revista PARANAENSE DE EDUCAÇÃO MATEMÁTICA

ANÁLISE EPISTEMOLÓGICA DE TEORIA DOS NÚMEROS E CRIPTOGRAFIA: IMPORTÂNCIA DESSAS ÁREAS NOS CURRÍCULOS DE LICENCIATURA EM MATEMÁTICA

DOI: https://doi.org/10.33871/22385800.2021.10.21.22-43

Saddo Ag Almouloud[1]
Teodora Pinheiro Figueroa[2]
Rubens Vilhena Fonseca[3]

Resumo: Esta pesquisa de cunho teórico-qualitativo apresenta os resultados de uma análise epistemológica de Teoria dos Números e Criptografia e evidencia a importância dos saberes/conhecimentos dessas áreas nos currículos dos cursos de Licenciatura em Matemática e nos currículos da Escola Básica. A pesquisa surgiu a partir de inquietações referentes à própria prática docente e, também, de relatos da comunidade científica incentivando um maior número de pesquisas na área de Educação Matemática em Teoria dos Números e a associação deste saber às aplicações em Criptografia. Diante deste fato, procuramos responder à seguinte questão de pesquisa: Por que Criptografia é um contexto significativo em Teoria dos Números para os currículos do curso de Licenciatura em Matemática? Para responder nossa questão de pesquisa, valemo-nos de alguns constructos da Teoria Antropológica do Didático e da dimensão epistemológica de um problema didático. Os resultados das pesquisas realizadas mostram que as respostas a essa questão são de fundamental importância tanto para o pesquisador em Didática da Matemática, como para o professor de Matemática.
Palavras-chave: Análise epistemológica. Teoria dos números. Criptografia. Licenciatura em Matemática.

EPISTEMOLOGICAL ANALYSIS OF NUMBER THEORY AND CRYPTOGRAPHY: THE IMPORTANCE OF THESE AREAS IN THE CURRICULUM OF MATHEMATICS

Abstract: This nature theoretical and qualitative research presents the results of an epistemological analysis of Number Theory and Cryptography and highlights the importance of knows / knowledge of these areas in the curricula of undergraduate courses in Mathematics and Elementary School. The research emerged from referring concerns about teaching practice also from the scientific community reports, which encourages a greater research quantity on Math education area within Number Theory and its knowledge's association with cryptography applications. In view of this fact, we try to answer the following research question: Why is Cryptography a significant context in Number Theory for the curricula of the Degree in Mathematics? To answer our research question, we used some constructs of the Anthropological Theory of Didactic and the epistemological dimension of a didactic problem. The results of the research carried out show that the answers to this question are of fundamental importance for the researcher in Didactics of Mathematics, as for the professor of Mathematics.
Keywords: Epistemological analysis. Number theory; Cryptography. Degree in Mathematics.

[1] Doutorado em Matemática e Aplicações, Universidade Federal do Pará (UFPA), E-mail: saddoag@gmail.com – ORCID: https://orcid.org/0000-0002-8391-7054
[2] Doutorado em Engenharia Mecânica, Universidade Tecnológica Federal do Paraná, Campus Pato Branco, (UTFPR), E-mail: teodora.pinheiro@gmail.com – ORCID: https://orcid.org/0000-0001-8680-5202
[3] Doutorado em Educação Matemática, Universidade do estado do Pará (UEPA), E-mail: rubens.vilhena@uepa.br – ORCID: https://orcid.org/0000-0001-8899-2945

Introdução

A Criptografia fascina pessoas de todas as gerações e, passou a ser um elemento decisivo do cotidiano das pessoas que possuem e/ou têm acesso a serviços como e-mail, aplicativos de bancos e outros serviços online e necessitam de senhas ou outros códigos para acessar esses ou outros serviços digitais. Mas, do ponto de vista do ensino e aprendizagem de Matemática, ela tem sido apresentada apenas como exemplo de aplicação em algum tópico em Teoria dos Números.

Litoldo e Lazari (2014) relataram, em sua pesquisa, que o tema Criptografia foi encontrado em apenas duas das cinco coleções de Livros Didáticos selecionados, para análise, pelo Programa Nacional do Livro Didático (BRASIL, 2012) para o ensino médio e, mesmo assim, apenas uma apresentando aplicação da teoria abordada em seções sob títulos de *Saiba Mais* e *Contexto*.

A discussão sobre a natureza científica da Criptografia em Teoria dos Números nos cursos de Licenciatura em Matemática é de fundamental importância, pois muitos princípios da Criptografia moderna são suficientemente descritos por conteúdos matemáticos do Ensino Fundamental ou Médio, tais como Números Primos, Divisibilidade, Fatoração, Potenciação, Funções Afins etc. Todavia, a falta de conhecimento destes princípios pode levar em níveis mais básicos, a uma citação com breve moderação, com o intuito de apenas "ilustrar" uma aplicação em Matemática. Em nossa opinião, na pior das hipóteses, pode conceder à Matemática o caráter de mera ferramenta utilitária, levando os alunos a insights matemáticos pontuais, e à subestimada ideia de que "a Criptografia apenas contém Matemática" para ser ilustrada como uma aplicação sem muita reflexão ou aprofundamentos.

Diante deste cenário, este trabalho se refere a um recorte de uma pesquisa em andamento e, apresenta um estudo do ponto de vista epistemológico de Teoria dos Números e Criptografia, a fim de provocar uma discussão e reflexão sobre quais contribuições a Criptografia em Teoria dos Números pode oferecer à pesquisa em Educação Matemática, especificamente à pesquisa sobre a formação de professores de Matemática, tanto a respeito do saber científico quanto do saber aplicado. E, assim consequentemente reflexões e/ou discussões na perspectiva do professor de Matemática tanto a nível de Ensino Superior como na sua prática.

Os métodos criptográficos modernos, em particular, são baseados na Teoria dos Números, os quais se encontram inseridos em publicações relacionadas tanto às pesquisas de Coutinho (2000) em Matemática quanto às pesquisas de Pomerance (1990) em ciência da

computação. Mas a conexão da Criptografia com a Teoria dos Números em sala de aula é uma prática de ensino encontrada, predominantemente, nos cursos de computação, devido à natureza do próprio curso, como, por exemplo, o ensino e a aprendizagem de diretrizes e códigos de segurança em Sistema de Informação (NBRISO/IEC27002, 2013), cuja programação computacional é um elemento predominante nestes tipos de Sistemas e em toda a grade curricular do curso.

Enquanto isso, no ensino de Matemática ocorre a fragmentação e não contextualização dos conteúdos, apesar dos Parâmetros Curriculares Nacionais enfatizarem a importância da conexão do ensino de Matemática a um contexto significativo.

> De fato, não basta revermos a forma ou metodologia de ensino, se mantivermos o conhecimento matemático restrito à informação, com as definições e os exemplos, assim como a exercitação, ou seja, exercícios de aplicação ou fixação. Pois, se os conceitos são apresentados de forma fragmentada, mesmo que de forma completa e aprofundada, nada garante que o aluno estabeleça alguma significação para as ideias isoladas e desconectadas umas das outras. Acredita-se que o aluno sozinho seja capaz de construir as múltiplas relações entre os conceitos e formas de raciocínio envolvidas nos diversos conteúdos; no entanto, o fracasso escolar e as dificuldades dos alunos frente à Matemática mostram claramente que isso não é verdade (BRASIL, 2000, p. 43).

