

CINEMA, MATEMÁTICA E CRIPTOGRAFIA

Adalberto A. Dornelles Filho¹

Raquel Milani²

Rosana Maria Gessinger³

Resumo

Educar na/para a diversidade implica propor atividades de ensino que busquem envolver a turma toda, de tal forma que todos sintam-se desafiados e possam avançar na construção de conhecimentos, de acordo com seus interesses e possibilidades. Pretendemos, no minicurso, apresentar uma atividade de ensino que busca, a partir da exibição de um episódio de uma série de TV a cabo, motivar os alunos para assuntos relacionados à Matemática e com isso dar condições para que possam ampliar os conhecimentos de acordo com seus interesses e possibilidades. Serão abordados temas que julgamos ser atuais e de interesse dos alunos, tais como o sigilo dos códigos na internet.

Palavras-chave: criptografia, internet, hipótese de Riemann.

Introdução

Ensinar matemática nos dias de hoje é uma tarefa que exige cada vez mais estratégias que despertem no aluno o desejo de aprender. Ao planejar as aulas, é importante reconhecer os alunos como seres únicos e singulares e valorizar suas diferenças, reconhecendo-as como fator de enriquecimento para o ensino e não como algo que precisa ser superado. Isso representa um desafio na medida em que exige redimensionamentos no pensar e no agir do professor.

Motivados pela idéia de contemplar um número cada vez maior de alunos em nossas aulas através de atividades de ensino diversificadas, envolvendo temas atuais, desenvolvemos uma atividade na Universidade de Caxias do Sul, em outubro de 2005, com alunos(as) dos cursos de Licenciatura em Matemática e Engenharia, na qual buscamos oportunizar a ampliação do conhecimento matemático a partir da exibição de um vídeo. No presente minicurso pretendemos compartilhar a atividade com os(as) colegas e explorar os limites e possibilidades da proposta.

Atividades a serem desenvolvidas

Inicialmente iremos fazer um breve relato da atividade desenvolvida com nossos alunos, que originou o presente minicurso. A seguir, exibiremos (em vídeo VHS) o episódio *Primeiro Suspeito*, da série NUMB3RS, produzido pela CBS norte-americana e transmitido

¹ aadorneff@ucs.br – professor da UCS

² rmilani@ucs.br – professora da UCS

³ rmgessinger@uol.com.br – professora da UCS e FAPA

no Brasil por TV a cabo no canal Telecine Premium. Seguem abaixo as sinopses da série e do episódio, que foram traduzidas a partir dos originais disponíveis no site www.cbs.com.

NUMB3RS é um drama sobre um agente do FBI que recruta seu irmão (um gênio da matemática) para ajudá-lo a resolver uma ampla variedade de crimes desafiadores em Los Angeles. Os dois irmãos atuam nos casos criminosos mais nebulosos a partir de uma perspectiva bastante distinta. Inspirados em casos reais, a série retrata o modo como a confluência entre trabalho policial e matemática proporciona revelações inesperadas e respostas para as mais surpreendentes questões criminais.

Episódio 5: Prime Suspect. Quando uma garotinha de cinco anos é raptada em plena festa de aniversário, Don e Terry iniciam uma investigação mas necessitam da ajuda de Charlie já que o pai da garota é também matemático. Charlie descobre o motivo do rapto quando Ethan revela que conseguiu provar a hipótese de Riemann, um difícil problema matemático. A solução do problema pode não apenas ser premiada com 1 milhão de dólares como ainda quebrar códigos de segurança na internet, revelando o maior segredo financeiro do mundo.

Após a exibição do filme, faremos um levantamento das dúvidas e questões sobre o tema do filme. A seguir, discutiremos as questões levantadas e faremos uma apresentação sobre dois temas abordados pelo episódio: a *Hipótese de Riemann* e a *Criptografia*. O objetivo da apresentação é esclarecer os termos usados e discutir o que é fato e o que é ficção no filme. Apresentamos abaixo uma breve síntese do que será exposto.

A Hipótese de Riemann: a função zeta de Riemann é a função de variável complexa s , definida no semi-plano $\Re(s) > 1$ pela série $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ e definida em todo C por continuação analítica. A Hipótese de Riemann (HR) consiste em afirmar que os zeros não-triviais de ζ possuem parte real $1/2$. A veracidade da HR é um problema em aberto desde 1859. O Clay Mathematics Institute (www.claymath.org) oferece um prêmio de US\$ 1.000.000 a quem resolver esse problema.

A HR é importante pois fornece uma excelente aproximação para a função $\pi(x)$, definida como quantidade de números primos menores ou iguais a x . Obter uma expressão para $\pi(x)$ é um importante problema em aberto. Além disso, na Teoria dos Números (e em outras áreas da Matemática) muitas hipóteses começam com “Se a HR for válida, então ...”.

Criptografia: a palavra *criptografia* vem do grego *kriptós* (escondido, oculto) – *grápho* (escrever). É a arte (técnica) de escrever mensagens cifradas. Alguns marcos:

- Código de César (~50 a.C.): cada letra da mensagem é trocada por sua subsequente no alfabeto. Por exemplo, MATEMATICA → NBUFNBUJDB.
- Enigma (~1940): durante a 2ª Guerra Mundial, os submarinos alemães codificavam mensagens usando um dispositivo eletro-mecânico. O matemático inglês Alan Turing liderou a equipe que “quebrou” o código alemão e permitiu a “virada” da guerra submarina no Atlântico.
- Internet (~1990): a segurança das transações comerciais via computador se desenvolve a partir da criação de sistemas de criptografia seguros e eficientes, entre eles o sistema RSA, uma técnica desenvolvida em 1978. (RIVEST, SHAMIR, ADLEMAN, 1978).

O processo RSA está fundamentado no fato de que dados dois números primos grandes, digamos p e q , é muito fácil (sob certas condições) obter $z = pq$, basta multiplicá-los. No entanto, é muito difícil (sob certas condições) fazer o processo inverso, isto é, fatorar o composto z . (COUTINHO, 2000).

A grande questão levantada pelo filme é: “Se a HR for verdadeira, os sistemas de criptografia serão ‘quebrados’?”. Há duas respostas para essa pergunta. Diretamente, a resposta é não, pois a HR (válida ou não) não está associada às técnicas de fatoração. Indiretamente, talvez, pois o processo de validação da HR pode desenvolver técnicas matemáticas que “iluminem” o problema da fatoração.

Após a exposição oral apoiada em lâminas que serão projetadas, proporemos uma atividade prática envolvendo criptografia. Os participantes, em grupos, serão convidados a criptografar uma palavra utilizando conhecimentos de Álgebra Matricial (produto matricial e matriz inversa). As mensagens codificadas serão trocadas entre os grupos, que deverão realizar o procedimento inverso, ou seja, descriptografá-las.

Para finalizar, promoveremos um debate sobre a atividade realizada, levantando questões sobre a viabilidade de sua utilização em uma aula de Matemática do ensino médio, os objetivos de uma atividade como essa, as posturas e ações que poderão ser despertadas nos alunos a partir de uma atividade como essa, entre outras.

Referências bibliográficas

COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2ed. Rio de Janeiro: IMPA/SBM, 2000.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. M. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 21(2):120-126, 1978.