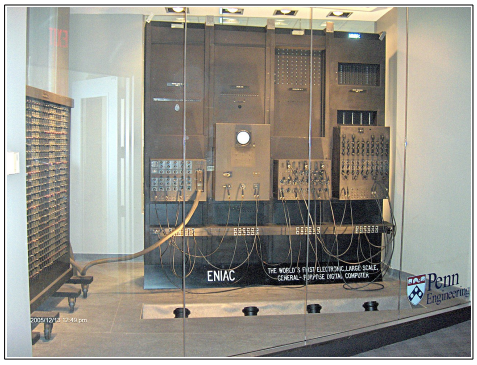
Boletim Lavrense de Matemática

Edição 9, 6 de maio de 2022



ENIAC. Fonte: ***Wikipédia***

Matemática, computação e a guerra

No início do século XX, lápis e papel eram os principais instrumentos do matemático. Com o desenrolar da Segunda Guerra Mundial, por volta de 1940, numerosos matemáticos foram convocados para atuar no esforço de guerra e a situação mudou. Juntamente com outros cientistas, como físicos e engenheiros, os matemáticos desempenharam um importante papel no desenvolvimento do computador eletrônico digital automático, um marco para a ciência da computação. Na reportagem especial desta edição contamos um pouco do surgimento dos primeiros computadores eletrônicos.

HOMENAGEM

Maio: um mês para celebrar

O mês de maio é marcado por importantes datas para a comunidade matemática brasileira. O dia 06 de maio é considerado o Dia Nacional da Matemática em homenagem a Malba Tahan, e o dia 12 de maio o dia Internacional das Mulheres na Matemática, em homenagem à matemática iraniana Maryam Mirzakhani.

Nós, editores do Boletim Lavrense de Matemática, homenageamos todas as pessoas que se aventuraram pelo maravilhoso mundo da Matemática.

CURIOSIDADES

Comunicação e criptografia

Com o aumento das formas de comunicação e em particular o aparecimento das redes sociais, a proteção das informações é cada vez mais importante. Essa necessidade de criptografar as comunicações não é algo novo, na Roma antiga o general Júlio César utilizava o Código de César. Outro código interessante é o Código Morse. Esses códigos foram de suma importância em determinadas épocas, pois enquanto um era um meio de comunicação que permitia que nem todos que lessem pudessem compreender o que se estava querendo dizer, o outro pelo contrário, tinha a intenção de simplificar a comunicação. Na seção Curiosidades explicamos melhor os códigos de César e de Morse.

– ... – – – . – . – .. . .. – .. – . – . .–

Índice

Matemática e computadores pág. 2

Curiosidades pág. 4

Projeto de Extensão pág. 5

Sugestões audiovisuais pág. 5

Desafios Matemáticos pág. 6

Contatos

Site: www.dmm.ufla.br/matematicaemtodolugar
e-mail: boletimdamatematica.dmm@ufla.br
Instagram: www.instagram.com/boletimlavrensedematematica

EDITORES
DMM/UFLA
Ana Claudia Pereira
Graziane Sales Teodoro
Helvécio G. F. Filho
Julia Terra Souza
Ricardo Edem Ferreira

ESPECIAL

Matemática e computadores

No período de 1939 a 1945 a humanidade viveu a guerra mais abrangente da história: a Segunda Guerra Mundial. A guerra envolveu a maioria das nações do mundo, incluindo todas as grandes potências, organizadas em duas alianças militares opostas: os Aliados e o Eixo.

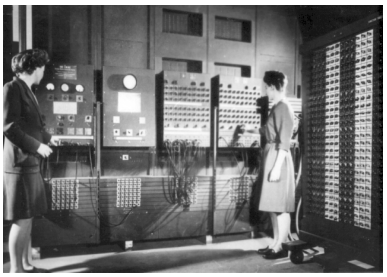
Enquanto muitas pessoas iam para a linha de frente, viver o horror da guerra, um grande número de cientistas, entre eles muitos matemáticos, foram convocados para estabelecimentos de pesquisa do governo, onde trabalharam em projetos secretos que também contribuíram para o esforço de guerra dos Aliados.

Na Grã-Bretanha o estabelecimento secreto de guerra foi a Escola de Código e Cifra do Governo em *Bletchley Park*. Até a década de 1970 poucas pessoas estavam cientes da atividade de quebra de códigos que havia lá durante a guerra.