No texto da Base Nacional Comum Curricular (BNCC) sobre a Matemática no Ensino Fundamental – Anos finais - é relatado que:

> Cumpre também considerar que, para a aprendizagem de certo conceito ou procedimento, é fundamental haver um contexto significativo para os alunos, não necessariamente do cotidiano, mas também de outras áreas do conhecimento e da própria história da Matemática (BRASIL, 2018, p. 299).

O levantamento feito pelos autores deste artigo, das 52 universidades federais, nas quais os currículos dos cursos de licenciatura adotam a disciplina Teoria dos Números ou equivalente, cinco delas trazem o assunto Criptografia em suas ementas. São elas, Universidade Federal de Alagoas (UFAL), Universidade Federal da Bahia (UFBA), Universidade Federal de Itajubá (UNIFEI), Universidade Federal de Juiz de Fora (UFJF) e Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM).

Diante deste fato surge a seguinte questão: Por que a Criptografia é um contexto significativo em Teoria dos Números para os currículos do curso de Licenciatura em Matemática?

Para tentar responder a esta questão, primeiramente, surgiu a necessidade de fazer uma pesquisa e análise epistemológica da Teoria do Números e da Criptografia, a fim de

evidenciar a natureza científica da Criptografia em Teoria dos Números e, consequentemente, discutir a importância deste saber nos currículos de Matemática. Além disso, procuramos apresentar alguns aspectos da Criptografia nos cursos de Licenciatura em Matemática e outros aspectos em termos das aplicações em Teoria dos Números.

Com relação à dimensão epistemológica, Farras, Bosch e Gascón (2013) afirmam que ela permite a análise da amplitude do âmbito matemático para situar, nosso problema didático, os tipos de problemas oriundos da problemática e as tentativas de abordar e, até mesmo, solucionar tal problemática. Ela auxilia na procura de respostas à questão: Quais as razões de ser desse objeto matemático e da problemática do seu ensino?

Para Almouloud (2007, p. 156), a análise epistemológica tem por base o desenvolvimento histórico, permitindo identificar as diferentes formas de concepções de um determinado objeto matemático que poderão favorecer a análise didática.

Nesta perspectiva, Godino (2003, *apud* MATOS, 2017) comunga com essa ideia, quando assevera que, no estudo dos fatores que afetam os processos de ensino e aprendizagem da matemática, devem ser considerados a natureza dos conteúdos, o papel da atividade humana, bem como o desenvolvimento sociocultural de ideias matemáticas. Portanto, a análise epistemológica de objetos matemáticos deve ajudar a esclarecer a natureza desses objetos.

Para a construção deste trabalho, valemo-nos, também, de alguns constructos da Teoria Antropológica do Didático (TAD), a qual estuda as condições e restrições do funcionamento dos Sistemas Didáticos, entendidos como relações sujeito-instituição-saber, ou seja, estuda o homem frente ao saber matemático e, mais especificamente, frente a situações matemáticas. Uma razão para a utilização do termo "antropológico" é que a TAD situa a atividade Matemática e, em consequência, o estudo da Matemática dentro do conjunto de atividades humanas e de instituições sociais (CHEVALLARD, 1999, p. 1).

Segundo Almouloud (2018), na TAD, as noções de (tipos de) tarefa, (tipo de) técnica, tecnologia e teoria permitem modelar as práticas sociais em geral e, em particular, a atividade Matemática, baseando-se em três postulados: Toda prática institucional pode ser analisada, sob diferentes pontos de vista e de diferentes maneiras, em um sistema de tarefas relativamente bem delineadas. O cumprimento de toda tarefa decorre do desenvolvimento de uma técnica. A palavra técnica é aqui utilizada como uma "maneira de fazer" uma tarefa, mas não é, necessariamente, como um procedimento estruturado e metódico ou algorítmico. A relação institucional que se estabelece entre uma instituição I (aluno, professor, ...) e um objeto depende das posições que tais elementos ocupam nessa instituição e do conjunto de

tarefas que essas pessoas devem cumprir usando determinadas técnicas.

Um conjunto de técnicas, de tecnologias e de teorias organizadas para um tipo de tarefa forma uma organização "praxeológica" (ou praxeologia) (Matemática ou Didática). A palavra praxeologia é formada por dois termos gregos, *práxis* e *logos*, que significam, respectivamente, prática e razão. praxeologia reporta-se, portanto, ao fato de que uma prática humana, em uma instituição, está sempre acompanhada de um discurso, mais ou menos desenvolvido, de um logos que a justifica, acompanha e lhe dá razão.

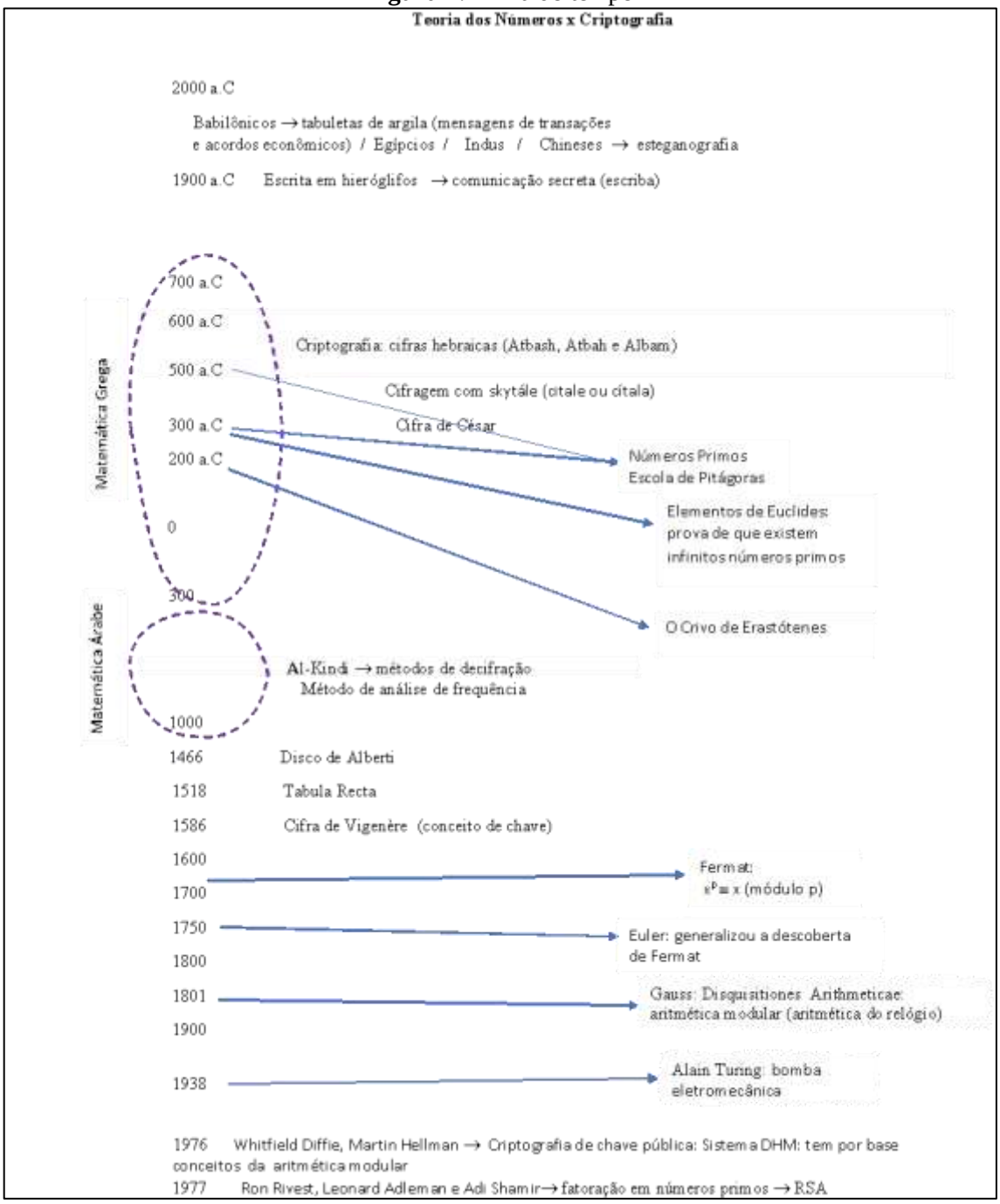
Uma grande parte das praxeologias matemáticas (PM) que são habitualmente estudadas no Ensino Básico e na universidade perdeu a sua razão de ser na instituição escolar, ou seja, desapareceram dessa instituição escolar as questões às quais ditas PM poderiam responder e, consequentemente, o seu estudo na citada instituição deixou de fazer sentido. Para evidenciar as possíveis razões de ser da Organização Matemática (OM), é exequível responder a certas questões, como por exemplo: Que razões históricas motivaram a construção de uma determinada PM? A que situações problemáticas a PM pode responder? Que situações novas podem ser construídas? Que problemas a PM vem resolver que as PM estudadas anteriormente não permitiam? Ou seja, quais são as vantagens em estudar a referida PM?

