ISSN: 2358-8829

ANÁLISE DAS DISSERTAÇÕES PRODUZIDAS NO ÂMBITO DO MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL (PROFMAT)*

Joaquim Denilson de Souza Silva [1]
Luiz Antônio da Silva Medeiros [2]
José Lucas Galdino da Silva [3]

RESUMO

Este trabalho apresenta uma análise das dissertações produzidas no âmbito do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), nos polos paraibanos, que abordam a temática da criptografia. A pesquisa tem como objetivo identificar tendências, abordagens metodológicas e contribuições dessas produções para o ensino de Matemática na Educação Básica, além de apontar lacunas — isto é, áreas da criptografia ainda pouco exploradas, mas com potencial para contribuir com o desenvolvimento do ensino da Matemática. A metodologia adotada foi o método misto concomitante, onde o pesquisador mistura dados quantitativos e qualitativos para realizar uma análise abrangente do problema da pesquisa. Realizou-se uma análise documental de dissertações disponíveis no repositório do PROFMAT que apresentam a criptografia em seus temas, considerando toda a série histórica. O referencial teórico se apoia em autores como D'Ambrósio, que enfatiza a necessidade de uma prática pedagógica que una teoria e vivência, respeitando o contexto cultural dos educandos, e Borba e Penteado, que tratam da utilização de tecnologias e abordagens interdisciplinares no processo educativo. A análise revelou que a maioria das dissertações utiliza a criptografia como ferramenta de materialização matemática, sobretudo nas áreas de Aritmética, Álgebra e Teoria dos Números, com ênfase na aplicação por RSA (Rivest-Shamir-Adleman). Os trabalhos evidenciam o potencial da criptografia como ferramenta didática para promover a interdisciplinaridade e despertar o interesse dos alunos pela Matemática. Também se observou uma variedade de abordagens, com destaque para o uso de ferramentas digitais e a valorização de aspectos históricos da criptografia. Conclui-se que uma quantidade considerável dos trabalhos possui um único viés: a aplicação das teorias estudadas ao longo do curso, como Teorema de Fermat, Função ϕ de Euler e o Teorema Chinês do Resto, o que abre campo para discussão e investigação sobre novas possibilidades de aplicação da criptografia no ensino de Matemática.

Palavras-chave: Criptografia, Ensino de Matemática, PROFMAT, Dissertações.

[1]Mestre pelo PROFMAT – Universidade Federal de Campina Grande (UFCG). E-mail: denilsonjoaquim@gmail.com;
[2] Doutor em Matemática Aplicada pela Universidade Estadual de Campinas (UNICAMP) – São Paulo, Brasil, 2008. E-mail: medeiros@mat.ufcg.edu.br.;
[3] Doutor em Matemática pela Universidade Federal de Campina Grande / Universidade Federal da Paraíba (UFCG/UFPB) – Paraíba, Brasil, 2024. E-mail: lucas.galdino@mat.ufcg.edu.br;

*Artigo resultante de projeto de pesquisa financiado pela Fundação de Apoio à Pesquisa do Estado da Paraíba (FAPESQ-PB).

ISSN: 2358-8829

INTRODUÇÃO

Este trabalho é um recorte de minha dissertação de mestrado, Silva (2025), intitulada Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico. Nossas pesquisas incluíam verificar os trabalhos realizados no programa do PROFMAT na Paraíba. Observar esse tema com mais foco nos permite vislumbrar o que tem sido produzido para o ensino básico público, visto que é da natureza do PROFMAT formar, quase que exclusivamente, professores desse segmento.

Existem diversos sistemas criptográficos que têm origem em diferentes áreas da Matemática — desde propriedades geométricas, como na cítale espartano, até fundamentos da aritmética modular, como no RSA. As dissertações paraibanas concentram-se principalmente no RSA, enquanto a nossa dissertação aborda um sistema criptográfico baseado em matrizes, além de explorar sistemas criptográficos clássicos, como o próprio cítale espartano.

As matrizes desempenham um papel fundamental no Ensino Básico, especialmente na segunda série do Ensino Médio. Segundo a Secretaria de Estado da Educação da Paraíba (2023), os objetivos de aprendizagem da unidade temática Álgebra incluem: (i) “identificar e representar os diferentes tipos de matrizes”; e (ii) “resolver problemas utilizando as operações com matrizes e a linguagem matricial”. No contexto do segundo objetivo, ao abordar operações com matrizes, muitos estudantes demonstram dificuldades em compreender o produto usual de matrizes.

