamente falsa, de produzir verdades infalíveis. A sua infalibilidade não é mais do que identidade. Dois vezes dois não é quatro, mas apenas dois vezes dois, e a isso chamamos quatro para abreviar. Mas o quatro não traz nada de novo. E assim se constroem sucessivamente conclusões, acontece apenas que nas fórmulas mais elaboradas a identidade se esconde da nossa vista.

Johann Wolfgang von Goethe

1. O QUE É QUE SABEMOS SOBRE OS NÚMEROS PRIMOS?

O conjunto dos números primos

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \cdots\}$$

ocupa uma posição central na Teoria dos Números. Embora as suas propriedades sejam estudadas há cerca de 2500 anos, muitas questões permancem em aberto e outras estão ainda certamente por descobrir. Não é naturalmente fácil obter resultados novos sobre o conjunto dos números primos. Sabemos, por exemplo, que se trata de um conjunto infinito (a demonstração aparece nos *Elementos* de Euclides). Por outro lado, sabemos que existem intervalos arbitrariamente grandes de inteiros sem números primos. Também é conhecida a densidade dos números primos: o número de primos no intervalo $[1, n]$ é assintoticamente $\frac{n}{\ln n}$. Este resultado diz-nos em particular que a probabilidade de encontrar um número primo no intervalo $[1, n]$ é $\frac{1}{\ln n}$, logo, tende para zero quando n tende para infinito. O leitor pode testar a sua intuição aritmética respondendo à seguinte questão: escolhendo ao acaso um número inteiro no intervalo $[1, 10^9]$ será mais provável esse número ser: i) número primo, ii) quadrado perfeito, ou iii) múltiplo de 17?

Terence Tao e Ben Green demonstraram em 2008 que existem progressões aritméticas finitas de comprimento arbitrariamente grande cujos elementos são todos números primos. Por exemplo,

$$199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089$$

é uma progressão aritmética com dez números primos.

Podem passar décadas sem que surjam resultados novos sobre o conjunto do números primos. O dia 13 maio de 2013 foi um dia muito especial para os primos. Enquanto o matemático peruano Harald Helfgott anunciava a conclusão da prova da versão ternária da conjetura de Goldbach, nesse mesmo dia o matemático chinês Yitang Zhang apresentava numa palestra o resultado mais importante sobre os números primos dos últimos 100 anos.

2. A CONJETURA TERNÁRIA DE GOLDBACH

Teorema 1 (Harald Hefgott). *Todo o número ímpar maior do que 5 pode ser escrito como soma de três primos.*

A denominada *conjetura ternária de Goldbach* agora demonstrada por Harald Helfgott afirma que todo o número ímpar maior do que 5 pode ser escrito como soma de três números primos. Por exemplo, $15 = 3 + 5 + 7$ ou $27 = 3 + 11 + 13$. Podemos facilmente verificar que, na maioria dos casos, dado um número ímpar n, é possível encontrar mais de uma maneira de escrever n como soma de três primos. Heuristicamente, e porque a densidade do conjunto dos números primos é quase linear, devem existir muitas representações desta forma. A questão está em saber se *todo* o número ímpar tem, pelo menos, uma representação deste tipo. Existe uma outra *conjetura de Goldbach* para os números pares, a qual, como a anterior, teve origem na correspondência entre Goldbach e Euler em 1742. Esta conjetura afirma que todo o número par maior do que 2 pode ser escrito como soma de dois números primos. A demonstração da conjetura par de Goldbach implicaria naturalmente a versão ternária agora demonstrada por Harald Helfgott: bastaria juntar o primo 3 às representações dos números pares como soma de dois números primos.

Diversos problemas clássicos em Teoria de Números envolvem questões de tipo aditivo como esta: dado um conjunto $A \subset \mathbb{N}$, queremos escrever todos os naturais n como soma de um certo número de elementos do conjunto A. Lagrange demonstrou, por exemplo, que todos os números naturais podiam ser escritos como soma de quatro (ou menos) quadrados perfeitos. Por exemplo, $39 = 25 + 9 + 4 + 1$. A própria representação decimal que usamos para os inteiros corresponde a uma soma com coeficientes entre 0 e 9 de potências de 10.

Harald Helfgott trabalhava já há algum tempo no problema de Goldbach. O argumento agora apresentado utiliza, como é habitual neste tipo de problemas aditivos, o método do círculo de Hardy-Littlewood-Vinogradov. A ideia é construir uma função geradora a partir do número de representações dos inteiros como soma de três primos, e reduzir o problema ao cálculo de um determinado integral dessa função ao longo de uma circunferência centrada na origem. Terence Tao tinha demonstrado em 2012 que todo o número ímpar podia ser escrito como soma de, no máximo, 5 primos. Vinogradov [4] deu o primeiro e decisivo passo ao mostrar que todo o número inteiro $n > C$ era soma de três números primos. O problema estava desde 1937 na constante C, a partir da qual o argumento se aplicava. No argumento inicial nem sequer aparece uma constante explícita, e através de diversos melhoramentos foi progressivamente possível reduzir a constante para $C = e^{3100}$. A prova agora apresentada funciona para $n > 10^{30}$. A verificação da conjetura para os números ímpares $n < 10^{30}$ foi feita com o auxílio do computador [3].

3. PRIMOS GÉMEOS AFASTADOS

Teorema 2.

$$\liminf_{n\to\infty} (p_{n+1} - p_n) < 7 \times 10^7,$$

onde p_n é o n-ésimo primo.

O segundo resultado do dia 13 de maio de 2013 sobre números primos é ainda mais importante do que o anterior e diz-nos algo sobre a distância que separa dois números primos consecutivos. Se observarmos os primeiros elementos da sequência dos números primos, podemos ficar com a ideia errada de que os saltos de um número primo para o seguinte são sempre inferiores a 10. No entanto, sabemos que existem pares de primos consecutivos a uma distância arbitrariamente grande. Por exemplo, todos os inteiros no intervalo [100! + 2, 100! + 100] são números compostos. Queremos saber se, ainda assim, existem infinitos pares de primos muito próximos. Da densidade dos números primos resulta que o n-ésimo primo p_n salta em média $\ln(p_n)$ até ao primo que lhe sucede, aproximadamente três vezes o número dos seus dígitos. A questão está em saber se os saltos *pequenos* tão frequentes no início tendem ou não a desaparecer. Uma famosa conjetura convida-nos mesmo a acreditar que existem saltos mínimos.

Conjetura (Primos gémeos). *Existem infinitos pares de primos que distam duas unidades.*

O surpreendente resultado de Yitang Zhang é um primeiro e decisivo passo na resolução da conjetura dos primos gémeos, ao mostrar a existência de infinitos pares de primos que distam no máximo 7×10^7. A demonstração foi submetida aos *Annals of Mathematics* em abril de 2013 e já foi aceite para publicação. Em 2005, Goldston, Pintz e Yildirim chegaram a acreditar que tinham resolvido o problema dos saltos pequenos nos números primos. Conseguiram na altura mostrar que existiam sempre saltos com ordem de grandeza $\epsilon \ln(p_n)$, para qualquer $\epsilon > 0$, isto é, infinitos pares de primos consecutivos afastados arbitrariamente da média. A demonstração agora apresentada aproveita as ideias de Goldston, Pintz e Yildirim e outros resultados de teoria analítica dos números.

Yitang tem 50 anos, vive nos EUA e era até aqui relativamente desconhecido, tendo apenas dois artigos científicos publicados. Não tem sequer uma posição permanente numa universidade, e chegou mesmo a trabalhar numa loja de *fast-food*. Apesar das dificuldades, nunca deixou de pensar em problemas de matemática interessantes. O seu exemplo servirá certamente para nos recordar a todos da importância de sermos persistentes no nosso próprio trabalho. Esperemos ainda que no futuro este resultado do matemático Yitang Zhang não venha a ser designado por *teorema chinês dos primos*, em sintonia com o que infelizmente fazemos com outro resultado clássico de Teoria dos Números.

O matemático Ben Green, depois de conhecer a complexidade das ferramentas usadas por Yitang Zhang na sua prova, comentava com um misto de desconfiança e admiração que: "A demonstração de Zhang para o conjunto dos saltos majorados nos primos utiliza uma estimativa das somas de Klooterman, a qual depende da demonstração de Deligne da Hipótese de Riemann. Isto é assustador – sem toda a máquina de Grothendieck não podemos simplesmente obter o resultado. Será que existe alguém capaz de entender todos os ingredientes da demonstração? Duvido muito."[1]

Em todo o caso, neste momento o problema já despoletou mais um projeto de colaboração: foi criado o problema polymath8, a 4 de junho, com o intuito de compreender a demonstração de Zhang e de melhorar o limite superior do salto mínimo, que, depois de algum trabalho subsequente ao de Zhang, já é de 4,802,22.[2]

Por enquanto, o resultado dos saltos pequenos dos primos terá de se apoiar nos ombros de gigantes; terá de passar mais algum tempo até que seja possível entender em detalhe todos os ingredientes do argumento. E talvez nessa altura os pequenos saltos dos primos sejam tão evidentes como $2 + 2 = 4$.

REFERÊNCIAS

[1] Goldston, Daniel A., Pintz, János, Yildirim, Cem Y., "Primes in tuples. I.". *Ann. of Math.* (2) 170 (2009), no. 2, 819-862.

[2] H. A. Helfgott. M*ajor arcs for Goldbach's problem*. Preprint ar- Xiv:1305.2897.

[3] H. A. Helfgott and D. Platt. *Numerical verification of ternary Goldbach*. Preprint.

[4] I. M. Vinogradov. "Representation of an odd number as a sum of three primes". *Dokl. Akad. Nauk*. SSR, 15, 291-294 (1937).

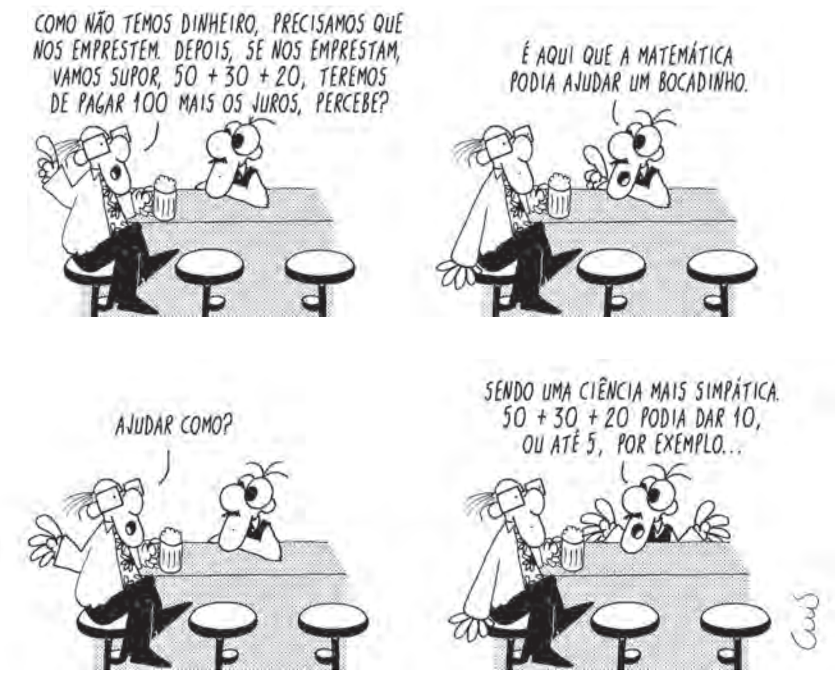
[5] Yitang Zhang. "Bounded gaps between primes". *Ann. of Math*. (2013).