Tanto a Grã-Bretanha quanto os Estados Unidos tinham grande interesse em pesquisas sobre radar. O desafio era melhorar a precisão e o alcance na identificação de alvos.

Em 1945, com o fim do conflito, vários cientistas desses estabelecimentos de pesquisa britânicos e americanos visitaram as organizações uns dos outros e trocaram ideias e experiências. Um dos frequentes assuntos discutidos por tais cientistas era a tarefa de realizar os cálculos e simulações necessários para o desenvolvimento de armas e a produção de equipamentos militares. Durante a guerra, esses cálculos foram feitos em máquinas digitais e analógicas, grandes e pequenas, a grande maioria dessas máquinas eram mecânicas ou eletromecânicas. Nos Estados Unidos, um grupo de pesquisa em particular decidiu superar as deficiências das calculadoras eletromecânicas lentas introduzindo técnicas eletrônicas de alta velocidade. Assim em 1945, na Pensilvânia, despontava a era da computação digital eletrônica.

Com a necessidade de acelerar o processo de preparação de mesas de tiro balístico para artilharia, uma enorme calculadora eletrônica chamada ENIAC (Computador Integrador Numérico Eletrônico) foi desenvolvida, sob um contrato do governo dos Estados Unidos na *Moore School of Electrical Engineering* da Universidade da Pensilvânia.



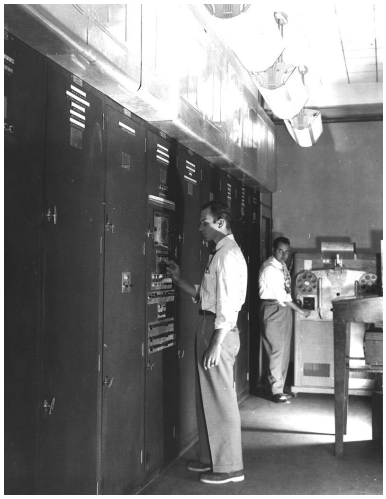
ENIAC
Fonte: *Wikipédia*

À medida que o trabalho de construção da ENIAC avançava, um respeitado matemático húngaro da Universidade de Princeton, John von Neumann (1903 - 1957), foi também inserido no projeto.

John von Neumann
Fonte: *Wikipédia*

Desde muito jovem von Neumann foi reconhecido por seu talento matemático. Isso permitiu que obtivesse um doutoramento em matemática em Budapeste praticamente estando ausente, uma vez que passava seu tempo em Zurique e Berlim. Sua carreira no ensino começou na Alemanha onde esteve por três anos, de 1927 a 1930, nas universidades de Berlim e Hamburgo. Em 1930 mudou-se para Princeton, onde ficou ligado à Universidade de Princeton até ser convidado a tornar-se membro do *Institute for Advanced Study* em 1933. Em 1943 o governo dos Estados Unidos continuava a recrutar gênios, e como tal, von Neumann foi contratado. Por volta de 1948 von Neumann usou o ENIAC para cálculos associados ao desenvolvimento da bomba de hidrogênio, e em 1955 foi designado para a Comissão de Energia Atômica.

Mesmo antes de finalizar a construção da ENIAC, a equipe já estava produzindo ideias para um computador sucessor, o EDVAC (Computador Automático de Variável Discreta Eletrônica).



EDVAC
Fonte: *Wikipédia*

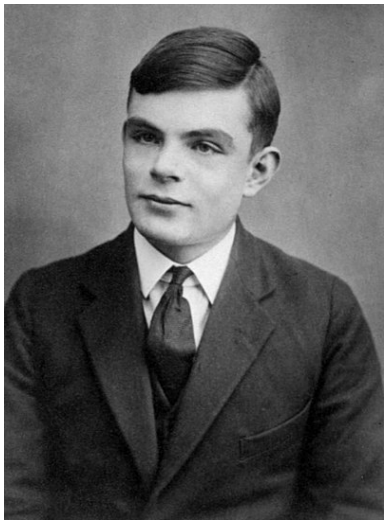
O desafio era: como tornar o ENIAC, de propósito mais geral, para que seus benefícios pudessem ser mais facilmente aplicados a uma gama muito maior de tarefas computacionais. As ideias foram escritas por von Neumann em junho de 1945 em um documento de 101 páginas intitulado *First draft of a report on the EDVAC*. Em 1946, cópias deste relatório já estavam sendo amplamente distribuídas e lidas com interesse por toda parte. Ainda em 1946, um projeto para construir o EDVAC foi lançado, mas a máquina só entrou em operação em 1951. O Relatório EDVAC de 1945 continha o primeiro relato amplamente disponível do que agora é conhecido como um computador digital eletrônico de programa armazenado de propósito geral, mas sem detalhes de engenharia. O EDVAC tornou-se formalmente conhe-