No mesmo sentido, segundo Base Nacional Comum Curricular (2018), sua quinta competência geral envolve as seguintes capacidades:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (Base Nacional Comum Curricular, 2018, p. 19)

Assim, é de suma importância que o aluno não se limite a atuar apenas como usuário de sistemas criptográficos, mas que também compreenda suas bases e conceitos, desenvolvendo a capacidade de modificá-los e aprimorá-los.

ISSN: 2358-8829

Objetivo geral

Este trabalho tem como objetivo principal analisar as produções acadêmicas sobre criptografia desenvolvidas no âmbito dos cursos do PROFMAT na Paraíba, identificando suas características, abordagens metodológicas e lacunas temáticas, além de apresentar uma proposta própria de aplicação didática da criptografia baseada no Produto de Hadamard, elaborada no contexto do mestrado profissional em Matemática (PROFMAT/UFCG).

Objetivos específicos

Para alcançar esse propósito, o trabalho busca:

- Mapear as dissertações e produções acadêmicas do PROFMAT da Paraíba que abordam a temática da criptografia;
- Analisar as principais tendências, enfoques teóricos e metodológicos adotados nessas produções;
- Identificar possíveis lacunas, limitações ou oportunidades de aprofundamento relacionadas à aplicação da criptografia no ensino de Matemática;
- Descrever a proposta didática desenvolvida pelo autor, fundamentada no Produto de Hadamard e em princípios de aprendizagem significativa;
- Evidenciar o potencial dessa proposta para o ensino de Matemática, destacando sua contribuição para o contexto educacional do PROFMAT e para a aproximação entre teoria e prática docente.

Assim, este artigo busca analisar as produções sobre criptografia desenvolvidas no âmbito do PROFMAT na Paraíba, identificando suas principais características, e apresentar uma proposta didática elaborada pelo autor, fundamentada no Produto de Hadamard, que se diferencia das demais por aproximar a criptografia de aplicações matemáticas contemporâneas.

ISSN: 2358-8829

METODOLOGIA

O método de pesquisa escolhido para realizar a análise bibliográfica foi o misto concomitante que, segundo Creswell (2010), são aqueles em que:

> [...] o pesquisador converge ou mistura dados quantitativos e qualitativos para realizar uma análise abrangente do problema da pesquisa. Nesse modelo, o investigador coleta as duas formas de dados ao mesmo tempo e depois integra as informações na interpretação dos resultados gerais. Além disso, nesse modelo, o pesquisador pode incorporar uma forma menor de dados com outra coleta de dados maior para analisar diferentes tipos de questões (o qualitativo é responsável pelo processo enquanto o quantitativo é responsável pelos resultados). (CRESWELL, 2010, p. 39)

Logo, uma pesquisa bibliográfica mista é aquela em que o pesquisador analisa a quantidade de trabalhos em um determinado escopo enquanto, de maneira concomitante, verifica a qualidade do que é trabalhado. Nossa pesquisa se enquadra nesse método, pois, ao mesmo tempo em que fazemos a verificação do quantitativo de trabalhos com o tema desejado, analisamos também a forma como esses trabalhos abordam os temas propostos, a fim de reconhecer os caminhos de pesquisa comumente adotados ao se estudar criptografia e verificar possíveis lacunas a serem preenchidas.

Quantificar os trabalhos existentes e analisar a profundidade com que os temas são abordados permite não apenas compreender suas abordagens, mas também identificar quantos são, quais os mais recorrentes, em que contextos aparecem, além de outras informações relevantes. Um método puramente qualitativo não forneceria essa dimensão estatística da bibliografia, o que enfraqueceria a base da análise.

Ao adotar uma abordagem mista, nossa pesquisa ganha maior robustez analítica, pois a combinação entre dados quantitativos e qualitativos possibilita uma compreensão mais ampla e profunda da produção acadêmica sobre criptografia. O mapeamento quantitativo indica onde há maior ou menor concentração de estudos, enquanto a análise qualitativa revela como os temas são tratados. Isso nos permite direcionar com mais precisão nossas investigações, visando preencher lacunas deixadas pelos trabalhos já realizados.