[1] "[Maths post] Zhang's proof of bounded gaps between primes uses an estimate for sums of Kloosterman sums that requires the full force of Deligne's proof of the Riemann hypothesis. This blows my mind - without the whole Grothendieck machine one simply doesn't get the result. Also, is there any single person who has understood all the ingredients of the proof? I very much doubt it."

[2] *http://polymathprojects.org*

BARTOON

Luis Afonso



Publicado originalmente no jornal Público, em 12/04/2013. Imagem gentilmente cedida pelo autor.

FICHA TÉCNICA

DIRETOR:
Rogério Martins Universidade Nova de Lisboa

VICE-DIRETOR:
Alessandro Margheri Universidade de Lisboa

CONSELHO EDITORIAL:
Afonso Pedrosa Pinto E. S./3 S. Pedro Vila Real • **António Rosa** E. S. Mª Amália Vaz de Carvalho • **Elisabete Rodrigues** E. S. Maria Amália Vaz de Carvalho • **Graciano de Oliveira** Universidade Lusófona de Humanidades e Tecnologia • **Henrique Leitão** Universidade de Lisboa • **João Filipe Queiró** Universidade de Coimbra • **José Francisco Rodrigues** Universidade de Lisboa • **José Miguel Rodrigues de Sousa** E. S. Felismina Alcântara • **Lina Fonseca** Escola Superior de Educação de Viana do Castelo • **Maria do Céu Pinto** Universidade de Coimbra • **Manuel Domingos Oliveira Cadete** Universidade Agostinho Neto • **Paulus Gerdes** Universidade Eduardo Mondlane, Moçambique • **Raquel Escórcio** antiga professora na E. S. Maria Amália Vaz de Carvalho • **Teresa Almada** Universidade Lusófona de Humanidades e Tecnologia • **Juan-Miguel Gracia** Universidad del País Vasco, Espanha

ASSISTENTE EDITORIAL:
Sílvia Dias SPM

REVISÃO:
Margarida Robalo

DESIGN:
Ana Pedro

IMPRESSÃO:
Dossier – Comunicação e imagem

CONCEÇÃO DO PORTAL WEB:
Alojamento Vivo

MANUTENÇÃO DO PORTAL WEB
Sílvia Dias SPM

PROPRIEDADE:
Sociedade Portuguesa de Matemática
Av. República 45, 3ºEsq. 1050-187 Lisboa
Tel.:217939785 Fax: 217952349 E-mail:spm@spm.pt

TIRAGEM **1500 Exemplares**
ISSN **0373-2681** • ICS **123299** • DEPÓSITO LEGAL: **159725/00**

Números inteiros: alguns critérios de divisibilidade

André Fonseca e Teresa Almada
Universidade Lusófona
andre.fonseca@ulusofona.pt, talmada@ulusofona.pt

Os programas do Ensino Básico incluem vários critérios de divisibilidade de números naturais. Neste artigo apresentamos um critério de divisibilidade para números inteiros que, apesar do seu nível de generalidade, tem uma demonstração muito simples. Apresentamos também um critério de divisibilidade por 7 que generalizamos a qualquer número primo com 10. Grande parte do artigo está escrita numa linguagem simples e informal, de modo a que possa ser lido mesmo por quem está a iniciar-se no estudo da matemática.

PRELIMINARES

Muitas questões relacionadas com o conceito de divisibilidade estão diretamente ligadas à possibilidade da divisão inteira no conjunto $\mathbb{Z}$ dos números inteiros. Começamos por ver que realmente é possível efetuar a divisão inteira em $\mathbb{Z}$. Antes, porém, recordamos como é que aprendemos, no 1.º ciclo, o algoritmo da divisão. Por exemplo, para dividirmos 9 por 4, perguntamos: "Em 9 quantas vezes há 4?" A resposta é 2. Em 9 há duas vezes 4 e sobra 1. Para dividirmos 25 por 7, perguntamos: "Em 25 quantas vezes há 7?" E a resposta é 3 e sobram 4. Na verdade, perguntar "quantas vezes há d ($d>0$) num número a", equivale a perguntar "qual é o número máximo de d's que há em a?", ou ainda, a perguntar "quando é que a diferença $a-dq$ é mínima e não negativa?". Dizer que há "q vezes d em a" equivale a dizer que $a-dq \geq 0$ e que q é máximo, isto é, a diferença $a-dq$ é mínima, ou seja, $0 \leq a-dq < d$.

Proposição 1. *Se a e d são números inteiros e d é não nulo, então existem números inteiros q e r, únicos, de tal modo que*

$$a = dq + r \text{ e } 0 \leq r < |d|.$$

Demonstração. Comecemos por demonstrar o resultado para $d>0$. Procuramos um número q de tal modo que a diferença $a-dq$ seja mínima e não negativa, isto é, pretendemos encontrar o elemento mínimo do conjunto

$$X = \{a - dx : x \text{ é um número inteiro e } a - dx \geq 0\}.$$

Como os elementos do conjunto X pertencem a $\mathbb{N}_0$, se este conjunto for não vazio, existe o elemento mínimo de X. Como $d \geq 1$, então $d|a| \geq |a| \geq -a$, ou seja, $a + d|a| \geq 0$. Logo, $a + d|a|$ é um elemento do conjunto X e, portanto, o conjunto X é não vazio. Seja r o elemento mínimo do conjunto X e seja q um número inteiro tal que

$$r = a - dq, \text{ ou seja, } a = dq + r$$

Demonstremos que $r<d$. Se $r<d$, então

$$a - dq - d = a - d(q+1) \geq 0.$$

Como $a-d(q+1)$ pertence a X e $a-d(q+1) \leq a-dq$, chegamos a uma contradição.

Provemos a unicidade dos números q e r nas condições referidas demonstrando que se q , q', r e r' designam números inteiros verificando as condições

$$a = dq + r \text{ com } 0 \leq r < d \text{ e } a = dq' + r' \text{ com } 0 \leq r' < d,$$

então

$$q = q' \text{ e } r = r'$$

Suponhamos que $dq + r = a = dq' + r'$. Como $d(q-q') = r' - r$, tem-se $|d(q-q')| = |r'-r|$.

Como

$$0 \leq r' < d \text{ e } 0 \leq r < d,$$

concluímos que

$$-d < r' - r < d, \text{ ou seja, } |r'-r| < d.$$

Assim,

$$d|q-q'| = |r'-r| < d \text{ isto é, } d|q-q'| < d.$$

Como d pertence a $\mathbb{N}$, terá de ser $|q-q'| = 0$, ou seja, $q = q'$. Então $dq + r = dq + r'$ e, portanto, $r = r'$.

Se $d<0$, então $-d>0$ e, portanto, existem q e r, únicos, tais que $a = -dq + r$, com $0 \leq r < -d$. Logo, $a = d(-q) + r$ com $0 \leq r < |d|$.

Vejamos alguns exemplos da divisão inteira em $\mathbb{Z}$.

Dividendo	Divisor	Quociente	Resto
-15	3	-5	0
15	-3	5	0
-21	6	-4	3
-21	-6	4	3

Dados a e d números inteiros e supondo que d é diferente de zero, dizemos que *d é um divisor de a*, ou que *d divide a*, ou ainda que *a é divisível por d*, ou até mesmo que *a é um múltiplo de d*, se o resto da divisão inteira de a por d é zero, isto é, se existir um número inteiro q de tal modo que $a = dq$.

Verificamos facilmente que se um número inteiro a é divisível por um produto d_1d_2 de números inteiros não nulos, então é divisível por cada um dos fatores d_1 e d_2. Com efeito, se

$a = (d_1d_2)q$, então $a = d_1(d_2q)$ e $a = d_2(d_1q)$.

No entanto, um número inteiro a ser divisível por d_1 e por d_2 não garante que a seja divisível pelo produto d_1d_2. Por exemplo, 36 é divisível por 3 e por 9 e, no entanto, não é divisível por 27. Há, no entanto, uma condição que garante que um número ao ser divisível por dois números é também divisível pelo seu produto. A demonstração deste resultado, que será apresentada mais à frente, envolve os conceitos de máximo divisor comum, de números primos entre si e de número primo. Antes de os recordarmos, apresentamos alguns resultados preliminares.

Se n é um número inteiro, representamos por $n\mathbb{Z}$ o conjunto de todos os múltiplos de n.

O conjunto $n\mathbb{Z}$ dos múltiplos de n tem as seguintes propriedades:

1. O conjunto $n\mathbb{Z}$ é não vazio, pois $0 = n \times 0$;
2. Se a pertence a $n\mathbb{Z}$ e b pertence a $n\mathbb{Z}$, então $a - b$ pertence a $n\mathbb{Z}$.
3. Se a pertence a $n\mathbb{Z}$ e m pertence a $\mathbb{Z}$, então ma pertence a $n\mathbb{Z}$.

Porque o conjunto $n\mathbb{Z}$ tem as propriedades (1) a (3), dizemos que $n\mathbb{Z}$ é um *ideal* de $\mathbb{Z}$.

A qualquer subconjunto de $\mathbb{Z}$ com estas propriedades chamamos um *ideal* de $\mathbb{Z}$, isto é, um ideal de $\mathbb{Z}$ é um subconjunto I de $\mathbb{Z}$ com as propriedades:

1. O conjunto I é não vazio;
2. Se a e b são elementos de I, então $a - b$ é um elemento de I;
3. Se a é um elemento de I e α é um número inteiro qualquer, então $a\alpha$ é um elemento de I.

Observamos que o conjunto $T = \{0\}$ e o conjunto $\mathbb{Z}$ são ideais de $\mathbb{Z}$, já que $T = 0\mathbb{Z}$ e $\mathbb{Z} = 1\mathbb{Z}$.

Um número inteiro d não nulo é divisor de um inteiro a se, e só se, a é um elemento de $d\mathbb{Z}$. Este facto evidencia o papel dos ideais na teoria da divisibilidade.

Observamos que se I é um ideal de $\mathbb{Z}$, então zero é um elemento de I. De facto, por I ser não vazio, existe um elemento a em I. Da propriedade 2 resulta que $a - a = 0$ é um elemento de I. Além disso, se a é um elemento de I, o mesmo acontece com $-a$, pois se a é um elemento de I, então, pela propriedade 2, $0 - a = -a$ é um elemento de I.

Proposição 2. *Um subconjunto I de $\mathbb{Z}$ é um ideal de $\mathbb{Z}$ se, e só se, existe um número inteiro não negativo n de tal modo que $I = n\mathbb{Z}$.*

Demonstração. Do que observámos antes decorre que os conjuntos da forma $n\mathbb{Z}$ são ideais de $\mathbb{Z}$. Falta mostrar que se I é um ideal de $\mathbb{Z}$, então existe um número inteiro não negativo n de tal modo que $I = n\mathbb{Z}$.