Os aspectos referentes à análise epistemológica serão abordados nas próximas seções, a partir da Linha do tempo: Teoria dos Números e Criptografia.

Linha do tempo: Teoria dos Números e Criptografia

A Figura 1 apresenta a linha do tempo sobre a evolução da Teoria dos Números e Criptografia, a qual procura mostrar que os desenvolvimentos de ambas as áreas são completamente interligados pela necessidade de o homem recorrer a um tipo de comunicação secreta e indispensável à sua época e que, atualmente, de certa forma, dependemos do desenvolvimento deste tipo de comunicação "secreta" na maioria de nossas transações diárias, principalmente, com o uso da internet.

Figura 1: Linha do tempo



Fonte: Os autores

Ao olharmos do ponto de vista histórico, o que hoje denotamos como Criptografia, é o resultado de uma ininterrupta descoberta em Teoria dos Números. A análise da figura 1 nos permite fazer os seguintes apontamentos.

As primeiras civilizações, cada uma com a sua forma de mensagem (hieróglifos, esteganografia, cifras hebraicas), usaram diversos tipos de registros para que seus integrantes se comunicassem uns com os outros e, posteriormente, em suas transações e acordos econômicos, os quais, segundo Bauer (2013, p. 3), podem ser denominados de

protocriptografia, ou seja, um tipo arcaico de criptografia. Independentemente do que possa ser considerado, estes tipos de registros comprovam a necessidade do homem se comunicar de forma secreta.

No livro "History of Cryptography and Cryptanalysis" de Dooley (2018), encontramos uma descrição em detalhes sobre a evolução da Criptografia desde os primeiros métodos usados para esconder mensagens, como a Cifragem com Cítala, a Cifra de César, o Método de Análise Frequência, o Disco de Alberti, a Tabula Recta até sistemas de cifragens mais sofisticados à época, como a Cifra de Vigenère, a qual também utiliza a Tabula Reta, mas, agrega conceito de chave, usada para cifrar e/ou decifrar mensagens. Até então, quem quisesse enviar uma mensagem secreta se depararia com um problema essencial: antes que o comunicado fosse transmitido, o emissor e o receptor teriam de se encontrar para decidir, por exemplo, qual cifra ou, método de codificação seria estabelecido entre eles.

Enquanto isso, diferentes povos, nações também desvendava interessantes padrões numéricos em Matemática, como por exemplo, na Grécia, os membros da escola Pitagórica discutiam e faziam descobertas sobre os números inteiros (na época, números naturais) e suas relações. Segundo Singh (2008, p.34), o filósofo e matemático grego Pitágoras (570 – 495 a.C.) era fascinado pelos ricos padrões e as propriedades dos números perfeitos[4] e outras sutilezas numéricas. Assim como os mesopotâmios, árabes, maias, chineses, indianos, entre outros (IFRAH, 1997).

Quando Os Elementos de Euclides apareceram (cerca de 300 a.C.) muitos dos resultados importantes sobre números primos tinham sido provados. No livro IX dos Elementos, segundo Boyer e Merzbach (2012, p. 96), existem vários teoremas interessantes e, desses, o mais célebre é a Proposição 20: "números primos são mais do que qualquer quantidade fixada de números primos". Isto é, Euclides dá a demonstração elementar bem conhecida do fato de que há infinitos números primos.

Há 200 a.C., o Grego Eratóstenes apresentou um método sistemático, para isolar os números primos, denominado Crivo de Eratóstenes (BOYER; MERZBACH, 2012, p.122).

Segundo Du Sautoy (2007, p. 48), durante gerações, tentou-se, sem sucesso, aperfeiçoar o entendimento de Euclides sobre os primos. Os matemáticos tentaram, com diferentes graus de êxito, encontrar fórmulas que, mesmo sem gerar todos os números primos, produzissem ao menos uma lista de primos.

[4] Um número se diz perfeito se é igual à soma de seus divisores próprios. Divisores próprios de um número positivo N são todos os divisores inteiros positivos de N exceto o próprio N. Por exemplo, o número 6, seus divisores próprios são 1, 2 e 3, cuja soma é igual à 6: 1 + 2 + 3 = 6.

Expresso na notação de Gauss para a aritmética modular, segundo Du Sautoy (2007, p. 249), Fermat, no século XVII, enunciou sem demonstrar que, dados a e p inteiros positivos, sendo p um número primo que não divide a, têm-se $a^{p-1} \equiv 1 (\text{mod } p)$. Essa notação nos diz que o número *a* elevado a uma potência *p-1* é congruente a 1 módulo *p*, significando que qualquer inteiro positivo elevado a uma potência igual a um número primo menos 1, quando dividido por esse número primo, sempre vai deixar como resto 1. Este resultado é conhecido como Pequeno Teorema de Fermat. Em 1758, Euler publicou uma demonstração e empregou essencialmente o ponto de vista da moderna Teoria dos Grupos. Com base em sua prova, Euler publicou uma generalização do resultado de Fermat em 1760 (OLIVEIRA, 2019).

Segundo Du Sautoy (2007, p. 119), a aritmética modular foi desenvolvida por Gauss no livro Disquisitiones Arithmeticae, publicado em 1801.

Do ponto de vista da Criptografia, no decorrer do tempo, foi necessário criar máquinas para decodificar mensagens enviadas diariamente pela inteligência alemã durante a Segunda Guerra Mundial. Mas, mesmo antes da Segunda Guerra Mundial, Alain Turing começou a se inspirar em criação de seus "Bombes", as máquinas para decifrar códigos, em tempos em que estudava Matemática em Cambridge, quando Hardy e Hilbert ainda estavam em ascensão. Turing já planejava máquinas que derrubariam dois dos 23 problemas de Hilbert. Toda esta especulação sobre máquinas era puramente teórica, ninguém ainda visualizava um objeto físico real, tratava-se de máquinas da mente: métodos ou algoritmos que gerassem respostas. Eram conjecturas apenas do ponto de vista da Matemática pura, mas que foram responsáveis pelo desenvolvimento do pensamento computacional, antes mesmo da concepção da ideia do computador.