cido como um computador de programa armazenado porque uma única memória era usada para armazenar as instruções do programa e os dados. O conceito de programa armazenado é a base de quase todos os computadores atuais. As máquinas que estão em conformidade com o padrão EDVAC também são às vezes chamadas de computadores von Neumann, para reconhecer a influência do autor do relatório.

Com o fim do conflito armado o desejo de consolidar as ideias de guerra da *Moore School* e de explicar os detalhes para um público americano mais amplo tomou forma, e assim, o governo dos Estados Unidos financiou um curso de oito semanas de palestras durante os meses de julho e agosto de 1946 sobre a Teoria e Técnicas para Projeto de Computadores Digitais Eletrônicos. Vinte e oito cientistas e engenheiros foram convidados a participar, entre estes apenas três ingleses. O Relatório EDVAC e as palestras da *Moore School* foram a inspiração para vários grupos em todo o mundo considerarem projetar seus próprios computadores eletrônicos de uso geral.

O matemático britânico Alan Turing (1912 - 1954) foi provavelmente o mais brilhante da equipe de pessoas recrutadas para trabalhar na *Bletchley Park*. Recém chegado de um doutorado nos Estados Unidos, acredita-se que Turing foi um dos primeiros matemáticos a ser recrutado em 1939, devido a um artigo teórico que ele havia escrito em 1935-6, intitulado *On Computable Numbers, with an application to the Entscheidungsproblem*. O *Entscheidungsproblem* (termo alemão para "problema de decisão") é um problema da lógica simbólica que consiste em achar um algoritmo genérico para determinar se um dado enunciado da lógica de primeira ordem pode ser provado.

Alan Turing era um homem notável e original, bastante indiferente à autoridade, convenção ou burocracia. Embora classificado como matemático e lógico, ele explorou áreas tão diversas quanto inteligência artificial e morfogênese (o crescimento e a forma dos seres vivos). Atualmente Turing é considerado o pai da ciência da computação teórica e da inteligência artificial.



Alan Turing aos 16 anos.
Fonte: *Wikipédia*

Em linguagem simples, em seu artigo Turing abordava um dos importantes problemas filosóficos e lógicos da época: "A matemática é decidível?". Essa questão havia sido colocada por estudiosos interessados em descobrir o que poderia e o que não poderia ser provado por uma determinada teoria matemática. Para raciocinar sobre esse chamado *Entscheidungsproblem*, Turing teve a ideia de usar um dispositivo de cálculo automático conceitual. O dispositivo era um processo passo a passo que manipulava símbolos de acordo com uma pequena lista de instruções muito básicas. É interessante observar que o processo proposto por Turing é uma descrição de um computador moderno.

Tendo em vista o trabalho teórico e o interesse de Turing por cifras, ele foi enviado para *Bletchley Park* em 4 de setembro de 1939, e foi imediatamente colocado para trabalhar decifrando os códigos da Enigma Naval Alemã. Enigma foi uma máquina eletromecânica de criptografia com rotores, utilizada tanto para criptografar como para descriptografar códigos de guerra. E Turing conseguiu cumprir a tarefa que lhe foi atribuída. Foi dito que, à medida que *Bletchley Park* crescia em tamanho e importância, a grande contribuição de Turing foi encorajar os outros decifradores de código nas equipes a pensar em termos de probabilidades e quantificação do peso da evidência. Por causa desse e de outros *insights*, Turing rapidamente se tornou a pessoa a quem todos os outros matemáticos de *Bletchley Park* se voltaram quando encontraram um problema de descriptografia particularmente complicado.