Seja I um ideal de $\mathbb{Z}$. Se $I = \{0\}$, então $I = 0\mathbb{Z}$. Suponhamos que $I \neq \{0\}$ e seja a um elemento não nulo de I. Ou $a > 0$ ou $-a > 0$, pelo que o conjunto P definido por $P = \{x \in I : x > 0\}$ é não vazio e os seus elementos são números naturais. Seja n o elemento mínimo de P e vejamos que $I = n\mathbb{Z}$. De acordo com a propriedade 3 da definição de ideal, qualquer múltiplo de n é um elemento de I, já que sendo n um elemento de P, n é também um elemento de I. Reciprocamente, seja a um elemento de I e vejamos que a é um múltiplo de n. Como n é diferente de zero, pela proposição 1 podemos garantir a existência de números inteiros q e r de tal modo que

$$a = nq + r \text{ e } 0 \leq r < n.$$

Pretendemos provar que $r = 0$. Se $r \neq 0$, então seria $a - nq = r > 0$. Como a e n são elementos de I, o mesmo acontece com $a - nq$ (propriedades 2 e 3 da definição de ideal). Assim, $a - nq$ é um elemento positivo de I e, portanto, um elemento de P. Dado que n é o elemento mínimo de P, tem-se que $n \leq a - nq = r$, contrariando o facto de se ter $r < n$.

Logo, $r = 0$ e, portanto, $a = nq$ é um elemento de $n\mathbb{Z}$.

Esta proposição permite mostrar que dados dois números inteiros, não ambos nulos, existe em $\mathbb{Z}$ o máximo divisor comum desses números. Antes, porém, recordamos a definição de máximo divisor comum de dois números inteiros.

Dados números inteiros a e b, não ambos nulos, um número inteiro positivo d diz-se *máximo divisor comum* de a e b se

1. d é divisor de a e de b, ou seja, d é divisor comum de a e b;
2. Se c é divisor de a e de b, então c é um divisor de d.

Proposição 3. *Se a e b são números inteiros não ambos nulos, então existe e é único o máximo divisor comum de a e b.*

Demonstração. Consideremos o conjunto I definido por

$$I = \{ax + by : x \text{ e } y \text{ são números inteiros arbitrários}\}.$$

Provemos que I é um ideal de $\mathbb{Z}$. I é não vazio pois, por exemplo, $a = a \times 1 + b \times 0$ e $b = a \times 0 + b \times 1$ são elementos de I.

Se $ax + by$ e $ax' + by'$ são elementos de I, então,

$$(ax + by) - (ax' + by') = a(x - x') + b(y - y)$$

o que prova que $ax + by - (ax' + by')$ é um elemento de I, e se $ax + by$ é um elemento de I e z é um número inteiro, então $z(ax + by) = a(zx) + b(zy)$ é um elemento de I. Assim, I é um ideal de $\mathbb{Z}$.

Como a e b são elementos de I e a e b não são ambos nulos, então, pela proposição 2, existe um número inteiro positivo d de tal modo que $I = d\mathbb{Z}$. Provemos que d é o máximo divisor comum de a e b.

Como a e b são elementos de $d\mathbb{Z}$, concluímos que d é um divisor comum a a e a b. Suponhamos que c é um divisor de a e de b. Então, a e b são elementos de $c\mathbb{Z}$ e, como este conjunto é um ideal, todos os elementos de $I = d\mathbb{Z}$ são elementos de $c\mathbb{Z}$, em particular o número $d = d \times 1$ é um elemento de $c\mathbb{Z}$, o que prova que c é um divisor de d.

Quanto à unicidade, observe-se que se d e d' são ambos máximos divisores comuns de a e de b, então, pela definição de máximo divisor comum, podemos afirmar que d divide d' e que d' divide d. Em $\mathbb{Z}$, tem-se $d = d'$ ou $d = -d'$, mas como um máximo divisor comum é, por definição, um inteiro positivo, concluímos que $d = d'$.

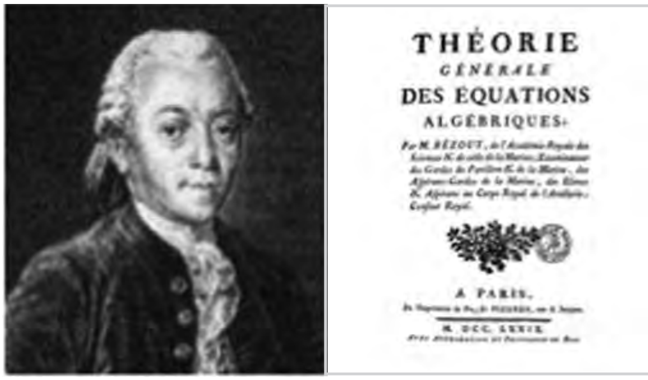
Se a e b são números inteiros não ambos nulos, escrevemos $d = \text{mdc}\,(a, b)$ para significar que d é o máximo divisor comum de a e b.

Corolário. Identidade de Bézout. *Se a e b são números inteiros não ambos nulos e $d = \text{mdc}(a,b)$, então existem números inteiros x e y tais que $d = ax + by$.*

Demonstração. Da demonstração da proposição anterior decorre que d é um elemento do conjunto

$$I = \{ax + by : x \text{ e y são números inteiros arbitrários}\}.$$

Assim, podemos garantir a existência de números inteiros x e y tais que $d = ax + by$.



Étiènne Bézout (1730–1783)

Observamos que os números inteiros x e y referidos na identidade de Bézout não são determinados de modo único. Por exemplo, mdc $(4, 6) = 2$ e $4 \times (-1) + 6 \times 1 = 2 = 4 \times 2 + 6 \times (-1)$.

Esta identidade foi provada pelo matemático francês Étiènne Bézout, autor de várias obras, das quais destacamos *Théorie générale des équations algebriques*. Esta obra existe na Biblioteca Nacional de França e pode ser consultada em *http://www.bnf.fr/fr/acc/x.accueil.html*

Recordamos que p se diz *primo* se p admitir exatamente dois divisores positivos distintos, a saber: o número 1 e o número $|p$.

De acordo com a definição, os números -1, 0 e 1 não são números primos, pois -1 e 1 têm apenas um divisor positivo, enquanto qualquer número inteiro positivo é divisor de 0.

Decorre das definições de número primo e de máximo divisor comum que se p é um número primo e a é um número inteiro não divisível por p, então $\text{mdc}(p, a) = 1$.

Dois números inteiros a e b dizem-se *primos entre si* se $\text{mdc}(a, b) = 1$.

Proposição 4. *Sejam a, b e p números inteiros e suponhamos que p é distinto de -1, de 0 e de 1.*

O número p é um número primo se, e só se, p dividir a ou dividir b, sempre que p divida o produto ab.

Demonstração. Suponhamos que p é um número primo e admitamos que p divide o produto ab e não divide a. Queremos mostrar que p divide b. Como p é primo e não divide a, então $\text{mdc}(p, a) = 1$. Pela identidade de Bézout existem números inteiros x e y tais que $px + ay = 1$. Então,

$$b = pbx + aby.$$

Como p divide o produto ab, existe um número inteiro q de tal modo que $ab = pq$. Substituindo ab na igualdade $b = pbx + aby$, obtemos que $b = pbx + pqy = p(bx + qy)$, ficando assim provado que p divide b.

Reciprocamente, suponhamos que se p divide um produto, então p divide um dos fatores e provemos que p é um número primo. Demonstremos que se d é um divisor positivo de p, então $d = 1$ ou $d = |p|$.

Seja d um divisor positivo de p. Então existe um número inteiro k de tal modo que $p = dk$. Todo o número inteiro não nulo é divisor de si próprio. Assim, p divide dk pelo que, usando a hipótese, se tem

$$p \text{ divide } d \text{ ou } p \text{ divide } k.$$

Se p divide d, então existe um número inteiro q_1 de tal modo que $d = pq_1$. Substituindo d na igualdade $p = dk$, obtemos $p = kq_1$. Logo, $kq_1 = 1$, ou seja, $k = 1$ ou $k = -1$. Se $k = -1$, então $d = -p = |p|$. Se $k = 1$, então $d = p = |p|$.

Se p divide k, existe um número inteiro q_2 de tal modo que $k = pq_2$. Substituindo k na igualdade $p = dk$, obtemos $p = pdq_2$, donde $dq_2 = 1$ e, consequentemente, $d = 1$.

ALGUNS CRITÉRIOS DE DIVISIBILIDADE

Proposição 5. *Sejam a, d_1 e d_2 números inteiros e suponhamos que d_1 e d_2 são números primos entre si. Tem-se que o produto d_1d_2 é um divisor de a se, e só se, os números d_1 e d_2 são divisores de a.*

Demonstração. Conforme foi observado anteriormente, se a é divisível por d_1d_2, então a é divisível por d_1 e por d_2. Suponhamos que um número inteiro a é divisível por d_1 e por d_2 com d_1 e d_2 primos entre si e demonstremos que a é divisível por d_1d_2. Sejam q_1 e q_2 números inteiros tais que

$$a = d_1q_1 \text{ e } a = d_2q_2.$$

Como $\text{mdc}(d_1, d_2) = 1$, pela identidade de Bézout, existem números inteiros x e y tais que $d_1x + d_2y = 1$. Tem-se

$$a = d_1ax + d_2ay = d_1d_2q_2x + d_2d_1q_1y = d_1d_2(q_2x + q_1y),$$

o que prova que o produto d_1d_2 divide a.

Esta proposição permite deduzir vários critérios de divisibilidade. Enunciamos, a título de exemplo, apenas alguns desses critérios.

Critério de divisibilidade por 6. Um número inteiro é divisível por 6 se, e só se, é divisível por 2 e por 3.

Critério de divisibilidade por 12. Um número inteiro é divisível por 12 se, e só se, é divisível por 3 e por 4.

Critério de divisibilidade por 14. Um número inteiro é divisível por 14 se, e só se, é divisível por 2 e por 7.

Critério de divisibilidade por 15. Um número inteiro é divisível por 15 se, e só se, é divisível por 3 e por 5.

Critério de divisibilidade por 18. Um número inteiro é divisível por 18 se, e só se, é divisível por 2 e por 9.

Critério de divisibilidade por 21. Um número inteiro é divisível por 21 se, e só se, é divisível por 3 e por 7.

CONGRUÊNCIAS

Se a, b e n são números inteiros e $n > 0$, dizemos que *a é congruente com b módulo n* se a e b têm o mesmo resto na divisão inteira por n. Neste caso escrevemos

$$a \equiv b (\text{mod} n).$$

Verificamos facilmente que se a, b e c são números inteiros, então

1. *Reflexividade:* $a \equiv a(\text{mod} n)$;
2. *Simetria*: se $a \equiv b(\text{mod} n)$, então $b \equiv a(\text{mod} n)$;
3. *Transitividade:* se $a \equiv b(\text{mod} n)$ e $b \equiv c(\text{mod} n)$, então $a \equiv c(\text{mod} n)$.