Turing engendrou a ideia de máquinas especiais que pudessem ser criadas para se comportar efetivamente como qualquer pessoa ou máquina que realizasse cômputos aritméticos. Posteriormente foram chamadas de máquinas de Turing. (DU SAUTOY, 2007, p. 198).

Em 1939, com a Segunda Guerra Mundial, as forças intelectuais britânicas foram reunidas em Bletchley Park, e as mentes passaram da busca por zeros à decifração de códigos. O sucesso de Turing na criação de máquinas para decifrar o Enigma (máquina eletromecânica de criptografia usada pelos alemães) se deve, em parte, à prática com o cálculo de zeros da função zeta de Riemann. Sua complexa rede de rodas dentadas interconectadas não conseguiu descobrir os segredos dos primos, mas os novos dispositivos de Turing foram eficazes em revelar os movimentos secretos da máquina de guerra alemã.

A partir da década de 1970, com o advento da internet, tornou-se necessário um

sistema de Criptografia para a era emergente de rápida comunicação global. Segundo Du Sautoy (2007, p. 242), assim como ocorreu em Bletchley Park, na decifração do Enigma durante a guerra, os matemáticos seriam outra vez os responsáveis pelo invento de uma nova geração de códigos que tirariam a Criptografia dos romances de espionagens e a levariam para a aldeia global. Esses códigos matemáticos foram a base para a criação do que é chamado de Criptografia de Chave Pública. Este sistema de Criptografia de Chave Pública é como uma porta com duas chaves diferentes: a chave A tranca a porta, mas uma chave B, a destranca. Não se mantém qualquer confidencialidade em relação à chave A. Sua segurança, numa explicação bem elementar, se baseia no complexo e extremamente difícil problema de fatorar um número que é produto de dois números primos gigantes.

A Criptografia de Chave Pública foi proposta em 1976 por dois matemáticos da Universidade de Stanford, na Califórnia, Whitfield Diffie e Martin Hellman (DIFFIE; HELLMAN, 1976).

Ron Rivest, do Instituto de Tecnologia do Massachusetts (MIT), se aliou a Adi Shamir, um matemático israelense que visitava o MIT, e começaram a buscar ideias para implementar um tipo de criptografia que ia contra todos os paradigmas antes estabelecidos. Enquanto exploravam fundamentos matemáticos para seus sistemas criptográficos embrionários, começaram a pesquisar conteúdos da Teoria dos Números, em particular a aritmética modular e Números Primos, o que também despertou o interesse de Leonard Adleman, um matemático, informático e biólogo molecular estadunidense.

A descoberta de Fermat de importantes resultados envolvendo números primos e posteriormente os trabalhos de Euler, provando esses resultados e generalizando e a aritmética modular de Gauss, foram os temas que inspiraram Rivest. Ele usou a generalização do pequeno teorema de Fermat, construído por Euler, que funciona em calculadoras-relógio construídas a partir de dois primos, em vez de um. Euler demonstrou que, nessas calculadoras, o padrão se repete após embaralharmos as cartas $(p -1) \cdot (q -1) + 1$ vezes. Assim, só é possível descobrir quanto tempo é necessário para que o padrão se repita no relógio com $N = p \cdot q$ horas, conhecendo-se os primos p e q. Saber, por meio da fatoração, quais são esses dois primos, torna-se, portanto, a chave para descobrir os segredos da Criptografia RSA.

Embora os dois números p e q sejam confidenciais, seu produto $N = p \cdot q$ pode ser divulgado. Assim, a segurança do código RSA de Rivest depende da dificuldade da tarefa de fatorar o número N. (DU SAUTOY, 2007, p. 252).

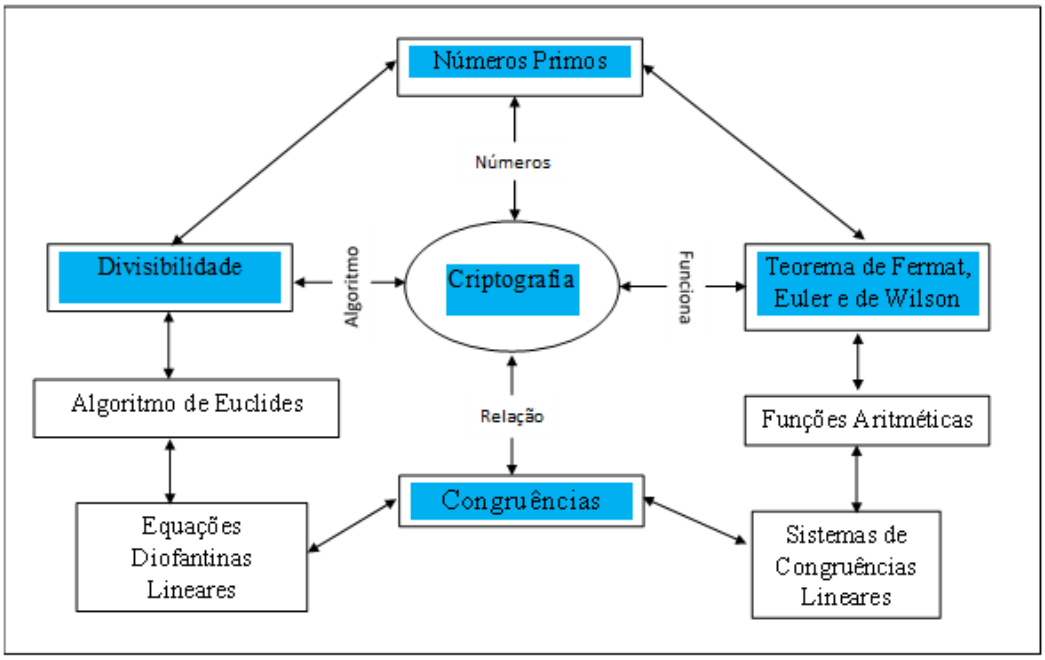
Os novos problemas que resultaram dessas incursões criptográficas levaram ao

desenvolvimento de uma Matemática profunda e difícil. (DU SAUTOY, 2007, p. 254).

Com base nesta linha do tempo, comentada e apresentada na figura 1, procuramos explicitar na figura 2 um Modelo Epistemológico de Referência (MER), pois segundo Barquero, Bosch e Gascón (2013), na formulação de um problema didático o didata deve utilizar mesmo que implicitamente uma descrição e interpretação (ou seja, um modelo epistemológico) do âmbito matemático que está em jogo. O MER é um modelo que deve ser explicitado e utilizado como referência para analisar os atos didáticos-matemáticos.

Na figura 2, deixamos em evidência, em azul, elementos da Matemática cujo desenvolvimento foi essencial no advento da Criptografia e, os quais podem ser explorados pelos professores no ensino fundamental e médio com as devidas transposições didáticas com ênfase em Criptografia, evidenciando também o contexto puramente matemático.