Nossa investigação teve início com a análise de trabalhos realizados no programa do PROFMAT. Em Sociedade Brasileira de Matemática (2017), encontramos o catálogo

ISSN: 2358-8829

de disciplinas do programa, no qual consta a disciplina MA14 – Aritmética. Essa disciplina aborda os conteúdos introdutórios necessários ao estudo do sistema de criptografia RSA, além de introduzir diretamente esse sistema. Essa é provavelmente a influência que levou a produção de diversos trabalhos de criptografia com base em Aritmética e aplicação em RSA dentro do programa do PROFMAT, constatado em nossa pesquisa.

Em 11 de novembro de 2024, realizamos uma busca pelo termo “criptografia” no repositório do PROFMAT e identificamos 121 trabalhos que o mencionam no título. Desses, 28 citam explicitamente a sigla RSA, representando aproximadamente 23\% do total.

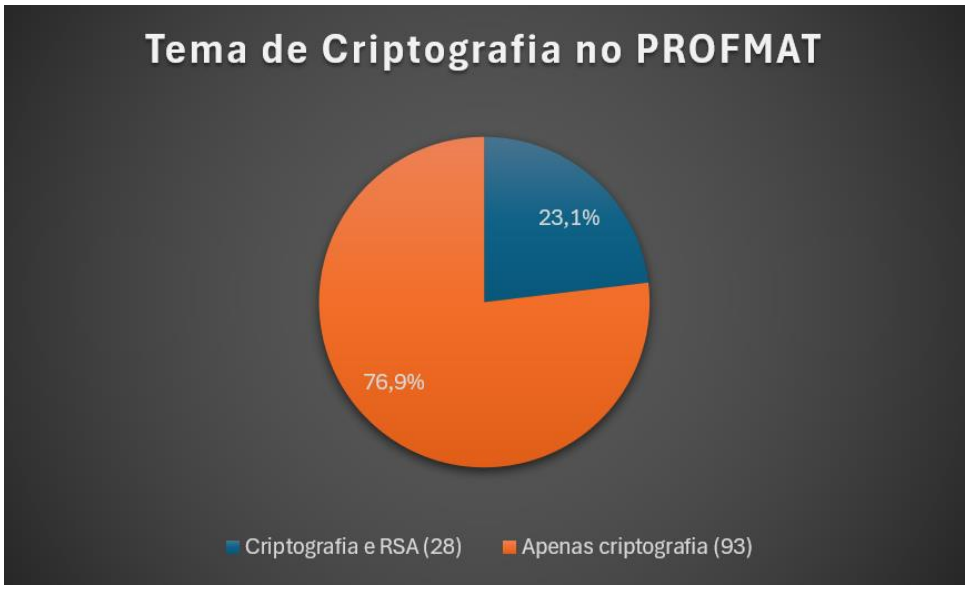

Figura 1 – Trabalhos do Repositório do PROFMAT com o termo criptografia no título.
Fonte: Autoria própria.

A Paraíba possui três polos do Profmat: um em João Pessoa, na Universidade Federal da Paraíba (UFPB), e outros dois em Campina Grande, sendo um na Universidade Federal de Campina Grande (UFCG) e o outro na Universidade Estadual da Paraíba (UEPB). No campo “Sigla da instituição” digitamos “PB” e em “Título da dissertação” digitamos “criptografia”, resultando nos trabalhos da UFPB e da UEPB. Conforme se verifica na Figura 2, foram encontrados 6 trabalhos com a palavra “criptografia” no tema, restritos à Paraíba: 4 deles na UFPB e 2 na UEPB. Para a UFCG, cuja sigla não possui as letras “PB”, realizamos uma pesquisa isolada, que não retornou nenhum resultado.