Porque a relação binária $\equiv (\text{mod} n)$ tem as propriedades (1) a (3), dizemos que a relação é uma *relação de equivalência*. Uma *relação de congruência* é uma relação de equivalência compatível com a operação de adição e com a operação de multiplicação.

Proposição 6. *Se a, b e n são números inteiros e n é positivo, então $a \equiv b(\text{mod} n)$ se, e só se, n é um divisor de $a - b$.*

Demonstração. Suponhamos que $a \equiv b(\text{mod} n)$. Então, a e b têm o mesmo resto na divisão inteira por n e, portanto, existem números inteiros q_1, q_2 e r tais que

$$a = nq_1 + r \text{ e } b = nq_2 + r, \text{ com } 0 \leq r < n.$$

Como $a - b = n(q_1 - q_2)$ concluímos que n divide $a - b$.

Reciprocamente, suponhamos que n é um divisor de $a - b$ e seja q um número inteiro tal que

$$a - b = nq.$$

Sejam q_1, q_2, r_1 e r_2 números inteiros tais que $a = nq_1 + r_1$ e $b = nq_2 + r_2$, com $0 \leq r_1, r_2 < n$.

Suponhamos que $r_2 \leq r_1$. Então

$$nq = a - b = n(q_1 + q_2) + (r_1 - r_2).$$

Como $0 \leq r_1 - r_2 < n$, então, pela unicidade do resto, obtemos que $r_1 = r_2$, ou seja $a \equiv b(\mathrm{mod}\, n)$.

Proposição 7. *Sejam a, b, c, d e n números inteiros com n positivo. Se $a \equiv b(\mathrm{mod}\, n)$ e $c \equiv d(\mathrm{mod}\, n)$, então $a + c \equiv b + d(\mathrm{mod}\ n)$ e $ac \equiv bd(\mathrm{mod}\, n)$.*

Demonstração. Suponhamos que $a \equiv b(\mathrm{mod}\, n)$ e $c \equiv d(\mathrm{mod}\, n)$. Então, $a - b$ e $c - d$ são múltiplos de n. Assim,

$$(a + c) - (b + d) = (a - b) + (c - d)$$

é um múltiplo de n e, portanto, $a + c \equiv b + d(\mathrm{mod}\ n)$.

Por outro lado, $ac - bd = (a - b)c + (c - d)b$ é múltiplo de n, e, portanto, $ac \equiv bd(\mathrm{mod}\, n)$.

Se a e n são números inteiros e n é positivo, representamos por $[a]_{\equiv(\mathrm{mod}\, n)}$ o conjunto de todos os números inteiros congruentes com a módulo n. A este conjunto chamamos *classe de congruência módulo n* do número inteiro a, isto é, o conjunto de todos os números inteiros que têm o mesmo resto que a na divisão inteira por n.

Tem-se

$$[a]_{\equiv(\mathrm{mod}\, n)} = [b]_{\equiv(\mathrm{mod}\, n)} \text{ se, e só se, } a \equiv b(\mathrm{mod}\, n).$$

É de notar que se a é um número inteiro, então

$$[a]_{\equiv(\mathrm{mod}\, n)} = [r]_{\equiv(\mathrm{mod}\, n)}$$

onde r é o resto da divisão inteira de a por n. Como os restos possíveis na divisão inteira por n são os números inteiros de 0 a $n - 1$, concluímos que existem exatamente n classes de congruência módulo n distintas.

Por exemplo, as classes de congruência módulo 5 são $[0]_{\equiv(\mathrm{mod}\, n)}$, $[1]_{\equiv(\mathrm{mod}\, n)}$, $[2]_{\equiv(\mathrm{mod}\, n)}$, $[3]_{\equiv(\mathrm{mod}\, n)}$ e $[4]_{\equiv(\mathrm{mod}\, n)}$.

A compatibilidade da relação $\equiv (\mathrm{mod}\, n)$ com as operações de adição e de multiplicação, permite definir no conjunto das classes de congruência módulo n uma operação de adição e uma operação de multiplicação do seguinte modo:

$$[a]_{\equiv(\mathrm{mod}\, n)} + [b]_{\equiv(\mathrm{mod}\, n)} = [a + b]_{\equiv(\mathrm{mod}\, n)}$$

e

$$[a]_{\equiv(\mathrm{mod}\, n)} \times [b]_{\equiv(\mathrm{mod}\, n)} = [ab]_{\equiv(\mathrm{mod}\, n)}.$$

Por exemplo,

$$[3]_{\equiv(\mathrm{mod} 5)} + [4]_{\equiv(\mathrm{mod} 5)} = [7]_{\equiv(\mathrm{mod} 5)} = [2]_{\equiv(\mathrm{mod} 5)}$$

e

$$[2]_{\equiv(\mathrm{mod} 5)} \times [4]_{\equiv(\mathrm{mod} 5)} = [8]_{\equiv(\mathrm{mod} 5)} = [3]_{\equiv(\mathrm{mod} 5)}.$$

CRITÉRIO GERAL DE DIVISIBILIDADE

Observamos que, dados números inteiros a e d, com d não nulo, provar que a é divisível por d é mostrar que a divisão inteira de a por d é exata, ou seja, que o resto da divisão é zero, isto é,

$$[a]_{\equiv(\mathrm{mod}\, d)} = [0]_{\equiv(\mathrm{mod}\, d)}.$$

Consideremos o número 27564. Como é sabido, este número pode ser representado na forma

$$27564 = 2\mathrm{x}10^4 + 7\mathrm{x}10^3 + 5\mathrm{x}10^2 + 6\mathrm{x}10^1 + 4\mathrm{x}10^0.$$

Na verdade, qualquer número inteiro pode ser escrito naquela forma. Se $a = a_k a_{k-1} ... a_1 a_0$ é a representação no sistema decimal de um número inteiro a, então

$$a = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 = \sum_{i\ 0}^{k} a_1 10^i.$$

Dados números inteiros não negativos i e d, com d diferente de zero, representamos por R_{id} o *resto da divisão inteira de* 10^i *por d*. Do que dissemos antes, resulta que

$$[10^i]_{\equiv(\mathrm{mod}\, d)} = [R_{id}]_{\equiv(\mathrm{mod}\, d)}.$$

Proposição 8. ***Critério geral de divisibilidade.***
Sejam $a = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$ e d números inteiros e suponhamos que d é não nulo.

Tem-se que o número a é divisível por d se, e só se, o número inteiro $\sum_{i=0}^{k} a_i R_{id}$ é divisível por d.

Demonstração. O número a é divisível por d se, e só se,

$$[a]_{\equiv(\mathrm{mod}\, d)} = [0]_{\equiv(\mathrm{mod}\, d)}.$$

Mas

$$[a]_{\equiv(\mathrm{mod}\, d)} = [\sum_{i=0}^{k} a_i 10^i]_{\equiv(\mathrm{mod}\, d)} =$$

$$= \sum_{i=0}^{k} [a_i]_{\equiv(\mathrm{mod}\ d)} \times [10^i]_{\equiv(\mathrm{mod}\ d)}$$

$$= \sum_{i=0}^{k} [a_i]_{\equiv(\mathrm{mod}\, d)} \times [R_{id}]_{\equiv(\mathrm{mod}\, d)} =$$

$$= [\sum_{i=0}^{k} a_i R_{id}]_{\equiv(\mathrm{mod}\, d)}.$$

Assim,

$[a]_{\equiv(\mathrm{mod}\, d)} = [0]_{\equiv(\mathrm{mod}\, d)}$ se, e só se,

$$[\sum_{i=0}^{k} a_i R_{id}]_{\equiv(\mathrm{mod}\, d)} = [0]_{\equiv(\mathrm{mod}\, d)}$$

e, portanto,

a é divisível por d se, e só se, o número inteiro $\sum_{i=0}^{k} a_i R_{id}$ é divisível por d.

Corolário 1. ***Critério de divisibilidade por 2.*** *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 2 se, e só se, o algarismo das unidades, a_0, é um número par.*

Demonstração. Como $R_{i2} = 0$ sempre que $i > 0$ e $R_{02} = 1$, então $\sum_{i=0}^k a_i R_{i2} = a_0$ e, portanto, de acordo com a proposição anterior, a é divisível por 2 se, e só se, a_0 é divisível por 2 ou, equivalentemente, a_0 é um número par.

Corolário 2. ***Critério de divisibilidade por 3.*** *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 3 se, e só se, o número $\sum_{i=0}^k a_i$ é divisível por 3.*

Demonstração. Como $R_{i3} = 1$, qualquer que seja o i, então a é divisível por 3 se, e só se, $\sum_{i=0}^k a_i R_{i3} = \sum_{i=0}^k a_i$, é divisível por 3. Assim, um número inteiro é divisível por 3 se, e só se, a soma dos seus algarismos é divisível por 3.

Corolário 3. Critério de divisibilidade por 4. *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 4 se, e só se, o número $a_1\, a_0$ é divisível por 4.*

Demonstração. Como $R_{14} = 2$, $R_{04} = 1$ e $R_{i4} = 0$, sempre que i seja maior do que 1, então a é divisível por 4 se, e só se, $\sum_{i=0}^k a_i R_{i4} = 2a_i + a_0$ é divisível por 4. Assim, de acordo com a proposição 8, $2a_1 + a_0$ é divisível por 4 se, e só se, $10a_1 + a_0$ é divisível por 4, ou seja, um número inteiro é divisível por 4 se, e só se, o número constituído pelos seus dois últimos algarismos for divisível por 4.

Corolário 4. ***Critério de divisibilidade por 5.*** *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 5 se, e só se, o algarismo das unidades, a_0, é zero ou cinco.*

Demonstração. Como $R_{i5} = 0$, sempre que $i > 0$ e $R_{05} = 1$, então $\sum_{i=0}^k a_i R_{i5} = a_0$.

Logo, a é divisível por 5 se, e só se, $a_0 = 0$ ou $a_0 = 5$. Logo, um número inteiro é divisível por 5 se, e só se, o algarismo das unidades é 0 ou 5.

Corolário 5. Critério de divisibilidade por 6. *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 6 se, e só se, o algarismo das unidades é um número par e a soma $\sum_{i=0}^k a_i$ é divisível por 3.*

Demonstração. De acordo com a proposição 5, o número a é divisível por 6 se, e só se, é divisível por 2 e por 3. O resultado decorre dos corolários 1 e 2.

Corolário 6. ***Critério de divisibilidade por 8.*** *Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 8 se, e só se, o número $a_2\ a_1\ a_0$ é divisível por 8.*

Demonstração. Como $R_{28} = 4$, $R_{18} = 2$, $R_{08} = 1$ e $R_{i8} = 0$ sempre que $i \geq 3$, então

$$\sum_{i=0}^k a_i R_{i8} = 4a_2 + 2a_1 + a_0.$$

Logo, de acordo com a proposição 8, o número $4a_2 + 2a_1 + a_0$ é divisível por 8 se, e só se, o mesmo acontece com $a_2 a_1 a_0 = 10^2 a_2 + 10a_1 + a_0$, ou seja, um número inteiro é divisível por 8 se, e só se, o número constituído pelos seus três últimos algarismos é divisível por 8.