Figura 2: Modelo Epistemológico de Referência (MER)



Fonte: os autores

A base Matemática de muitos criptossistemas fundamenta em muitos tópicos da Teoria dos Números contidos na figura 2 e, a partir das conexões entre tópicos indicados pelas setas de duplo sentido, também podemos destacar a importância que cada tópico retroalimenta o entendimento de conteúdos matemáticos e de alguns conceitos chave, como ilustramos a seguir:

- Congruência: (i) justificativa para alguns testes de divisibilidade conhecidos de anos anteriores na escola básica; (ii) generalização de técnicas de provas; (iii) perspectiva / consolidação: como um novo entendimento do conjunto dos números inteiros de

funções unidirecionais.

- Algoritmo euclidiano: (i) comparação da eficácia na determinação do Máximo Divisor Comum (MDC), quando comparado aos fatores primos; (ii) perspectivas / consolidação: cálculo de inversos multiplicativos.
- Teorema de Euler: (i) perspectiva / consolidação: conceito de ordem e raiz primitiva.
- conceito-chave de número: o conhecimento dos números naturais é aprofundado. A ocasião para isso são questões de construção de chave para o algoritmo RSA e sua segurança. Estes levam aos primos, sua distribuição, testes de primalidade e o problema da fatoração. Além disso, testes familiares de divisibilidade são comprovados com a ajuda da congruência e, portanto, são legitimados retrospectivamente. Em particular, isso apresenta uma oportunidade para destacar problemas elementares de Matemática não resolvidos ou discutidos.
- conceito-chave de algoritmo: a questão da geração de chaves leva ao algoritmo euclidiano que os alunos podem descobrir por si mesmos. Este e outros algoritmos ilustram as vantagens da resolução algorítmica de problemas; perguntas sobre a eficiência dos algoritmos surgirão quase por si mesmas. A importância do uso do computador para a aplicação desses e de outros algoritmos pode ser conectada à história da criptografia. Isso contrasta com o uso normal de algoritmos no ensino médio, que geralmente se limita a resolver sistemas de equações ou, em geral, para o processamento de problemas de cálculo (gráfico de curvas).
- conceito-chave de relação funcional: o conceito de função unidirecional necessária na criptografia aumenta os tipos de funções inversíveis (mesmo que limite seu domínio) já conhecidas. Além disso, se o tópico for abordado em profundidade, os alunos possuirão a rara oportunidade de trabalhar com funções em domínios discretos.

Outros conceitos chaves surgem da necessidade de números primos adequadamente grandes para a construção de chaves no RSA, como A comparação das probabilísticas nos testes de primalidade, números pseudoprimos e as relações com a segurança do algoritmo RSA.

Sendo assim, mais estudos devem ser feitos, pesquisas com relação a formação docente em conexão com o que aqui é apresentado, poderão ser capazes de assegurar a importância que, nos cursos de Licenciatura em Matemática, esses elementos sejam estudados de forma mais aprofundada com aspectos da própria evolução histórica conforme comentado e apresentado na figura 1. Pois do ponto de vista epistemológico, quando se fala em Teoria

dos Números, também se estabelecem conexões com a Criptografia, um assunto essencial na atualidade em função do avanço tecnológico e, como relatamos, extremamente necessário desde as primeiras civilizações, para a comunicação de forma secreta. Constatamos em nossa pesquisa que este tipo de comunicação no decorrer do tempo se apoiou em fundamentos matemáticos hoje estudados em sua grande maioria na Teoria dos Números para obter chaves cifradoras/decifradoras a fim de proteger os dados/informações. Logo, pode-se dizer que a razão de ser de Criptografia é a Teoria dos Números.

A seguir apresentaremos aspectos da Criptografia no curso de Licenciatura em Matemática.

Criptografia na Licenciatura em Matemática

Do ponto de vista dos estudantes de um curso de Licenciatura em Matemática, faz-se necessário um conhecimento do saber matemático, de tal forma que o professor de matemática seja capaz de fazer as adaptações necessárias para que ele se transforme no saber a ensinar. Essas adaptações que visam transpor o saber matemático para o saber a ser ensinado é denominado de transposição didática (CHEVALLARD, 1996).

O foco central desta pesquisa está associado à formação inicial de professores de Matemática, ou seja, o nosso público-alvo são os alunos do ensino superior de Licenciatura em Matemática. O objeto de pesquisa se refere à epistemologia de Teoria dos Números e Criptografia, evidenciando que os conceitos matemáticos na Teoria dos Números são a base fundamental da Matemática estudada na educação básica e superior, pois, refere-se ao estudo das propriedades dos números inteiros.

Diante da nossa questão de pesquisa “Por que Criptografia é um contexto significativo em Teoria dos Números para os currículos do curso de Licenciatura em Matemática?”, podemos evidenciar no relato sobre a Linha do Tempo, figura 1, que Teoria dos Números e Criptografia estão conectados e, que a razão de ser da Criptografia é a Teoria dos Números.

Ao procurar responder à questão de pesquisa, deparamo-nos com algumas inquietações apresentadas pela comunidade científica, as quais são:

- as poucas pesquisas sobre Teoria dos Números, na área de Educação Matemática, relatada nas pesquisas de Campbell, Zakzis (2006), que defendem a importância do ensino de Teoria dos Números em cursos de Licenciatura em Matemática, devido a uma variedade de perspectivas, ou seja: sua natureza formal, sua beleza e misticismo, sua prática e utilidade, sua importância na história da Matemática e,

principalmente, a sua importância do ponto de vista pedagógico. Eles defendem que Teoria dos Números é útil para o ensino e a aprendizagem da Matemática. Que os tópicos, em Teoria dos Números, fornecem caminhos naturais para o desenvolvimento e a solidificação do pensamento matemático, especialmente no que diz respeito à identificação e reconhecimento de padrões.

- a preocupação em ressignificar a disciplina de Teoria dos Números no sentido de estabelecer um diálogo entre o ensino superior (licenciatura em Matemática) e o ensino fundamental e médio (MANDLER, 2017, RESENDE, 2007, TABACH et al., 2011, PEREIRA, 2018).
- a importância da Criptografia, no ensino de Matemática, relatada nas pesquisas de Olgin (2011), Sant'anna (2013), Galdino (2014), Rodrigues (2016), Santos (2016), Lage (2018), Rosseto (2018), Rodrigues; Sa (2019). Lage (2018) comenta, por exemplo, que a aritmética modular tem aplicações presentes no cotidiano dos alunos da educação básica, porém muitas vezes ignorada por não saberem sua origem e/ou seu funcionamento.

Além disso, como comentado anteriormente, devido ao aumento do tráfego de dados eletrônicos, a criptografia é de relevância prática para todos que fazem uso – seja por meio de transações bancárias online, e-mails, cartões eletrônicos, passaportes eletrônicos ou proteção de dados pessoais. Nessas aplicações, a criptografia não apenas garante o sigilo dos dados trocados, mas também fornece meios confiáveis para a autenticação dos participantes da comunicação e para verificação da integridade dos dados. Portanto, entende-se que é imprescindível que os alunos adquiram conhecimentos básicos sobre o uso de aplicativos criptográficos.

Pode-se também comprovar este fato a partir de pesquisas na área de computação (LOTT e CIANCONI, 2018) cujos objetivos gerais para a aprendizagem a este respeito são:

- ➢ Sensibilizar para a segurança dos dados, especialmente, o conhecimento de que os dados trocados na Internet podem, em princípio, ser monitorados e, portanto, inseguros;
- ➢ Derivado disso, perceber a necessidade de encriptação e a capacidade de executar e verificar a encriptação;
- ➢ Garantir a capacidade do conhecimento de que a identidade dos participantes da comunicação pode ser verificada;

A seguir, apresentaremos alguns aspectos de Criptografia na área de Teoria dos Números a fim de mostrar esta conexão do ponto de vista da pesquisa científica nesta área.

