Explorando os números primos e uma das suas aplicações atuais: a criptografia

Adriana Xavier Freitas[1], Vivian da Silveira Miranda[2]
PROFMAT UFLA, Lavras, MG

Resumo. Os números primos são um grande mistério na Matemática, com grandes questionamentos e curiosidades sobre eles. Será que existe uma função que nos fornece todos os números primos? Como saber se um determinado número é primo ou não? Qual a utilidade dos números primos? Perguntas como essas nos motivaram a escrever sobre esse tema pouco discutido na educação básica e de tamanha importância, principalmente nos dias de hoje. Uma de suas aplicações, que tem influência direta no nosso dia a dia, é na criptografia. Quando fazemos uma transação bancária, mandamos uma mensagem ou até mesmo escrevemos um bilhete em códigos, estamos usando a criptografia e consequentemente a Matemática. O objetivo deste trabalho, em um primeiro momento, é discutir conceitos sobre números primos, funções que os geram, testes de primalidades, primos especiais e alguns teoremas fundamentais sobre eles. Em seguida, são abordadas as criptografias RSA e ElGamal. Por último são propostas atividades para despertar o interesse dos alunos dos anos finais do Ensino Fundamental e do Ensino Médio e reforçar a importância da Matemática na vida de todos. O objetivo da primeira atividade é os alunos perceberem que $\sqrt{2}$ não pertence ao conjunto dos números racionais. Já a segunda atividade aborda a criptografia RSA.

Palavras-chave. Números primos. Criptografia. Educação básica

1 Introdução

Constantemente os professores são cobrados para que os conteúdos ministrados sejam contextualizados e despertem o interesse em seus alunos. A Matemática apresenta uma vantagem pois, praticamente tudo que vamos fazer em nosso dia a dia, seja explicita ou implicitamente, envolve cálculos, raciocínio lógico, equações, proporções ou conceitos da geometria.

Até mesmo mandar uma mensagem, algo que parece não ter absolutamente nada a ver com a Matemática, pode conter cálculos e propriedades matemáticas. Certamente ao enviar uma mensagem ou uma informação, você se deparou com a seguinte mensagem: "As mensagens e as chamadas são protegidas com criptografia de ponta a ponta". E é sobre essa segurança que iremos abordar neste trabalho.

Estudaremos sobre a CRIPTOGRAFIA, ciência de transformar, através de um processo conhecido como chave, uma informação de sua forma original em outra ilegível aos que não têm acesso à essa chave. E a Matemática tem papel crucial nessa transformação. A palavra criptografia vem do grego e significa escrita secreta e segundo [1], criptografia: "É a arte dos 'códigos secretos', que todos já praticamos quando criança".

Os números primos também têm um grande destaque neste trabalho. Ao ensinarmos os números primos na educação básica, passamos ao aluno a falsa ideia de que esses números servem apenas para fazermos o mínimo múltiplo comum e o máximo divisor comum. Mas ao estudarmos um

[1] adrianafreitas@ufla.br
[2] vivian_silveira2008@hotmail.com

pouco mais sobre esses incríveis números, percebemos quão grandiosas são sua aplicação e suas particularidades. Unir o ensino dos números primos com a aplicação na criptografia se torna extremamente interessante e o aluno passa a enxergar a utilidade de seu aprendizado e este passa a ter sentido. Este trabalho é baseado na dissertação [3].

2 Metodologia

O metodologia usada neste trabalho foi pesquisa em livros, artigos e na internet sobre resultados que abordavam os assuntos e que pudessem auxiliar em uma melhor compreensão do tema.

3 Resultados e Discussão

Neste trabalho estudamos os números primos, algumas definições e teoremas sobre sua importância e como todos os números naturais podem se originar deles. Apresentamos também algumas funções que geram os primos, embasados em estudos de matemáticos que se dedicaram para encontrar e formular tais funções.

Abordamos como é a distribuição dos números primos, se a distância entre eles é infinita ou se há algum intervalo no qual sempre irá existir um número primo contido nele. Apresentamos alguns primos que são conhecidos como primos especiais, primos que possuem alguma característica específica. E para saber se um determinado número grande é primo, estudamos os testes de primalidade. Todo esse conhecimento serviu de base para o estudo sobre criptografias.

Analisamos os algoritmos de codificação e decodificação das criptografias RSA e ElGamal, exemplos práticos e suas respectivas autenticidades.

Para aplicar tudo o que foi estudado sugerimos duas atividades para serem desenvolvidas pelos professores com os alunos dos anos finais do Ensino Fundamental ou Ensino Médio. Atividades que incentivam os alunos a praticarem a Matemática de forma prazerosa e descontraída, mas sem deixar de lado suas propriedades.