Corolário 7. ***Critério de divisibilidade por 9.*** Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 9 se, e só se, a soma $\sum_{i=0}^k a_i$ é divisível por 9.

Demonstração. O resultado decorre imediatamente da proposição 8 e do facto de $R_{i9} = 1$ qualquer que seja o $i > 0$.

Corolário 8. ***Critério de divisibilidade por 10.*** Um número inteiro $a = a_k a_{k-1}...a_1 a_0$ é divisível por 10 se, e só se, $a_0 = 0$.

Demonstração. O resultado decorre do critério geral e do facto de se ter $R_{0,10} = 1$ e $R_{i10} = 0$ sempre que $i \geq 1$.

CRITÉRIO DE DIVISIBILIDADE POR UM NÚMERO PRIMO SUPERIOR A 5

Seja a um inteiro e suponhamos que

$$a = a_k...a_1 a_0 = \sum_{i=0}^k a_i 10^i.$$

Notemos que o número inteiro

$$b = a_k \ldots a_1 \text{ se escreve na forma } \sum_{i=1}^k a_i 10^{i-l}.$$

Proposição 9. ***Critério de divisibilidade por 7.*** *Um número inteiro $a = a_k...a_1 a_0$ é divisível por 7 se, e só se, o número inteiro $a_k...a_1 - 2a_0$ é divisível por 7.*

Demonstração. Suponhamos que $a = \sum_{i=0}^k a_i 10^i = 7q$. Então,

$$\sum_{i=1}^k a_i 10^i + a_0 = 7q \text{ donde } -2a_0 = 2\sum_{i=1}^k a_1 10^i - 2 \times 7q.$$

Vejamos que $\sum_{i=1}^k a_i 10^{i-1} - 2a_0$ é divisível por 7. Ora,

$$\sum_{i=1}^{k} a_i\,10^{i-1} - 2a_0 = \sum_{i=1}^{k} a_i\,10^{i-1} + 2\sum_{i=1}^{k} a_i 10^{i} - 2\times 7q =$$

$$= \sum_{i=1}^{k} a_i 10^{i-1} + 2\times 10\sum_{i=1}^{k} a_i 10^{i-1} - 2\times 7q =$$

$$= (1+20)\sum_{i=1}^{k} a_i\,10^{i-1} - 2\times 7q =$$

$$= 7(3\sum_{i=1}^{k} a_i\,10^{i-1} - 2q),$$

o que prova que o número

$$\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0 \text{ é divisível por 7.}$$

Reciprocamente, suponhamos que $\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0 = 7p$.. Então, multiplicando ambos os membros por 10, obtemos,

$$\sum_{i=1}^{k} a_i 10^{i} - 20a_0 = 7\times 10p, \text{ donde}$$

$$\sum_{i=1}^{k} a_i 10^{i} + a_0 - (20+1)a_0 = 7\times 10p.$$

Logo,

$$a = \sum_{i=1}^{k} a_i 10^{i} + a_0 = 21a_0 + 7\times 10p = 7(3a_0 + 10p),$$

o que prova que

$$a = \sum_{i=0}^{k} a_i 10^{i} \text{ é divisível por 7.}$$

Observamos que este critério pode ser aplicado sucessivamente até obter um número que seja fácil verificar se é múltiplo de 7. Vejamos um exemplo. Consideremos o número a = 129654 e apliquemos o critério sucessivamente para averiguarmos se este número é divisível por 7. Ora, o número 129654 é divisível por 7 se, e só se, 12965–8 = 12957 é divisível por 7. Mas, 12957 é divisível por 7 se, e só se, 1295–14 = 1281 é divisível por 7. Da mesma forma, 1281 é divisível por 7 se, e só se, o mesmo acontece com 128–2 = 126. Como $126 = 7\times 18$, então 129654 é divisível por 7.

Analisemos o critério de divisibilidade por 7: um número inteiro $\sum_{i=0}^{k} a_i 10^{i}$ é divisível por 7 se, e só se, o mesmo acontece com o número inteiro $\sum_{i=1}^{k} a_i 10^{i-1} - 2a_0$. A primeira pergunta que nos ocorre é: porquê o número 2 e não outro? Qual é o papel do número 2 na demonstração deste critério? Analisando, verificamos que a razão para ser o número 2 é o facto de $10\times 2+1$ ser um múltiplo de 7. Isto sugere que o critério talvez possa ser generalizável a qualquer número primo p superior a 5 se pudermos garantir a existência de um número inteiro k_p de tal modo que

$$10k_p + 1 \text{ seja um múltiplo de } p.$$

Se p é um número primo superior a 5, então p não divide 10, e, portanto, p e 10 são primos entre si. Pela identidade de Bézout, existem números inteiros x e y de tal modo que $10x + py = 1$. Então $py = 1 - 10x$. Consideremos $k_p = p - x$ e vejamos que $10(p-x)+1$ é um múltiplo de p. Ora,

$$10(p-x)+1 = 10p - 10x + 1 = 10p + py = (10+y)p.$$

Parece estar encontrado um valor possível para k_p. Coloca-se, no entanto, uma questão. Os coeficientes da identidade de Bézout não são determinados de modo único. Como resolver esta questão? A primeira ideia que nos ocorre é tomar para valor de k_p o resto da divisão inteira de $p-x$ por p. O resto é determinado de forma única. No entanto, se $10x + py = 1$ e $10z + pw = 1$, será que $p - x$ e $p - z$ têm o mesmo resto na divisão inteira por p? Vejamos que sim. O que queremos provar é que $p - x \equiv p - z (mod p)$. De acordo com a proposição 6, tudo o que teremos de mostrar é que $(p-x)-(p+z) = z - x$ é um múltiplo de p.

Da igualdade $10x + py = 1$ decorre que $10x = 1 - py$ e da igualdade $10z + pw = 1$ resulta que $10z = 1 - pw$. Assim, podemos afirmar que

$$10(z-x) = 10z - 10x = 1 - pw - 1 + py = p(y-w).$$

A igualdade $10(z-x) = p(y-w)$ garante que p divide o produto $10(z-x)$. Assim, como p não divide 10, pela proposição 4, p divide $z - x$, ficando assim provado que $p - x$ e $p - z$ têm o mesmo resto na divisão inteira por p. A questão está resolvida: **dado um número primo p superior a 5 e números inteiros x e y de tal modo que 10x+py =1, tomamos para valor de k_p o resto da divisão inteira de p–x por p.**

Na tabela seguinte apresentamos alguns valores de k_p .

p (nº primo)	10x+py=1 (Id de Bézout)	p-x	p–x=pq+r (divisão de $p-x$ por p)	k_p=r
11	$10\times(-1)+11\times 1=1$	12	$11\times 1+1$	1
13	$10\times(-9)+13\times 7=1$	22	$13\times 1+9$	9
17	$10\times(-5)+17\times 3=1$	22	$17\times 1+5$	5
19	$10\times(-17)+19\times 9=1$	36	$19\times 1+17$	17
23	$10\times(-16)+23\times 7=1$	39	$23\times 1+16$	16
29	$10\times(-26)+29\times 9=1$	55	$29\times 1+26$	26
31	$10\times(-3)+31\times 1=1$	33	$31\times 1+3$	3

Proposição 10. ***Critério de divisibilidade por um número primo superior a 5.*** *Seja p um número primo superior a 5 e sejam x e y inteiros tais que 10x+py=1. Seja k_p o resto da divisão de p–x por p. Tem-se que um número inteiro $a = a_k ... a_1 a_0$ é divisível por p se, e só se, o número inteiro $a_k ... a_1 - k_p a_0$ é divisível por p.*

Demonstração. Suponhamos que $\sum_{i=0}^{k} a_i 10^i = np$. Então,

$$\sum_{i=1}^{k} a_i 10^i + a_0 = np, \text{ donde } -k_p a_0 = k_p \sum_{i=1}^{k} a_i 10^i - k_p np.$$

Vejamos que $\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0$ é divisível por p. Ora,

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 = \sum_{i=1}^{k} a_i 10^{i-1} + k_p \sum_{i=1}^{k} a_i 10^i - k_p np =$$

$$= \sum_{i=1}^{k} a_i 10^{i-1} + k_p \times 10 \sum_{i=1}^{k} a_i 10^{i-1} - k_p np =$$

$$= (1 + k_p \times 10) \sum_{i=1}^{k} a_i 10^{i-1} - k_p np.$$

Como $1 + 10k_p$ é um múltiplo de p, então $1 + 10k_p$ é de forma mp, para algum número inteiro m. Assim,

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 =$$

$$= (1 + k_p \times 10) \sum_{i=1}^{k} a_i 10^{i-1} - k_p np =$$

$$= p(m \sum_{i=1}^{k} a_i 10^{i-1} - k_p n),$$

o que prova que

$$\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 \text{ é divisível por } p.$$

Reciprocamente, suponhamos que $\sum_{i=1}^{k} a_i 10^{i-1} - k_p a_0 = np$. Então, multiplicando ambos os membros por 10, obtemos

$$\sum_{i=1}^{k} a_i 10^i - 10k_p a_0 = 10np, \text{ donde}$$

$$\sum_{i=1}^{k} a_i 10^i + a_0 - (10k_p + 1) a_0 = 10np. \text{ Logo}$$

$$\sum_{i \quad 1}^{k} a_i 10^i + a_0 = (10k_p + 1) a_0 + 10np.$$

Como $10k_p + 1$ é um múltiplo de p, então $10k_p + 1 = mp$, para algum número inteiro m.
Assim, $\sum_{i=1}^{k} a_i 10^i + a_0 = (10k_p + 1) a_0 + 10np = mpa_0 + 10np = p(ma_0 + 10n)$, logo

$$a = \sum_{i=0}^{k} a_i 10^i \text{ é divisível por } p.$$

Observamos que da análise à demonstração que acabamos de apresentar se conclui que o critério de divisibilidade pode ser estendido a qualquer número inteiro que seja primo com 10.

Vejamos alguns exemplos de aplicação da proposição 10.

O número 155023 é divisível por 11. De facto, o valor de $\boldsymbol{k_{11}}$ **é 1**. Considerando a seguinte sequência de números,

155023 ▷ 115502 – 3 × 1 = 15499 ▷ 1549 – 9 × 1 = 1540 ▷ 154 – 0=154 ▷ 15 – 4 × 1 =11

Concluímos, uma vez que 11 é divisível por 11, que 155023 é divisível por 11.

O número 96993 é divisível por 13. Neste caso, o valor de $\boldsymbol{k_{13}}$ **é 1**. Considerando a seguinte sequência de números,

96993 ▷ 9699 – 3×9 = 9672 ▷ 967 – 2×9 = 949 ▷ 94 – 9×9 = 13

Concluímos, uma vez que 13 é divisível por 13, que o mesmo acontece com 96993.

O número 1381675 é divisível por 17. Basta atender a que o valor de $\boldsymbol{k_{17}}$ **é 1** e consideremos a seguinte sequência de números:

1381675 ▷ 138167 – 5×5 =138142 ▷ 13814 – 2×5 = 13804 ▷ 1380 – 4×5 = 1360 ▷ 136 – 0×5

Verificamos, como 136 = 8x17, que então 1381675 é divisível por 17.