Acredita-se que estas informações tendem a ampliar os horizontes dos futuros professores de Matemática.

Criptografia e a Teoria dos Números

Segundo o que podemos concluir de Lovász (2008), para os alunos visualizarem uma imagem autêntica da Matemática como ciência e, em particular, da importância da Teoria dos Números, é necessário mostrar os desenvolvimentos científicos atuais em Matemática. Nesse sentido, a Criptografia é um conteúdo muito interessante devido à sua importância em um mundo altamente conectado e, além disso, pode-se dizer que traz contribuições aos professores de Teoria dos Números, a coincidência de como muitas técnicas e alguns algoritmos modernos, em Criptografia, são totalmente explicados e não requerem sofisticados conhecimentos matemáticos (basicamente conceitos como congruências) para serem compreendidos.

A seguir, comentaremos sobre o exemplo do sistema criptográfico RSA e sobre alguns assuntos intimamente relacionados, os quais são usados para evidenciar a possibilidade de ampliar os conhecimentos de Matemática adquiridos no ensino médio.

O conteúdo da Matemática escolar não se estende além do conhecimento científico matemático conhecido até o século XVIII, com exceção da Teoria da Probabilidade e de algumas formalidades. Mesmo o conteúdo dos ramos clássicos da escola Matemática (aritmética, álgebra, cálculo e geometria) é encontrado sob os termos mais amplos já em 1905 e tem sido intensamente formado e trabalhado desde então (BURTON, 2016).

A oportunidade de fazer com que os alunos enfrentem problemas científicos não resolvidos, dificilmente existe dentro do escopo do currículo padrão. Esse fato tem um motivo muito prático: questões científicas abertas nos ramos supramencionados são difíceis de serem descritas em nível escolar fundamental e, portanto, dificilmente acessível ao aluno. Por outro lado, várias questões abertas na Teoria dos Números são compreensíveis, mas o currículo não oferece chances de um encontro natural com tais questões. Nesta perspectiva, Guy (2004, p. 1) diz que:

> A Teoria dos Números fascina tanto o amador quanto o profissional há mais tempo do que qualquer outro ramo da Matemática. Assim, existem mais problemas não resolvidos hoje e, embora muitos deles não sejam resolvidos por muitas décadas, isso provavelmente não impedirá as pessoas de tentarem. São tão numerosos que já preencheram mais de um volume.

O matemático húngaro Paul Erdös (1913-1996) era um ardente defensor da resolução de problemas e propostas. Inclusive, é de sua autoria inúmeras questões ainda abertas até hoje (CHUNG, 1998).

Shanks (1978) afirma que "Grande parte da teoria elementar dos números surgiu da investigação de três problemas; a de números perfeitos, a de decimais periódicos e a de números pitagóricos. Organizamos o livro em três capítulos longos" (SHANKS, 1978, p. xi).

O autor expande e tece em conjunto as ideias que surgem, nessas três áreas, para fornecer uma cobertura bastante abrangente da teoria dos números elementares. Cada problema leva a mais problemas, alguns resolvidos e outros ainda não resolvidos

A partir do que foi exposto acima, consideramos que comentar a respeito de questões ainda em aberto em cursos de licenciatura em Matemática pode ser um fator importante para despertar, no aluno, a curiosidade e, até mesmo, a iniciativa em tentar resolvê-los e, dessa forma também pode contribuir para o ensino e aprendizagem de Criptografia. Nossa consideração se apoia no interessante método utilizado por Marshal, Odell e Starbird (2007).

Em *Number Theory Through Inquiryn* (MARSHAL; ODELL; STARBIRD, 2007) destacam que a Teoria dos úmeros é o tópico perfeito para um curso de introdução às provas. Uma vez que o estudante universitário, muito provavelmente, conhece as propriedades básicas dos números, a exploração desses números familiares pode levar a um rico cenário de ideias. É possível pensar, de acordo com o que se depreende da leitura, em um modelo, projetar um curso, em específico de Teoria dos Números e ao assunto Criptografia em particular.

Assim, questões ainda não resolvidas na Teoria dos Números que poderiam despertar a curiosidades de licenciandos em Matemática, seriam, por exemplo:

(1) Existe um número infinito de primos ímpares gêmeos?

(2) Existe sempre um primo entre n^2 e $(n+1)^2$?

(3) Existe uma maneira eficiente de encontrar os fatores primos de grandes números?

As duas primeiras perguntas são fáceis de entender e são acessíveis por experimentação. Aparecem em conexão com a distribuição de números primos.

A terceira pergunta é particularmente interessante do ponto de vista criptográfico. Em Ciência da Computação, uma função unidirecional ou função de sentido único é uma função simples de calcular para qualquer entrada (qualquer valor do seu domínio), mas difícil de inverter, dada a imagem de uma entrada aleatória. Aqui "fácil" e "difícil" são entendidos em termos da teoria da complexidade computacional, especificamente, a teoria dos problemas de tempo polinomial, entretanto o fato de não ser injetiva, não é considerado suficiente para uma função ser chamada de "mão única". A existência de funções de sentido único, ainda é uma

conjetura em aberto.

O processo de codificação e decodificação no sistema RSA pode ser visto como uma função unidirecional, ou seja, uma função praticamente impossível de inverter, se algumas informações não forem fornecidas de antemão. Na prática, não há uma abordagem eficiente para o problema de quebrar mensagem criptografada, quando se utiliza chaves cujo valor é produto dois números primos muito grandes e distantes entre si. A questão do afastamento entre números primos é importante, mesmo que sejam gigantescos. Pois, se estiverem muito próximos, ou forem primos consecutivos, seus valores se aproximam da raiz quadrada do produto entre eles (vide método de fatoração de Fermat). A situação é equivalente ao conhecimento da decomposição em fatores primos (ROSEN, 2011). Este fato é usado como segurança na construção do sistema criptográfico RSA, como evidenciado adiante.

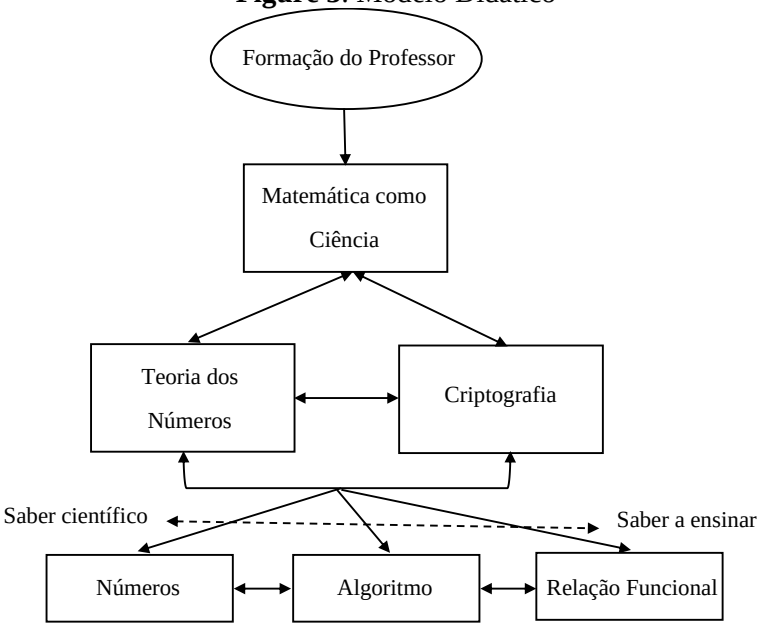
A dificuldade Matemática em resolver, neste caso, não representa falha, mas é essencial para a segurança da função que é usada no sistema criptográfico RSA. Isso dá aos alunos a oportunidade de aprofundar sua compreensão acerca de números inteiros, nas aulas de Teoria dos Números, no contexto da criptografia e permite que vejam a ciência Matemática como ainda incompleta. Além disso, a utilização da falta de conhecimento, apoia uma abordagem pouco usada na experiência escolar dos alunos.