ISSN: 2358-8829

Data de defesa	Aluno	Título da Dissertação	Instituição	Dissertação
27/02/2023	WÉLISSON MARTINS MOTA	TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA	UFPB	PDF
26/08/2016	JOSEMBERG DOS SANTOS SILVA	ALGUNS MÉTODOS DE CRIPTOGRAFIA	UEPB	PDF
26/09/2014	UELDER ALVES GALDINO	TEORIA DOS NÚMEROS E CRIPTOGRAFIA COM APLICAÇÕES BÁSICAS	UEPB	PDF
13/08/2013	ROBERVAL DA COSTA LIMA	CRIPTOGRAFIA RSA E A TEORIA DOS NÚMEROS	UFPB	PDF
13/08/2013	GLAUBER DANTAS MORAIS	A MATEMÁTICA VIA ALGORITMO DE CRIPTOGRAFIA ELGAMAL	UFPB	PDF
15/04/2013	THIAGO VALENTIM MARQUES	CRIPTOGRAFIA: ABORDAGEM HISTÓRICA, PROTOCOLO DIFFIE-HELLMAN E APLICAÇÕES EM SALA DE AULA	UFPB	PDF

Figura 2 – Dissertações do PROFMAT abordando criptografia nas universidades paraibanas.
Fonte: Print de tela feito pelo autor a partir de pesquisa realizada no Sociedade Brasileira de Matemática (SBM) (2024), em 11 nov. 2024.

Na Paraíba, 2 dos 6 trabalhos contêm a sigla RSA no título. Entretanto, o mesmo padrão se repete com a abordagem do tema dentro dos trabalhos. Observamos que Silva (2016), no capítulo 4, aborda diversos tipos de criptografia, sendo um deles o RSA. O mesmo ocorre com Galdino (2014), mas agora no capítulo 6, sendo o RSA uma palavra-chave do trabalho. Já Morais (2013) e Marques (2013) abordam o tema de forma bem mais discreta, com Marques (2013) citando o RSA como exemplo de criptografia assimétrica.

Nota-se que os trabalhos realizados são mais antigos. Além disso, os 3 trabalhos de 2013 realizados na UFPB possuem o mesmo orientador, aparentando ser partes de uma pesquisa maior. Com isso, percebemos que o tema em nosso estado não foi tão explorado. Entretanto, como em trabalhos de universidades de outros estados pesquisados, o RSA é extremamente presente.

A pesquisa revela uma forte tendência em desenvolver o conteúdo da disciplina Aritmética Modular. Ao tomar conhecimento dessa abordagem recorrente, percebemos que nosso trabalho poderia ser mais produtivo ao explorar aspectos diferentes da criptografia.

REFERENCIAL TEÓRICO

A criptografia está presente no dia a dia do cidadão comum como nunca antes na história da humanidade. Ao ouvirem o termo, muitas pessoas associam-no imediatamente à segurança digital — reflexo da ampla utilização da criptografia nos sistemas de comunicação modernos, como o WhatsApp. Suas aplicações vão além, sendo utilizadas

ISSN: 2358-8829

também em sistemas financeiros, como cartões de crédito, e até na estrutura de moedas digitais, como o Bitcoin.

Ao longo da história, diferentes métodos de proteção da informação foram sendo desenvolvidos, desde técnicas rudimentares até algoritmos modernos. A evolução dessas práticas acompanha a necessidade humana de guardar segredos — seja para fins pessoais, políticos, militares ou econômicos. Entender a ciência por trás desses métodos, tanto os clássicos quanto os modernos, é uma forma de iniciação do aluno como criador de novos processos de segurança. A educação se torna útil à sociedade quando permite que seus educandos modifiquem o mundo ao seu redor.

Conforme apresentado brevemente na introdução, os trabalhos realizados no âmbito do PROFMAT na Paraíba que abordam o tema da criptografia concentram-se, em sua maioria, no estudo e aplicação do algoritmo RSA. Esse método, desenvolvido por Rivest, Shamir e Adleman em 1977, é um dos sistemas criptográficos de chave pública mais utilizados no mundo. O RSA baseia-se em conceitos de aritmética modular e na dificuldade de fatorar números primos muito grandes, garantindo segurança nas trocas de mensagens em meios digitais. No contexto educacional, ele costuma ser explorado como exemplo de aplicação prática da teoria dos números e da multiplicação modular, permitindo ao estudante perceber a utilidade de conteúdos matemáticos abstratos em sistemas reais de segurança da informação.

Entretanto, observa-se que, apesar de sua relevância, o RSA não é o único caminho possível para o ensino da criptografia, e sua aplicação não é tão simples de ser implementada no Ensino Básico, devido à complexidade envolvida na teoria do sistema.