O número 136078 é divisível por 19. De facto, o valor de $\boldsymbol{k_{19}}$ **é 17** e, considerando a seguinte sequência de números,

136078 ▷ 13607 – 8×17 = 13471 ▷ 1347– 17 = 1330 ▷ 133 = 7×19

Concluímos que 136078 é divisível por 19.

O número 209921 é divisível por 23. Notemos que o valor de $\boldsymbol{k_{23}}$ **é 16**, pelo que, considerando a seguinte sequência de números:

209921 ▷ 20992 – 1×16= 20976 ▷ 2097 – 6×16 = 2001 ▷ 200 – 1×16 =184

Dado que 184 = 8×23, então concluímos que 209921 é divisível por 23.

O número 236205 é divisível por 29. Notemos que o valor de k_{29} **é 26**, pelo que considerando a seguinte sequência de números,

$$236205 \triangleright 23620 - 5\times 26 = 23490 \triangleright 2349 - 0\times 26 = 2349 \triangleright 234 - 9\times 26 = 0$$

concluímos que 236205 é divisível por 29.

O número 218922 é divisível por 31. Neste caso, o valor de k_{31} **é 3**. Considerando a seguinte sequência de números,

$$218922 \triangleright 21892 - 2\times 3 = 21886 \triangleright 2188 - 3\times 6 = 2170 \triangleright 217 = 7\times 31$$

podemos afirmar que 218922 é divisível por 31.

BIBLIOGRAFIA

Niven, I., Zuckerman, H., Montgomery, H., *An Introduction to the Theory of Numbers*, 5th Edition, Wiley & Sons, 1991.

Van der Waerden, B., *Algebra*, Springer-Verlag, 2003.

SOBRE OS AUTORES

André Fonseca obteve o grau de Doutor (PhD) em Matemática, no ano de 2004, na Universidade de Leicester, Reino Unido, e efetuou um pós-doutoramento na Universidade de Chicago durante o ano 2005. Atualmente é Professor no Departamento de Matemática da Universidade Lusófona de Lisboa. Desenvolve investigação na área da Teoria de Representações.

Teresa Almada tem o grau de Doutor em Matemática pela Universidade de Lisboa desde 1994. É diretora do Departamento de Matemática da Universidade Lusófona de Lisboa. Desenvolve investigação em Teoria dos Reticulados e em Álgebras da Lógica. Desde longa data que Teresa Almada se interessa por questões relacionadas com o ensino da Matemática, a que tem dedicado algum do seu tempo.

Bernardo Mota
Universidade de Lisboa
bernardomota@campus.ul.pt

FAZER **CONTAS** COM NUMERAIS **ROMANOS**

É comum ouvir dizer que os numerais romanos não facilitam a realização das operações aritméticas. Hoje, voltamos aos bancos da escola, em Roma, e aprendemos a fazer contas de somar e multiplicar.

A computação com numerais romanos é normalmente considerada difícil, senão mesmo impossível. Esta ideia foi defendida por importantes historiadores da matemática e ainda hoje se encontra bem disseminada. Uma das razões para a sua permanência é o facto de não terem sobrevivido obras de autores romanos sobre aritmética prática. Estamos confinados, para o estudo deste tema, à análise de alguns passos de Varrão, Vitrúvio, Plínio-o-Velho, Columela, Frontino, e alguns autores mais tardios. No entanto, estes autores não nos mostram como é que chegam aos seus resultados, e acabamos por ficar reduzidos ao conhecimento de procedimentos calculatórios que utilizam o ábaco e os dedos das mãos. A verdade é esta: não temos qualquer prova direta de que os romanos realizavam operações aritméticas com os seus numerais.

No entanto, há que separar a dificuldade histórica da cognitiva. Uma coisa é determinar como realizavam os romanos as suas contas e quais os algoritmos que aplicavam. Outra é determinar se o uso de numerais romanos resulta numa prática impossível da aritmética. Ora, o que alguns estudos têm vindo a realçar é que, contrariamente ao que se pensa, as operações aritméticas com numerais romanos são relativamente simples, podendo mesmo ser mais simples do que as que utilizam os numerais árabes. Contrariamente ao sistema posicional que usamos (dependente de uma base e do valor e da posição de cada símbolo), os romanos utilizavam um sistema aditivo, em que cada símbolo corresponde a um valor fixo e o valor de um numeral é obtido somando-se os valores de todos os seus símbolos. A notação subtrativa, em que, por exemplo, o número 4 é representado por IV, tornou-se habitual apenas em época mais tardia e deixá-la-emos de lado (as dificuldades que levanta, de resto, são facilmente solucionáveis). Os símbolos fundamentais do sistema são: I, V, X, L, C, D, M; colocando-se uma barra sobre cada um destes símbolos, multiplicamos o seu valor base por 1000.

A operação da adição com numerais romanos é, na realidade, muito simples. Para adicionar números, só temos de justapor os símbolos dos números a adicionar, ordená-los de acordo com o seu valor e simplificar os conjuntos obrigatórios (IIIII→V; VV→X, etc.). Na tabela 1 deixamos, como exemplo, a operação da soma de MMMDXXVIII (3528) com CCXV (215) e LXXII (72).

A operação da multiplicação é igualmente fácil de aprender. A tabela da multiplicação dos numerais romanos é francamente mais regular do que a nossa; um algoritmo parecido com o nosso é muito fácil de aplicar: multiplica-se cada símbolo de um fator por cada símbolo do outro fator e soma-se os resultados intermédios. Na tabela 2, para 56 × 72 (LVI × LXXII).

Em 1970, numa pequena carta enviada ao editor da revista *Nature*, Margaret Lazarides apresentou um algoritmo simples para a multiplicação que dispensa o conhecimento de tabelas de multiplicação.

A verdade é que, com um pouco de treino, é possível realizar as demais operações aritméticas fundamentais com numerais romanos sem grande dificuldade. Não quer isto dizer que o nosso sistema não seja mais simples do que o sistema romano. Apenas realça que fazer cálculos com o sistema de numeração romano é muito mais simples do que normalmente pensamos e que uma comparação rigorosa do grau de dificuldade dos dois sistemas é uma tarefa mais complexa do que pode parecer à primeira vista. Não podemos esquecer-nos de que a aprendizagem do nosso sistema, que consideramos tão fácil, nos tira muitas horas de brincadeira em período escolar, e que simplesmente não sabemos quais os resultados que poderíamos atingir se gastássemos o mesmo número de horas a aprender um outro sistema.

REFERÊNCIAS:

Uma boa base de partida para o leitor interessado é esta: Schlimm, D., Neth, H. (2008). "Modeling Ancient and Modern Arithmetic Practices: Addition and Multiplication with Arabic and Roman Numerals"; in V. Sloutsky, B. Love & K. McRae (Eds.), *Proceedings of the Thirtieth Annual Meeting of the Cognitive Science Society*, Austin, TX, Cognitive Science Society [disponível no endereço: *http://csjarchive.cogsci.rpi.edu/proceedings/2008/pdfs/p2097.pdf*]; assinalo outros dois artigos: Detlefsen, M., Erlandson, D. K., Heston, J. C., & Young, C. M. (1975). "Computation with Roman Numerals", *Archive for History of Exact Sciences*, 15, 141-148, por estar publicado numa revista de referência e disponível na B-On; Anderson, W. French, "Arithmetical Computations in Roman Numerals", *Classical Philology*, 51.3, 1956, 145-150; por ser um dos primeiros artigos que se debruça sobre este tema. A carta de M. Lazarides mencionada no artigo foi publicada com o título "Quare Multiplicandum Est", na pág. 195 da edição n. 226 de 1970 da revista *Nature*.

Linha	Passo 1	Passo 2 (IIIII→V)	Passo 3 (VV→X)	Passo 4 (XXXXX→L)	Passo 5 (LL→C)	Passo 6 (Resultado)
M	MMM	MMM	MMM	MMM	MMM	MMMDCCCXV
D	D	D	D	D	D	
C	CC	CC	CC	CC	CCC	
L	L	L	L	LL	-	
X	XXXXX	XXXXX	XXXXXX	X	X	
V	VV	VVV	V	V	V	
I	IIIII	-	-	-	-	

Tabela 1: Operação da SOMA de MMMDXXVIII com CCXV e LXXII (3528+215+72)

Linha	Passo 1 (I × LXXII)	Passo 2 (V × LXXII)	Passo 3 (L × LXXII)	Passo 4 (Soma)	Passo 5 (Simplificação)
M	-	-	MM	MM	MMMM
D	-	-	DDD	DDD	-
C	-	CC	-	CC	-
L	L	LLL	LL	LLLLL	-
X	XX	-	-	XX	XXX
V	-	VV	-	VV	-
I	II	-	-	II	II

Tabela 2: Operação da MULTIPLICAÇÃO de LVI com LXXII (56 × 72)

COMEÇOU A **ÉPOCA** DAS **OLIMPÍADAS** DE **MATEMÁTICA ALÉM-FRONTEIRAS**

OIM REALIZAM-SE EM **JULHO,** NA **COLÔMBIA**

A equipa que este ano representará Portugal nas Olimpíadas Internacionais de Matemática (OIM) está já a postos para a competição. David Martins, Francisco Andrade, Luís Duarte, Miguel Moreira, Miguel Santos e Nuno Santos viajarão este mês para a cidade de Santa Marta, na Colômbia, para participarem na 54ª edição das OIM, entre os dias 18 e 28 de julho. Cerca de 550 participantes de mais de uma centena de países marcarão presença nesta competição, que se estreou em 1959, na Roménia, com apenas cinco países. Portugal participou pela primeira vez nas OIM em 1989 e, desde então, já conquistou duas medalhas de ouro, duas de prata, 16 de bronze e 20 menções honrosas.

MAPUTO RECEBE PELA PRIMEIRA VEZ **OLIMPÍADAS** DA **CPLP**

Entre 4 e 10 de agosto, a capital moçambicana será a anfitriã das próximas Olimpíadas da CPLP (OCPLP). Realizadas pela primeira vez em Portugal em 2011, as OCPLP passaram na sua segunda edição por São Salvador, no Brasil, rumando agora ao continente africano. Esta competição envolve jovens da comunidade dos países que partilham a língua portuguesa: Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal, São Tomé e Príncipe e Timor-Leste. A equipa que representará Portugal em Moçambique é composta por David Andrade, Henrique Santos, João Rocha e Miguel Costa.

TARDES DE MATEMÁTICA NOS AÇORES

Nos meses de setembro e outubro, a população de Ponta Delgada poderá assistir a duas palestras do ciclo Tardes de Matemática. No dia 21 de setembro, pelas 15h30, a Biblioteca Pública e Arquivo Regional de Ponta Delgada recebe João Cabral (Universidade dos Açores) para "Uma aventura no mundo dos padrões". "Estatística: para que te quero?" é o tema da sessão do dia 26 de outubro, apresentado por Áurea Sousa e Osvaldo Silva (Universidade dos Açores), no mesmo local.