Modelo Didático

A partir dos resultados desta pesquisa, construímos uma proposta de Modelo Didático (MD) (Figura 3) para os cursos de Licenciatura em Matemática, o qual apresenta a visão da Matemática como Ciência no topo da Formação do Professor, de modo a se consolidar esta visão nestes cursos, mostrando a importância da epistemologia do saber no processo de apropriação dos conceitos científicos das disciplinas de Matemática. Este Modelo Didático propõe que os professores formadores instiguem, nos alunos, a busca pelo conhecimento matemático na perspectiva de sua história, conexão com o mundo em que se vive e, dos desafios que ainda existem, mostrando assim que a Matemática é uma ciência viva em constante evolução.

No caso desta pesquisa, em específico, abordamos a disciplina de Teoria dos Números e, propusemos a associação desta disciplina com Criptografia para o desenvolvimento de conceitos da Teoria dos Números. O que requer uma visão da disciplina da Teoria dos Números como ciência pura e aplicada, presente em nosso cotidiano e, onde ainda prevalecem desafios matemáticos.

Figure 3: Modelo Didático



Fonte: Os autores

Neste Modelo Didático (Figura 3), também procuramos explicitar, por meio das setas de duplo sentido, que existem relações entre os conceitos chaves: Número, Algoritmo e Relação Funcional, as quais devem ser discutidas nos cursos de Licenciatura, na perspectiva de levar os alunos a fazerem associações do saber científico ao saber escolar, cujos conteúdos relacionados foram explicitados anteriormente.

Nosso MD nos leva a refletir sobre qual o papel que a apresentação dessa transferência pode ou deve ter na implementação do ensino. A profundidade desta apresentação também depende da extensão temporal da unidade de ensino e a ponderação das relações interdisciplinares, e visa, principalmente, propiciar uma compreensão dos princípios criptográficos.

Nosso MD, nos permite sugerir o estudo de alguns objetos de saber, tais como, os seguintes conteúdos que discutimos em nosso MER: O conceito-chave de *número*, congruência, algoritmo euclidiano, teorema de Euler e o conceito chave de *relação funcional*.

Estas discussões e associações auxiliarão o futuro professor em seu processo de transposição didática, de modo a proporcionar aos alunos, não apenas manipulação de algoritmos de resolução, mas de relações entre os conceitos. Esperamos que pudessem assim estabelecer conjecturas, para assumir uma postura interpretativa e crítica; de modo que o saber a ser ensinado seja de fato institucionalizado do ponto de vista da importância dos conceitos e da visão Matemática também como ciência, incitando a curiosidade, com o objetivo de desenvolver a habilidade de investigação.

Considerações finais

Diante do que aqui foi exposto, podemos sugerir e/ou inferir que a Criptografia é adequada para expor aos alunos de Teoria dos Números, perguntas não resolvidas em ciências matemáticas, em um contexto puramente matemático, como relatamos na seção sobre Criptografia e Teoria dos Números.

Ao mesmo tempo, na seção sobre a Linha do Tempo, procuramos mostrar que o conhecimento matemático não é uma ciência pronta e, sim em constante desenvolvimento, é uma ciência que gera, vividamente, novos conceitos e está envolvida em uma troca constante de ideias com aplicações práticas, como por exemplo, a Criptografia.

Sendo assim, esta pesquisa inicial traz reflexões sobre considerar a importância da Criptografia nos currículos dos cursos de Licenciatura em Matemática, pois ela amplia e aprofunda os conhecimentos e percepções preexistentes da Matemática. Isto diz respeito, em particular, aos principais conceitos-chave explicitados anteriormente, presentes no Modelo Didático (Figura 3).

Inferimos que os elementos desta pesquisa explicitaram considerações determinantes para a resposta da questão de pesquisa “Por que a Criptografia é um contexto significativo em Teoria dos Números para os currículos do curso de Licenciatura em Matemática?”, assim como para reflexões tanto do ponto de vista do pesquisador em didática da Matemática, quanto do professor de Matemática.

Do ponto de vista do pesquisador em Educação Matemática, a pesquisa sobre a epistemologia da Teoria dos Números e Criptografia evidencia possibilidades de investigação sobre vários objetos matemáticos e as conexões entre os tópicos indicados pelas setas de duplo sentido (Figura 2), principalmente, no sentido de que cada tópico retroalimenta o entendimento de conteúdos matemáticos e de alguns conceitos chave importantes no ensino fundamental e médio.

Do ponto de vista do professor, o contexto da Criptografia na disciplina de Teoria dos Números em um curso de Licenciatura em Matemática e a discussão dos tópicos envolvidos de forma aprofundada, considerando as relações com a Matemática escolar, contribuem para o processo de transposição didática do saber científico para o saber ensinar. Neste contexto, em particular, os futuros professores deveriam ter elementos a fim de poderem fazer associações para despertar a curiosidade dos alunos sobre as aplicações da Criptografia no contexto atual e mostrar a importância da Matemática em nosso dia a dia.

Referências

ALMOULOUD, S. **Fundamentos da Didática da Matemática**. Curitiba: Editora da UFPR, 2007.

ALMOULOUD, S. **A engenharia do percurso de estudos e pesquisa** (Conferência plenária), 2018. Disponível em: Almouloud2018A.pdf (uniandes.edu.co).

BARQUERO, B., BOSCH, M. e GASCÓN, J. Las tres dimensiones del problema didáctico de la modelización matemática. **Educação Matemática e Pesquisa**, São Paulo, v.15, n. 1, pp.1-28, 2013.

BAUER, C.P. **SecretHistory, The storyofcryptology**. Taylor and Francis Group, LLC, 2013.

BOYER, C.B; MERZBACH, U.C. **História da Matemática**. São Paulo: Blucher, 2012.

BRASIL. Ministério da Educação. Secretaria de Educação Básica. **Parâmetros Curriculares Nacionais**: ensino médio. Brasília, DF: MEC, 2000. Disponível em: http://portal.mec.gov.br/expansao-da-rede-federal/195-secretarias-112877938/seb-educacao-basica-2007048997/12598-publicacoes-sp-265002211. Acesso em: 15/04/2020.

BRASIL. **Base Nacional Comum Curricular** (BNCC). Brasília: MEC, 2018. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_20dez_site.pdf. Acesso: 15/04/2020.

BRASIL. **Programa Nacional do Livro Didático**, 2012. Disponível em: https://www.fnde.gov.br/index.php/programas/programas-do-livro/pnld/guia-do-livro-didatico/item/2988-guia-pnld-2012-ensino-m%C3%A9dio. Acesso em 21/042020.