Pensando nessa direção, menciona-se o trabalho intitulado “Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico”, desenvolvido no âmbito do PROFMAT da Universidade Federal de Campina Grande. O referido estudo propõe o uso do Produto de Hadamard — uma operação entre matrizes de mesma ordem em que a multiplicação é feita elemento a elemento — como mecanismo de criptografia de imagens. Nesse processo, cada elemento de uma determinada matriz quadrada é associado a um pixel, de modo que a codificação da matriz resulta diretamente na codificação da imagem correspondente.

O processo de codificação envolve o uso do Produto de Hadamard — uma operação entre matrizes mais simples que o próprio produto matricial usual ensinado no Ensino Médio —, dos quadrados latinos, já conhecidos por muitos alunos por meio do jogo Sudoku, e de um breve algoritmo de associação entre as matrizes da imagem, do

ISSN: 2358-8829

quadrado latino e de uma matriz-chave criada pelo próprio aluno. Essa atividade cria intimidade com matrizes, confere significado às operações e, se associada à computação — presente em algumas escolas —, possibilita a criação de programas capazes de criptografar múltiplas imagens. A proposta demonstra uma forma alternativa e visual de compreender a criptografia, aproximando os alunos da linguagem digital contemporânea e explorando, simultaneamente, conceitos de álgebra matricial, proporcionalidade e transformação de dados.

Essa atividade é aplicável a partir do Ensino Médio, onde o conceito de matriz é introduzido. Entretanto, o trabalho também apresenta, por meio de sistemas de criptografia clássica, métodos ainda mais simples que podem ser trabalhados no Ensino Fundamental. É o caso da atividade com o Cítale Espartano, na qual os alunos produzem um suvenir cilíndrico usado para codificar e decodificar mensagens escritas em tiras de papel, além de servir como embalagem para guardar e presentear.

RESULTADOS E DISCUSSÃO

A pesquisa identificou 121 trabalhos com o termo “criptografia” no título no repositório do PROFMAT, sendo 28 deles explicitamente relacionados ao algoritmo RSA, representando aproximadamente 23% do total. A análise quantitativa permite perceber a concentração e a distribuição desses trabalhos nos polos da Paraíba, conforme ilustrado nas Figuras 1 e 2, indicando maior produção nas universidades UFPB e UEPB, e uma lacuna relativa na UFCG, apesar de ser um dos polos do programa.

A análise qualitativa evidencia que a maioria dos trabalhos aborda a criptografia a partir do RSA ou de métodos clássicos de aritmética modular, utilizando abordagens teóricas e aplicações práticas direcionadas à disciplina de Matemática, com foco em ensino superior e formação de professores.

Observa-se, portanto, que há espaço para sistemas criptográficos além do RSA, talvez até com maior potencial de aplicação para o Ensino Básico. Nesse contexto, entra a proposta desenvolvida em minha dissertação “Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico”. Esta metodologia utiliza Produto de Hadamard, quadrados latinos e algoritmos de associação matricial como recurso didático, permitindo aos alunos explorar a criptografia de forma prática e significativa, aproximando conceitos matemáticos de aplicações digitais contemporâneas.

ISSN: 2358-8829

A comparação entre os trabalhos existentes e a proposta apresentada evidencia algumas contribuições inovadoras:

Abordagem visual e prática: enquanto a maioria dos trabalhos utiliza sistemas matemáticos abstratos, a proposta com Hadamard e imagens permite que o aluno veja o resultado da codificação de forma concreta.

Integração de conhecimentos: o método relaciona álgebra matricial, raciocínio lógico e tecnologias digitais, favorecendo a aprendizagem significativa e multidisciplinar.

Potencial de aplicação pedagógica: a simplicidade do método possibilita sua implementação no Ensino Médio, e adaptações com o Cítale Espartano permitem introdução em etapas iniciais do Ensino Fundamental, ampliando o alcance da aprendizagem da criptografia.

CONSIDERAÇÕES FINAIS

Diante dos processos expostos neste capítulo, concluímos que o nosso trabalho poderá gerar um impacto relevante na área em que se propõe atuar, por abordar um tema praticamente inexistente na literatura nacional e que, mesmo em âmbito internacional, tem sido explorado de forma restrita, principalmente em contextos muito específicos da pós-graduação.