OIAM EM **SETEMBRO,** NO **PANAMÁ**

De 20 a 28 de setembro, outra grande competição internacional terá lugar na Cidade do Panamá. Mais de 20 países da América do Sul e da Península Ibérica competirão na 28ª edição das Olimpíadas Ibero-Americanas de Matemática. Portugal, que participa nesta competição desde 1990, e que foi o país anfitrião das OIAM em 2007, será representado por uma equipa de quatro elementos, à semelhança dos anos anteriores. A organização das OIAM pelo Panamá insere-se nas comemorações dos 500 anos da descoberta do "Mar del Sur", o Oceano Pacífico.

A participação das delegações portuguesas nestas competições internacionais é organizada pela SPM, e a seleção e a preparação dos alunos está a cargo do Projecto Delfos, do Departamento de Matemática da Universidade de Coimbra.

ESCOLA DE **VERÃO** DA **SPM** ABRE PORTAS NO DIA **5 DE SETEMBRO**

Nos próximos dias 5, 6 e 7 de setembro, o Museu Nacional de História Natural e da Ciência, em Lisboa, acolherá mais uma edição da Escola de Verão da SPM (EVSPM2013), que este ano celebra a Matemática do Planeta Terra. Entre as diversas atividades que decorrerão ao longo dos três dias do encontro, os participantes poderão assistir a sessões plenárias e participar em mini cursos. "Matemática e o Google Earth", "Simetrias nas equações diferenciais", "Estrutura e dinâmica da população portuguesa" serão alguns dos temas tratados neste encontro dirigido a professores de matemática dos ensinos básico e secundário, investigadores e estudantes, bem como a todos aqueles que se interessam por matemática e suas aplicações. A organização do evento considera que a EVSPM2013 proporcionará à comunidade científica e escolar a oportunidade de explorar e discutir importantes aspetos da matemática, segundo a perspetiva da Matemática no Planeta Terra. As inscrições podem ser efetuadas na página oficial do evento, em *www.evspm2013.spm.pt.*

DUZENTAS **"VÍDEO-AULAS"** DE MATEMÁTICA À **DISTÂNCIA** DE UM **CLIQUE**

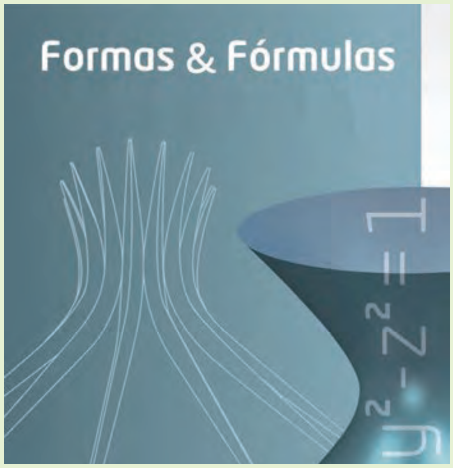
Já estão disponíveis em *http://fundacao.telecom.pt/*, de forma gratuita, cerca de 200 vídeos de matemática desenvolvidos pela Khan Academy, uma organização que disponibiliza vídeos interativos com conteúdos educativos. Em Portugal, a Fundação Portugal Telecom abraçou esta iniciativa, apoiando a adaptação para português dos vídeos, originalmente em inglês, de acordo com o currículo escolar nacional, contando com a colaboração da SPM para a certificação dos conteúdos. Até ao final do ano estarão disponíveis cerca de 400 vídeos, que abordarão essencialmente matérias dos 2.º, 4.º, 6.º, 9.º e 12.º anos. Em 2014, a Fundação PT espera disponibilizar cerca de 800 vídeos de matemática, física, química e biologia. Além do público português, o projeto pretende também chegar aos internautas dos Países Africanos de Língua Oficial Portuguesa e de Timor-Leste através do Sapo Internacional. Os vídeos, que procuram servir de reforço às matérias lecionadas na sala de aula, são narrados por Rogério Martins e por quadros da PT. O repositório da Khan Academy, criada em 2006 por Salman Khan, conta já com mais de quatro mil vídeos sobre matemática, física, química, história e economia, entre outras áreas.

CIÊNCIA À VOLTA DE UMA **MESA DE CAFÉ,** NO **MUHNAC**

No âmbito do Ano Internacional da Matemática do Planeta Terra, o Museu Nacional de História Natural e da Ciência (MUHNAC), em Lisboa, promove o World Cafe, uma iniciativa que pretende estimular o raciocínio em grupo, numa atmosfera informal, à volta de uma mesa de café. O ciclo arrancou em abril e decorrerá até dezembro. A próxima apresentação realiza-se no dia 28 de setembro, às 11 horas, e terá como tema "Modelos Matemáticos da Evolução – Darwin. Árvores Filogenéticas", por Fabio Chalub (FCTUNL). A 19 de outubro, António Machiavelo (FCUP) apresentará "Polaridade e Simetria – Forma, crescimento e função", e a 16 de novembro, Alberto Pinto (FCUP) falará sobre "Teoria dos Jogos – Altruísmo e mutualismo". Para fechar o ciclo, Tiago Domingos (ISTUNL) apresentará "Modelos Preditivos – Biodiversidade e conservação". A entrada é gratuita mas necessita de marcação prévia. O World Cafe tem o apoio da SPM.

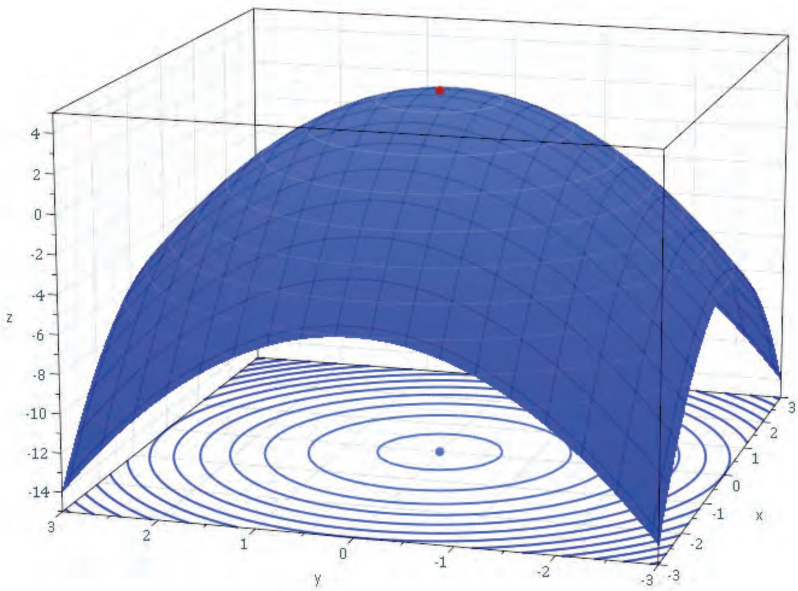
LANÇADO CATÁLOGO DA EXPOSIÇÃO **"FORMAS & FÓRMULAS"**

Foi lançado recentemente o catálogo da exposição "Formas & Fórmulas", patente no Museu Nacional de História Natural e da Ciência (MUHNAC) desde junho do ano passado. No catálogo agora publicado é possível fazer uma viagem pela exposição que mostra como imagens e conceitos da geometria e da álgebra interagem, relacionando fórmulas matemáticas com modelos geométricos, objetos de uso comum e formas de arquitetura. O período de permanência da exposição no MUHNAC foi prolongado até ao dia 29 de setembro de 2013.



***WORKSHOP* MMNSEA** REGRESSA À **UNIVERSIDADE DO MINHO**

No dia 13 de setembro, realiza-se mais uma edição do *Workshop* MMNSEA – Mathematical Modelling and Numerical Simulation for Engineering Applications, na Universidade do Minho. Durante o encontro, que decorrerá entre as 9h e as 17h, serão feitas diversas apresentações sobre a investigação realizada nas áreas de matemática aplicada e aplicações na engenharia. As inscrições para o *Workshop* MMNSEA2013 são gratuitas e podem ser feitas em: *http://w3.math.uminho.pt/mmnsea2013*



CONFERÊNCIA SOBRE OTIMIZAÇÃO NAS **CIÊNCIAS NATURAIS**

A discussão dos mais recentes desenvolvimentos na investigação em otimização e suas aplicações nas ciências naturais estará em destaque na EURO Mini-Conference on Optimization in the Natural Sciences, que se realizará na Universidade de Aveiro, de 5 a 9 de fevereiro do próximo ano. O encontro procurará promover a troca de conhecimentos e experiências entre investigadores nas áreas de computação científica, otimização e estatística e ainda física, química, biologia e ciências médicas. As inscrições para a conferência já se encontram abertas e o prazo para a submissão de comunicações termina a 1 de novembro de 2013.

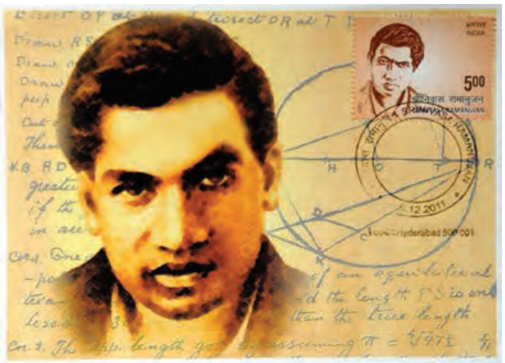
SEUL RECEBE **MAIOR ENCONTRO** DE MATEMÁTICOS **DO MUNDO** EM **2014**

A Coreia do Sul receberá o International Congress of Mathematicians (ICM) em 2014. O congresso, organizado de quatro em quatro anos pela International Mathematical Union, é o maior e mais importante encontro internacional de matemáticos. O programa do ICM 2014, que decorrerá entre 13 e 21 de agosto, incluirá uma grande variedade de atividades, nomeadamente sessões plenárias, comunicações, apresentações de *posters*, entre outras. Teoria dos números, geometria, topologia, análise e suas aplicações, sistemas dinâmicos, equações diferenciais parciais, física matemática, probabilidade e estatística são apenas algumas das áreas que serão abordadas ao longo dos oito dias em que decorrerá o ICM. Na cerimónia de abertura do congresso serão ainda divulgados os vencedores da Medalha Fields, assim como dos prémios Nevanlinna e Gauss. O ICM realizou-se pela primeira vez em 1897, em Zurique, cidade que já recebeu três vezes o congresso. A Coreia do Sul vai estrear-se como anfitriã no próximo ano, e a organização acredita que esta será uma experiência memorável para todos os participantes.

LAUREADOS E **JOVENS** BRILHANTES DA **MATEMÁTICA** JUNTOS NO **1.º HEIDELBERG LAUREATE FORUM**

Está já confirmada a presença de cerca de 40 laureados com os prémios Abel, Fields e Turing na primeira edição do Heidelberg Laureate Forum, que se realizará entre os dias 22 e 27 de setembro, na cidade de Heidelberg, na Alemanha. Durante o encontro, os grandes nomes da matemática e da computação científica reunir-se-ão com duas centenas de jovens cientistas com um percurso promissor nestas áreas, de 47 países distintos. Este fórum é promovido pela Klaus Tschira Stiftung (KTS), fundação alemã para a investigação, em parceria com o Heidelberg Institute for Theoretical Studies. O Heidelberg Laureate Forum segue o modelo da Reunião Anual de Lindau para laureados com o Prémio Nobel, criada há 60 anos para impulsionar a geração de novas ideias.