BURTON, D. M. **Teoria elementar dos números**. LTC, Rio de Janeiro, 7 ed., 2016.

CAMPBELL, S.R.; ZAZKIS, R. **Number theory in mathematics education**: perspectives and prospects. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2006.

CHEVALLARD, Y. La transposition didactique et l'avenir de l'École. Fenêtre sur Cours, **Bulletin par le SNUipp**, 1996.

CHEVALLARD, Y. L´analyse des pratiques enseignantes en théorie anthropologique du didactique. **Recherches en Didactique des Mathématiques**. Grenoble: La Pensée Sauvage-Éditions, v. 19.2, p. 221-265, 1999

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Série de Computação e Matemática n. 2, IMPA e SBM, segunda edição (revisada e ampliada), 2000.

CHUNG, F.; GRAHAM, R. **Erdös on Graphs**: His Legacy of Unsolved Problems, A K Peters/CRC Press, 1998.

DIFFIE, W.; HELLMAN, M. **New Directions in Cryptography**. Trans. IEEE Inform. Theory, IT-22, 6, p. 644-654, 1976.

DOOLEY, J. F. **History of Cryptography and Cryptanalysis**: codes, ciphers, and their algorithms. Springer International Publishing AG, 2018.

DU SAUTOY, M. **A música dos números primos**. Rio de Janeiro: Zahar, 2007.

FARRAS, B. B.; BOSCH, M.; GASCÓN, J. Las tres dimensiones del problema didáctico de la modelización matemática. **Educação Matemática Pesquisa**, São Paulo, v. 15, n. 1, p. 1-28, 2013.

GODINO, J. D. **Teoría de las Funciones Semióticas**. Un enfoque ontológico semiótico de la cognición e instrucción matemática. Trabajo de investigación presentado para optar a la Cátedra de Universidad de Didáctica de la Matemática de La Universidad de Granada, 2003.

GALDINO, U. A. **Teoria dos números e criptografia com aplicações básicas**. (77 f.) Dissertação de Mestrado em Matemática. Programa de Pós-Graduação em Matemática em Rede Nacional. PROFMAT. CCT-UEPB, 2014.

GUY, R. K. **Unsolved Problems in Number Theory**, Springer-Verlag New York, 2004.

LAGE, F. D. A. S. M. **Um estudo de aritmética modular para a educação básica**. (61 f.) Dissertação de Mestrado em Matemática. Programa de Pós-Graduação em Matemática em Rede Nacional. PROFMAT. UFOP, 2018.

LITOLDO, B. F.; LAZARI, H. Uma análise do uso da criptografia nos livros didáticos de matemática do ensino médio. **REMATEC**, Natal (RN), ano 9, n. 17, p. 135 – 156, 2014.

LOTT, Y.M.; CIANCONI, R. B. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. **Perspectivas em ciência da informação**. vol.23, n°.4 Belo Horizonte, 2018.

LOVÁSZ, L. **Trends in Mathematics**: How they could Change Education?, 2008. Disponível em: https://web.cs.elte.hu/~lovasz/lisbon.pdf . Acesso em 18/09/2020.

MANDLER, M.L.; GOMES, M. A. O.; SANTOS, L. M. Prática Docente Compartilhada em Teoria de Números: uma articulação entre a formação na Licenciatura e a prática docente na escola. In: VIII EEPEM (Encontro de Ensino e Pesquisa em Educação Matemática) e VI EEMOP (Encontro de Educação Matemática de Ouro Preto), 2017, Ouro Preto. **Anais do VI EEMOP e VIII EEPEM**. Ouro Preto: Universidade Federal de Ouro Preto (UFOP), p. 579-591, 2017.

MARSHALL, D. C.; DELL, E.; STARBIRD, M. **Number Theory Through Inquiry**, 1st ed. Washington, DC: Mathematical Association of America, Inc., 2007.

MATOS, F. C. **Praxeologias e modelos praxeológicos institucionais**: o caso da álgebra linear. Tese em Educação em Ciências e Matemáticas, do Instituto de Educação Matemática e Científica da Universidade Federal do Pará, 2017.

NBR ISO/ IEC 27002. **Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação**, 2013. Disponível em : https://www.normas.com.br/produto/normas-brasileiras-e-

mercosul/pesquisar?expressao=seguran%C3%A7a+em+c%C3%B3digos+computacionais. Acesso em 21/04/2020.

OLGIN, C. A. **Currículo no ensino médio**: uma experiência com o tema criptografia.(136 f) Dissertação (Mestrado em Ensino de Ciências e Matemática) - Programa de Pós-Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil, Canoas, 2011.

OLIVEIRA, F. E. F. **Sobre Várias Demonstrações do Pequeno Teorema de Fermat e as Inter-relações entre as Áreas da Matemática**. Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.

PEREIRA, R. C.; PAIVA, M. A. V.; FREITAS, R. C. O. A transposição didática na perspectiva do saber e da formação do professor de matemática. **Educação Matemática Pesquisa**, São Paulo, v.20, n.1, p. 41-60, 2018.

POMERANCE, C. **Cryptology and Computational Number Theory**. Providence, R. I.: American Mathematical Society, 1990.

RESENDE, M. R. **Ressignificando a disciplina de Teoria dos Números na formação do professor de Matemática na Licenciatura.** (281 f.) Tese de Doutorado em Educação Matemática. Programa de Pós-Graduação em Educação Matemática. PUC-SP. São Paulo, 2007.

RODRIGUES, M. A. **Tópicos de criptografia para o ensino médio**. (95 f.). Dissertação de Mestrado em Ciências. Programa de Mestrado Profissional em Matemática. ICMC-USP, 2016.

RODRIGUES, L.P.O.; SA, L.C. Matrizes e criptografia: contribuições de uma atividade sobre o whatsapp no ensino médio. **REnCiMa**, v. 10, n.6, p. 255-273, 2019

ROSEN, K. H. **Elementary number theory and its applications**, 6th Edition. Addison Wesley, 2011.

ROSSETO, C. K. **Criptografia como recurso didático**: uma proposta metodológica aos professores de matemática (84 f). Dissertação (Mestrado Profissional) – Programa de Mestrado Profissional em Matemática em Rede Nacional, Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto, 2018.

SANT'ANNA, I. K. **Aritmética modular como ferramenta para as séries finais do ensino fundamental.** (36 f.). Dissertação de Mestrado em Matemática. Programa de Pós-Graduação em Matemática em Rede Nacional. PROFMAT. IMPA, 2013.

SANTOS, A.P.F. **A Criptografia no ensino fundamental II:** contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas outras curiosidades. (131f). Dissertação de Mestrado em Matemática. Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro. 2016.

SHANKS, D. **Solved and Unsolved Problems in Number Theory**. 2th ed. New York: AMS Chelsea, 1978

SINGH, S. **O último teorema de Fermat**. Tradução de Jorge Luiz Calife. 13ª. Edição. Editora Record, 2008.

TABACH, M.; LEVENSON,E.; BARKAI, R.; TSAMIR, P.; TIROSH, D.; DREYFUS, T. Secondary teachers' knowledge of elementary number theory proofs: the case of general-cover proofs. **J Math Teacher Educ,** 14, p.465–481, 2011.

Recebido em: 29 de agosto de 2020
Aprovado em: 18 de novembro de 2020