Atividade 1: Na primeira atividade, instigamos os alunos a perceberem que o número $\sqrt{2}$ tem um comportamento diferente dos números que eles estão acostumados: os naturais, inteiros e racionais. O objetivo é trabalhar com os alunos o conceito de número irracional. Sugerimos o uso da calculadora no desenvolvimento da atividade, isso estimula o interesse dos alunos e não atrapalha o objetivo da atividade. Inicialmente, questionamos aos alunos entre quais raízes conhecidas $\sqrt{2}$ está. Como $\sqrt{2}$ é um número pequeno espera-se que rapidamente eles respondam entre $\sqrt{1}$ e $\sqrt{4}$. Incentive-os a concluir que $\sqrt{2}$ deve ser um número entre 1 e 2. No próximo passo, peça aos alunos que acrescentem uma casa decimal ao número 1 e verifiquem se, ao elevarem o novo número ao quadrado, ele será igual a 2. Neste momento, indague-os sobre qual deve ser o primeiro número decimal. O número 2 está mais perto de 1 do que 4, assim $\sqrt{2}$ deve estar mais próxima de $\sqrt{1}$ do que de $\sqrt{4}$, ou seja, mais perto de 1 do que de 2. Isso fará com que eles escolham os números 1, 2, 3, 4 ou, no máximo, 5 para serem a primeira casa decimal. Seguindo a ideia apresentada no passo anterior pedimos aos alunos para construírem números com 4 casas decimais de modo que um dos números obtidos seja menor do que $\sqrt{2}$ e o outro maior. Após várias etapas, notamos que os números, ao serem elevados ao quadrado, se aproximam cada vez mais do número dois, mas nunca são exatamente ele. Para que não haja dúvidas, peça para que os alunos façam $1,4142135623$ ao quadrado e verifiquem que, mesmo com dez casas decimais, não encontramos $\sqrt{2}$. Apesar de não ser uma demonstração esse processo ilustra o fato de $\sqrt{2}$ ser irracional. Após essa construção de raciocínio, o professor deverá apresentar a demonstração formal para seus alunos.

Esta atividade também pode ser feita em um laboratório de informática utilizando o Excel. Esse software auxilia nos cálculos e, diferentemente da calculadora, consegue fazer potências com mais

casas decimais, facilitando a compreensão de que $\sqrt{2}$ possui infinitas casas decimais não periódicas.

Atividade 2: A segunda atividade, chamada Caça ao Tesouro, envolve a criptografia RSA. A ideia desta atividade é fazer um mapa do tesouro criptografando os números que nele aparecem. Aqui todos os grupos irão criptografar e descriptografar mensagens. A separação da quantidade de grupos e alunos fica a critério do professor. Sugerimos que essa atividade seja realizada em quatro aulas: as duas primeiras para explicar o conteúdo, a terceira para criptografar uma mensagem e a quarta para descriptografar essa mensagem. Suponhamos que haja 4 grupos. Cada um desses grupos irá criptografar uma mensagem para o grupo "seguinte" e descriptografar a mensagem do grupo "anterior". Por isso, já em um primeiro momento deve ficar bem clara a ordem dos grupos para que não haja erro na troca de informações. O grupo campeão será aquele que gastar menor tempo para criptografar e descriptografar a mensagem. Basta somarmos o tempo gasto nas duas últimas aulas. Cabe ao professor, com criatividade, escolher qual será o "tesouro" que os alunos encontrarão.

4 Considerações Finais

Ao longo deste trabalho observamos que os números primos são importantes não só para a Matemática, mas também para o nosso dia a dia. Com o aumento significativo do uso da tecnologia e da troca de informações pelos meios digitais fez-se necessária a criação de métodos para transmitir essas informações de forma segura. E a criptografia ajudou a tornar isso possível.

Os números primos sempre foram alvo de muitos estudos, o que nos forneceu avanços consideráveis em relação às suas propriedades e particularidades. Isso auxiliou muito no desenvolvimento da criptografia. Com a criptografia conseguimos exemplificar a aplicação de vários conteúdos do Ensino Fundamental e Médio, tais como: divisão euclidiana, máximo divisor comum, potenciação, radiciação, propriedades transitiva, reflexiva, simétrica entre outras. A vantagem de ilustrar essas aplicações é que ressaltamos para os alunos a importância da Matemática em seu cotidiano.

Estudamos duas criptografias que se destacam atualmente: RSA e ElGamal. Ambas baseadas na troca de chaves assimétricas. Estudos atuais mostraram que a Criptografia ElGamal é menos arriscada que a RSA, que apresentou falta de segurança em duas de cada mil chaves coletadas (veja [2]).

A criptografia foi se desenvolvendo ao longo da história e percebemos que houve muitas mudanças na forma de executá-la. O que começou apenas com uma troca na ordem das letras do alfabeto se tornou algo sofisticado e com a presença de propriedades e conceitos matemáticos mais refinados. O conhecimento não é algo estático, está sempre em movimento, e a criptografia está acompanhando esse movimento. Hoje, utilizamos os números primos na criptografia de informações e a segurança dos sistemas de criptografia baseia-se em problemas matemáticos que são difíceis de resolver nos computadores atuais. Por outro lado, vemos também um grande avanço computacional, o que poderá acarretar em uma mudança na segurança desses métodos.

Pesquisas vêm sendo desenvolvidas na busca de métodos alternativos que possam substituir os que existem hoje. Estudos nos mostram que o próximo passo será a Criptografia Quântica, que se baseia nos princípios da mecânica quântica, não mais em números primos.

Referências

[1] S. C. COUTINHO. **Números Inteiros e Criptografia RSA**. 2a. ed. Rio de Janeiro: IMPA, 2009.

[2] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung e Christophe Wachter. “Ron was wrong, Whit is right”. Em: **Cryptology ePrint Archive** (2012). URL: `https://eprint.iacr.org/2012/064`.

[3] V. S. Miranda. “Explorando os números primos e uma das suas aplicações atuais: a criptografia”. Dissertação de mestrado. UFLA, 2020.