PRÉMIO RAMANUJAN 2013 ATRIBUÍDO A **YE TIAN**



O investigador chinês Ye Tian foi o contemplado com o Prémio Ramanujan 2013 para Jovens Matemáticos de Países em Desenvolvimento, atribuído pela International Mathematical Union e pelo Abdus Salam International Centre for Theoretical Physics. Ye Tian foi premiado pelo trabalho desenvolvido na Academia Chinesa de Ciências, que inclui o estudo dos pontos de Heegner e da conjetura de Birch e Swinnerton-Dyer, cujos resultados foram considerados um importante contributo para o campo da Teoria dos Números.

PIERRE DELIGNE DISTINGUIDO COM **PRÉMIO ABEL**

Fotografia de Cliff Moore

O Prémio Abel 2013 foi atribuído ao belga Pierre Deligne. O anúncio, feito pela Academia Norueguesa de Ciências e Letras no final do mês de março, destacava as importantes contribuições do investigador do Institute for Advanced Study, Princeton, New Jersey (EUA), para a área da geometria algébrica e o seu papel crucial para o desenvolvimento da Teoria dos Números, da Teoria de Representação e áreas similares. Ragni Piene, presidente da Comissão Abel, salientou a influência dos conceitos, ideias, resultados e métodos de Deligne para a geometria algébrica e para a matemática, em geral, acrescentando que o investigador nascido em Bruxelas "levou o 21.º problema de Hilbert a uma dimensão mais elevada". Entre as importantes contribuições de Deligne, de 68 anos, destaca-se a solução de uma das mais complexas conjeturas de Weil, análoga à hipótese de Riemann, que lhe valeu a atribuição da Medalha Fields, em 1978, pela International Mathematical Union, e do Crafoord Prize, 1988, pela Royal Swedish Academy of Sciences, em conjunto com Alexandre Grothendieck. Recentemente, Deligne, foi galardoado com o Balzan Prize (2004) e o com o Wolf Prize (2008), juntamente com Phillip Griffiths e David Mumford.

2013

tardes de MATEMÁTICA

Ponta Delgada
AÇORES

Biblioteca Pública e Arquivo
Regional de Ponta Delgada

15h30

Mais informações:
Sociedade Portuguesa de Matemática
217 939 785 www.spm.pt

www.tmacores.uac.pt

27 de abril

PARADOXOS: AMOR E ÓDIO

Francisco Martins, Departamento de Informática da Universidade de Lisboa
Maria do Carmo Martins, Departamento de Matemática da Universidade dos Açores

25 de maio

JOGOS E MATEMÁTICA

Sandra Vinagre, Departamento de Matemática da Universidade de Évora

21 de setembro

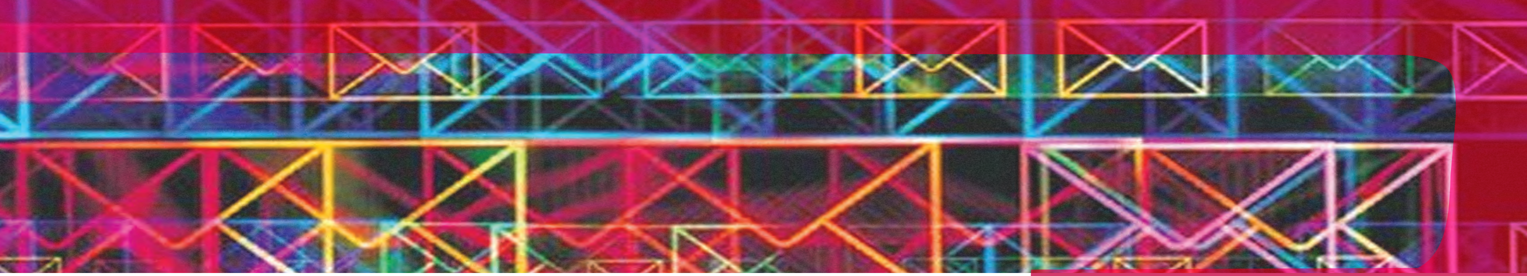
UMA AVENTURA NO MUNDO DOS PADRÕES

João Cabral, Departamento de Matemática da Universidade dos Açores

26 de outubro

ESTATÍSTICA: PARA QUE TE QUERO?

Áurea Sousa e **Osvaldo Silva**, Departamento de Matemática da Universidade dos Açores



Fernando Pestana da Costa
Vice-Presidente SPM
fernando.costa@uab.pt

ESCOLA DE **VERÃO** DA **SPM** E A **MATEMÁTICA** DO PLANETA **TERRA**

A iniciativa Matemática do Planeta Terra 2013 (*http://www.mpe2013.org)* foi apresentada aos leitores desta *Gazeta* na Carta da Direção do n.º 166, em março do ano passado. Aí ficou expresso o compromisso de dedicar a Escola de Verão de 2013 a esta temática. E como o verão já está entre nós e o prometido é devido, teremos em breve uma Escola de Verão da SPM totalmente dedicada à Matemática do Planeta Terra (*http://evspm2013.spm.pt/pt/*).

Organizada por Carla Martinho (ISCAL), João Teixeira Pinto (IST) e pelos dois vice-presidentes da SPM, Jorge Buescu (FCUL) e o autor desta Carta da Direção, Fernando Pestana da Costa (UAb), a Escola de Verão de 2013 é, desta vez, e contrariamente ao usual, uma iniciativa diretamente a cargo da direção da SPM. Contámos, naturalmente, com o apoio e a colaboração de diversas entidades na sua concretização: o Centro de Análise Matemática, Geometria e Sistemas Dinâmicos do IST, o Centro de Matemática e Aplicações Fundamentais da FCUL, o Museu Nacional de História Natural e da Ciência, a Fundação para a Ciência e a Tecnologia, a Agência Nacional para a Cultura Científica e Tecnológica "Ciência Viva", a Comissão Nacional da UNESCO, a Associação de Professores de Matemática, a Câmara Municipal de Lisboa e a Texas Instruments.

A Escola decorrerá entre 5 e 7 de setembro nas instalações do Museu Nacional de História Natural e da Ciência, em Lisboa, e consistirá em oito comunicações plenárias e seis minicursos sobre variadíssimos tópicos relativos à Matemática do Planeta Terra. Entre as catorze apresentações, os participantes ficarão a conhecer: a matemática por detrás do GPS e do Google Earth, a utilização da estatística para a modelação dos fogos florestais em Portugal, os instrumentos matemáticos usados nos estudos demográficos portugueses, ou na análise de vibrações sísmicas e suas aplicações à engenharia civil, ou a matemática dos recursos biológicos, dos mercados competitivos, e muitos outros aspetos da utilização da matemática para o estudo do planeta onde vivemos e dos seres que nele habitam.

A Escola de Verão deste ano contará também com a novidade de ser acompanhada por um "texto de apoio". De facto, durante a Escola decorrerá a sessão de lançamento do livro *Matemática do Planeta Terra*, publicado pela IST Press (*http://www.istpress.ist.utl.pt/lmatematica_planeta_terra.htm*) e editado por três dos quatro organizadores da Escola. Não sendo exatamente uma versão escrita da Escola, a intersecção das duas iniciativas não é nem residual nem fruto do acaso: das 14 sessões da Escola de Verão, 12 refletem capítulos do livro e são proferidas pelos seus autores; mas, além destas, o livro tem mais cinco capítulos sobre temas da Matemática do Planeta Terra que não serão abordados na Escola (como a modelação climática, a prospeção geofísica, ou a epidemiologia). Assim, todos os participantes cujo apetite por estes assuntos for despertado pelo que virem e ouvirem na Escola poderão, no livro, não só recordar e aprofundar o que viram, como partir para outras explorações!

Mas a Escola terá ainda outros eventos: uma visita guiada à belíssima exposição temporária "Formas e Fórmulas", patente no Museu, o lançamento de um postal dos CTT alusivo à Matemática do Planeta Terra, uma mostra de trabalhos sobre estes assuntos submetidos por escolas e realizados no âmbito de qualquer disciplina ou ano letivo (*http://evspm2013.spm.pt/pt/outras*).

Espera-se, portanto, uma animada Escola de Verão: uma excelente forma de acabarmos as férias e de iniciarmos um novo ano letivo, rodeados por matemática e por ciência num ambiente descontraído.

Até breve!

Gazeta de Matemática

FUNDADA POR: **António Monteiro • Bento Caraça • Hugo Ribeiro • J. Silva Paulo • M. Zaluar Nunes**

POLÍTICA EDITORIAL DA GAZETA DE MATEMÁTICA:

A Gazeta de Matemática continua a ser, tal como acontece desde a sua fundação em 1939, o principal elo de ligação da Sociedade Portuguesa de Matemática com a comunidade matemática portuguesa.

A Gazeta de Matemática é uma publicação essencialmente de divulgação da cultura matemática. Pretende estimular o gosto pelo estudo da matemática assim como a troca de ideias entre quem estuda, ensina, investiga, usa ou simplesmente se interessa pela matemática.

A Gazeta de Matemática publica artigos submetidos espontaneamente, artigos convidados e secções permanentes.

Incentivamos os nossos leitores a enviarem textos para publicação na Gazeta de Matemática. Damos preferência a artigos curtos (4 a 6 páginas) sobre temas que tenham interesse para o nosso público: algo relacionado com um tema de investigação que possa ser explicado à comunidade matemática em geral, algum aspecto curioso de matemática menos conhecido, uma nova perspectiva sobre um tema do interesse do leitor ou simplesmente algo que tenha uma ligação com o mundo matemático.

Os artigos poderão ser submetidos à apreciação de um ou mais especialistas com o objectivo de obter um parecer sobre a sua adequação para publicação na Gazeta de Matemática.

Os textos podem ser submetidos em **LaTeX** ou em **Word** (com uma versão em **PDF**). No caso de o documento conter muitas fórmulas aconselhamos o primeiro formato. Deve submeter o texto, junto com as imagens, para o seguinte endereço: ***gazeta@spm.pt.***

ASSINATURA DA GAZETA PARA O ANO 2013

Preço de Capa (avulso) + portes de envio	Assinatura				Assinatura para sócios SPM	Assinatura de Apoio
	Portugal	Europa	Guiné-Bissau S. Tomé e Príncipe Timor Leste	Resto do Mundo		
4.2€	12€	15€	12€	17€	0€	≥ 17.5€

A SPM disponibiliza na página **http://www.spm.pt/carreira/carreira.phtml** informação sobre emprego e carreira para matemáticos. As pessoas interessadas em incluir anúncios neste site devem enviar um email com os dados para *imprensa@spm.pt*

VISITE O SITE DA **SOCIEDADE PORTUGUESA DE MATEMÁTICA**

www.spm.pt

E O DA ***GAZETA DE MATEMÁTICA***

www.gazeta.spm.pt

Sociedade Portuguesa de Matemática • Av. da República 45, 3° esq. • 1050-187 Lisboa • Telf.: 21 793 97 85 • Email: *spm@spm.pt*

VISITE A LOJA SPM EM *WWW.SPM.PT*

NOVIDADE!

Textos de Matemática
FCUL