Com base em seu trabalho teórico anterior, Turing foi recrutado pelo *National Physical Laboratory* (NPL) em Teddington em outubro de 1945. A equipe sênior da NPL tinha ouvido falar do ENIAC e do EDVAC e desejava construir seu próprio computador digital de uso geral. Embora estivesse bem ciente dos desenvolvimentos na *Moore School* e conhecesse von Neumann pessoalmente, Turing geralmente não estava inclinado a seguir os planos de qualquer outra pessoa. Em três meses, ele havia esboçado o projeto completo de seu próprio computador de programa armazenado de uso geral, no qual adotou a notação e a terminologia usadas no Relatório EDVAC. O projeto de Turing, chamado ACE (Mecanismo de Computação Automática), deu origem ao primeiro computador projetado no Reino Unido. A primeira versão construída do ACE foi a Pilot ACE, uma implementação menor do projeto original. A versão completa só foi construída mais tarde, em fins dos anos 1950 e ficou operacional em 1957.

Válvulas do Pilot ACE.
Fonte: *Wikipédia*

Já no final da década de 1940, o trabalho ativo em computadores digitais eletrônicos de alta velocidade não era exclusividade da Grã-Bretanha. Havia pelo menos uma dúzia de projetos pioneiros na América. Na Alemanha, Konrad Zuse projetou uma série de computadores eletromecânicos engenhosos entre 1938 e 1945, mas estes foram máquinas controladas por sequência e não com programa armazenado.

Referência:

Alan Turing and his contemporaries. Building the world's first computers, Simon Lavington. BCS, 2012. ■

CURIOSIDADES

Cifra de César e Código Morse

Júlio César foi um grande líder militar e político romano de 60 a.C a 44 a.C. Para se comunicar com seus generais César muitas vezes usava o código que ficou conhecido como Código de César ou Cifra de César em sua homenagem. Esse código era utilizado para proteger mensagens enviadas a seus generais, assim, se essa mensagem caísse em mãos inimigas, a informação não poderia ser compreendida, e uma vez que muitos dos seus inimigos eram analfabetos e outros não conheciam a língua, acredita-se que o código passava um mínimo de segurança. O Código de César era um sistema simples de substituição, no qual cada letra da mensagem original era trocada pela letra que se situava em três posições à sua frente. Por isso, qualquer código em que haja substituição de uma letra por outra com deslocamento fixo, é considerado um Código de César.

Original	ABCDEFGHIJKLM
Cifrado	DEFGHIJKLMNOP
Original	NOPQRSTUVWXYZ
Cifrado	QRSTUVWXYZABC

Por exemplo:

Matemática em todo lugar.
Pdwhpdwlfd hp wrgr oxjdu.

Temos ainda algumas melhorias que podem ser aplicadas ao Código de César, como a Cifra Monoalfabética, que consiste em trocar cada letra por uma outra letra qualquer, sem seguir um padrão, assim, existem 26! formas de combinação (permutação de 26 letras) possíveis, o que dificultaria a obtenção do texto original. Exemplo:

Original	ABCDEFGHIJKLM
Cifrado	UMGSCWXZFPBNT
Original	NOPQRSTUVWXYZ
Cifrado	KHEYOVRDIAJLQ

Por exemplo:

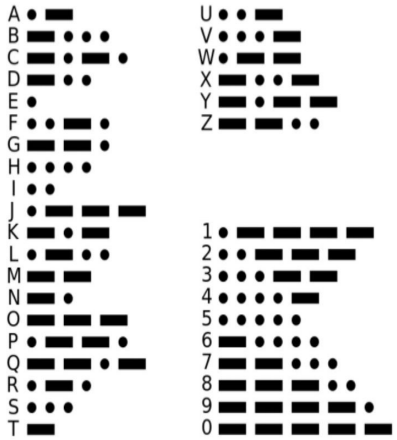
Matemática em todo lugar.
Turcturfgu ct rhsh ndxuo.

Até 1915, a Cifra de César continuava em uso: o exército russo empregou-a em substituição às cifras mais complicadas que provaram serem muito difíceis de suas tropas entenderem; no entanto, criptoanalistas alemães e austríacos tiveram pouca dificuldade em descriptografar suas mensagens. Atualmente, Cifras de César podem ser encontradas em brinquedos infantis, como os anéis decodificadores.