Acreditamos que o Produto de Hadamard, por ser um produto simples e de intuição natural para alunos do Ensino Médio, possa ser um conteúdo aderente ao aprendizado e uma porta de entrada para a introdução de sistemas mais avançados (como processos de encriptação digital), motivando e até direcionando a carreira desses estudantes.

Desse modo, defendemos sua utilização como recurso pedagógico no ensino de conceitos ligados à criptografia e à segurança da informação — temas que despertam o interesse dos jovens e dialogam com a realidade digital em que estão inseridos. Essa abordagem pode não apenas facilitar o acesso a conteúdos matemáticos mais abstratos, como também ampliar o horizonte dos estudantes em relação às aplicações da Matemática em áreas tecnológicas e científicas.

Portanto, ao propor essa articulação entre Matemática Elementar, Álgebra Matricial e temas de relevância tecnológica, o trabalho busca contribuir tanto para a inovação didática quanto para o fortalecimento da formação matemática na Educação Básica.

ISSN: 2358-8829

REFERÊNCIAS

BASE NACIONAL COMUM CURRICULAR. *Base Nacional Comum Curricular*. Brasília: Ministério da Educação, 2018. Disponível em: https://basenacionalcomum.mec.gov.br/. Acesso em: 14 fev. 2025.

CRESWELL, John W. *Projeto de pesquisa: métodos qualitativo, quantitativo e misto*. Porto Alegre: Artmed, 2010. Disponível em: https://www.unirio.br/cultura/ppgcp/processo-seletivo/mestrado-edital-n-01-2023/bibliografia/creswell-john-w-projeto-de-pesquisa-metodos-qualitativo-quantitativo-e-misto-porto-alegre-armed-2010-capitulo-8/view. Acesso em: 26 fev. 2025.

GALDINO, Uelder Alves. *Teoria dos números e criptografia com aplicações básicas*. Juazeiro do Norte: Universidade Federal do Cariri, 2014. Monografia (Graduação em Matemática). Disponível em: <link se houver>. Acesso em: 8 set. 2025.

MARQUES, Thiago Valentim. *Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula*. Juiz de Fora: Universidade Federal de Juiz de Fora, 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional).

MORAIS, Glauber Dantas. *A matemática via algoritmo de criptografia El Gamal*. João Pessoa: Universidade Federal da Paraíba, 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional).

SECRETARIA DE ESTADO DA EDUCAÇÃO DA PARAÍBA. *Proposta Curricular do Ensino Médio da Paraíba (PCEM-PB)*. João Pessoa, 2023. Disponível em: https://paraiba.pb.gov.br/arquivos/pdfs/PropostaCurriculardoEnsinoMdiodaParabaPCEMPB23.pdf. Acesso em: 14 fev. 2025.

SILVA, Josemberg dos Santos. *Alguns métodos de criptografia*. Campina Grande: Universidade Estadual da Paraíba, 2016. Dissertação (Mestrado em Matemática). Disponível em: https://tede.bc.uepb.edu.br/jspui/handle/tede/2619. Acesso em: 14 fev. 2025.

SILVA, Joaquim Denilson de Souza. *Produto de Hadamard, criptografia e suas aplicações didático-conceituais no ensino básico*. Campina Grande: Universidade Federal de Campina Grande, 2025. Dissertação (Mestrado Profissional em Matemática – PROFMAT). Disponível em: https://dspace.sti.ufcg.edu.br/handle/riufcg/43590. Acesso em: 29 out. 2025.

SOCIEDADE BRASILEIRA DE MATEMÁTICA. *Catálogo de disciplinas – PROFMAT*. São Paulo: SBM, 2017. Disponível em: https://sbm.org.br/profmat/wp-content/uploads/sites/4/sites/4/2021/10/Catalogo-de-Disciplinas_2017.pdf. Acesso em: 3 jul. 2025.

ISSN: 2358-8829

SOCIEDADE BRASILEIRA DE MATEMÁTICA (SBM). *Dissertações do PROFMAT – Mestrado Profissional em Matemática em Rede Nacional*. 2024. Disponível em: https://profmat-sbm.org.br/dissertacoes/. Acesso em: 13 nov. 2024.