Outro código muito conhecido, é o Código Morse, que é um sistema binário de representação à distância de números, letras e sinais gráficos, utilizando-se de sons curtos e longos, além de pontos e traços para transmitir mensagens. Foi criado por Samuel Morse (1791-1872), que foi um pintor e físico norte-americano, responsável pela invenção deste código em 1835, porém sua primeira transmissão só ocorreu quase 10 anos depois, em 1844, quando foi apresentado o telégrafo - que também foi desenvolvido por Morse. Esse sistema é composto por todas as letras do alfabeto latino e todos os algarismos de 0 a 9. Os caracteres são representados por uma combinação específica de pontos e traços, conforme exposto na tabela a seguir. Para formar as palavras, basta realizar a combinação correta de símbolos. As mensagens são transmitidas por meio de intervalos de som (apito) ou luz (lanterna), podendo ser captadas por diversos aparelhos, como, por exemplo, o radiotelégrafo e o telégrafo. Morse criou o sistema de acordo com a frequência que cada letra era usada em inglês, porém, modificações foram desenvolvidas na Alemanha em 1948 a fim de tornar o Código Morse um padrão mundial, assim, o Código Morse é descrito pelos caracteres apresentados na tabela abaixo.

Código Morse Internacional

1. O comprimento de um ponto é uma unidade.
2. Um traço são três unidades.
3. O espaço entre partes da mesma letra é uma unidade.
4. O espaço entre as letras é de três unidades.
5. O espaço entre as palavras é de sete unidades.



Código Morse
Fonte: *Wikipédia*

Esse meio de comunicação foi muito utilizado por marinheiros durante o século XIX, porém, já no final desse século e com a invenção do telefone, o Código Morse perdeu espaço nas comunicações pessoais, mas algumas de suas combinações tornaram-se tão famosas que ainda são usadas. É o caso do SOS (sequência de: ponto-ponto-ponto barra-barra-barra ponto-ponto-ponto). O SOS é usado para sinalizar perigo e muito traduzido como "save our souls" e "save our ship" (salvem nossas almas e salvem nosso barco, respectivamente, na tradução do inglês). Mas, na verdade, não se tratava de uma abreviação e, sim, de uma combinação fácil de ser memorizada. A sequência foi uma das tantas que surgiram com a ideia de simplificar a comunicação.

Referência:
GTA UFRJ. Princípios de Criptografia. Disponível em: www.gta.ufrj.br. Acesso em: 11 abr. 2022. ■

PROJETO DE EXTENSÃO

Iniciação ao Xadrez

Você sabia que a prática do jogo de xadrez nas escolas é uma atividade que, além de propiciar lazer, também permite valorizar o raciocínio por meio de uma atividade lúdica? Dentre os vários benefícios desta prática para a cognição, podemos citar: desenvolver o raciocínio lógico; aprimorar habilidades de observação, memorização, reflexão, análise e síntese; aperfeiçoar habilidades necessárias à tomada de decisões; solucionar problemas pela análise do contexto em que estão inseridos; melhorar o desempenho nos estudos, em particular, em Matemática e suas linguagens. Além disso, as características de outras práticas esportivas como o fortalecimento da determinação, da ética e do caráter são bastante trabalhadas.

Tendo em vista a importância desta modalidade, o projeto "Iniciação ao Xadrez", coordenado pelo Professor Júlio Sílvio de Sousa Bueno Filho do Departamento de Estatística (DES) da Universidade Federal de Lavras- UFLA ocorre desde 2003. Este projeto tem como objetivo aumentar o interesse dos estudantes pelo jogo de xadrez e oferecer aos professores do ensino fundamental e médio de Lavras e região uma proposta didático-pedagógica que envolve o ensino de xadrez para crianças em idade escolar.

Para obter mais informações, você pode encaminhar um e-mail para `jssbueno@ufla.br`.

Nós, editores do Boletim Lavrense de Matemática, agradecemos ao Professor Júlio Bueno que gentilmente colaborou para essa reportagem. ■

SUGESTÕES AUDIOVISUAIS

Filmes, séries, matemática, xadrez e muito mais

O Jogo da Imitação

O Jogo da Imitação, vencedor do Oscar de melhor roteiro adaptado em 2015, é baseado no livro *Alan Turing: The Enigma* que conta a vida do matemático Alan Turing. Durante a Segunda Guerra Mundial, o governo britânico criou uma equipe de cientistas com o objetivo de decifrar a Enigma, a criptografia utilizada pelos alemães. O brilhante matemático Turing acaba se tornando o líder da equipe. O objetivo de Turing era construir uma máquina capaz de decodificar a criptografia alemã de modo que as informações pudessem ser usadas para mudar o rumo da guerra.

Fonte: adorocinema.com

O Matemático

O Matemático conta a história de Stanislaw Marcin Ulan um brilhante matemático judeu polônes. Então com 30 anos em 1942 Stan teve problemas com sua bolsa de estudos na Universidade de Harward. Stan aceita então uma proposta de emprego do seu melhor amigo Johnny que o leva para o Novo México com sua esposa Françoise, onde ele acaba trabalhando em projeto ultra secreto para a construção da bomba atômica. Enquanto sua vida particular segue, Stan e Johnny se juntam para criar o primeiro computador que deu origem a era digital.

Fonte: adorocinema.com

O Gambito da Rainha

A minissérie de 2020, conta a história da brilhante enxadrista Beth Harmon. Orfã, Beth tenta resolver seus problemas e vencer seus vícios enquando aprimora suas habilidades no xadrez. O Gambito da Rainha, estrelada por Anya Taylor-Joy, se tornou a minissérie mais vista da história da Netflix. A minissérie venceu as categorias de Melhor Roteiro para Scott Frank e Melhor Minissérie no Emmy Awards em 2021.

Fonte: adorocinema.com

■

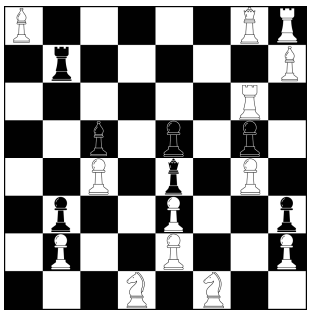
DESAFIOS

Desafios da Edição

Envie sua resolução dos desafios desta seção para nosso e-mail. A mais criativa será divulgada na próxima edição do Boletim.

1) Vimos na reportagem Curiosidades, desta edição, sobre a criptografia de César. Definimos a chave como a palavra que é inserida no início do alfabeto para que sejam embaralhadas as letras na criptografia de César. Usando o alfabeto de 26 letras e uma chave, uma palavra foi codificada em: NJCAHT. Qual é esta palavra? Dica: a chave usada foi o nome de um matemático famoso.

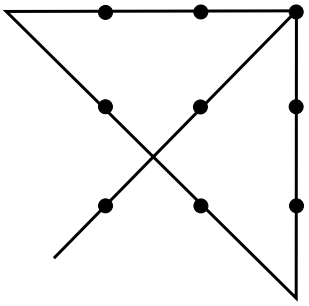
2) Nosso segundo desafio é no tabuleiro de xadrez. Faça um movimento com as peças brancas de modo que não resulte em um xeque mate.



Referência:
My best mathematical and logic puzzles, Martin Gardner. Dover, 1994.

Respostas dos desafios da edição anterior (acesse aqui a 8ª edição)

Desafio 1: Uma possível solução está mostrada na figura (neste problema devemos pensar fora da caixa!).



Desafio 2: A resposta é 99! As pessoas podem combinar de responder "branco" se o número de chapéus pretos à sua frente for par e "preto" se o número de chapéus pretos à sua frente for ímpar. Desse modo, se a última pessoa da fila (que será a primeira a responder) falar "branco", por exemplo, o número de chapéus pretos à sua frente será par. Se a penúltima pessoa (a segunda a responder) enxergar um número par de chapéus pretos é porque seu próprio chapéu é branco. Se ela enxergar um número ímpar de chapéus pretos é porque seu próprio chapéu é preto. A pessoa seguinte sabendo da estratégia também conseguirá acertar seu chapéu. E assim por diante, até a primeira pessoa. Portanto, apenas a primeira pessoa a responder que não terá certeza de acertar a cor do próprio chapéu. ■

Participação

O Boletim Lavrense de Matemática quer ouvir você. Envie-nos sugestões de reportagem, sua opinião, correções e dúvidas através de nosso e-mail.