

10^o

FEPEG FÓRUM

ENSINO • PESQUISA
EXTENSÃO • GESTÃO
RESPONSABILIDADE SOCIAL: INDISSOCIABILIDADE
ENSINO, PESQUISA E EXTENSÃO UNIVERSITÁRIA



ISSN 1806-549 X

Autor(es): CLAUDEMILSON DA SILVA OLIVEIRA, STÊNIO VIDAL MENEZES

Uso das aplicações de congruência modular para o ensino de aritmética na educação básica

Palavras-Chave

Congruência modular; aritmética, ensino.

Introdução

A matemática tem fascinado curiosos e pesquisadores desde a antiguidade, seja para a solução de problemas do cotidiano, explicação de situações complexas, ou para demonstração de sua versatilidade. Em ambos os casos, os amantes dessa disciplina têm dedicado esforço para aprimorar os conhecimentos adquiridos e consolidar sua relevância para a humanidade. A matemática está presente em todos os campos do conhecimento e é necessária em qualquer atividade humana.

Entretanto, dada a sua complexidade, criou-se uma ideia de que o estudo da matemática seja apropriado apenas às pessoas dotadas de intelecto privilegiado, sendo de difícil compreensão e, portanto, não recomendada aos sujeitos comuns. Aliado a esse fator a aplicação de metodologias mais conservadoras têm promovido desestímulo aos estudantes, o que ajuda a reforçar o estigma imposto a essa ciência. Uma saída seria desenvolver metodologias mais atraentes que se baseiem nas aplicações da matemática no cotidiano [10].

É difícil encontrar aplicações para tudo na matemática, por isso, não se deve ter a preocupação de ensinar apenas o que possui aplicação conhecida. Entretanto, sempre que possível após ensinar determinado conteúdo para o qual existe uma aplicação, é bom que os alunos sejam estimulados a experimentar. Os experimentos têm o poder de fixar os conhecimentos e consolidar o saber.

Logo, fazer a opção por metodologias “diversificadas, apelativas e interativas” promove condições para acessar os indivíduos que não gostam ou apresentam alguma dificuldade para aprender matemática. A utilização de recursos inovadores representa a possibilidade de romper as barreiras da aprendizagem e possibilitar a desmistificação da matemática como uma ciência dura e destinada apenas a intelectuais [6].

O principal objetivo desse trabalho é estudar as principais aplicações da congruência modular em sistemas de identificação e codificação usados na atualidade. Especificamente, pretendeu-se: a) Apresentar aspectos históricos relacionados à aritmética modular; b) Expor os fundamentos da matemática relacionada à congruência modular utilizada na composição de códigos de barras, CPF e criptografia; c) Levantar experiências de ensino na educação básica baseadas em congruência modular; d) Propor metodologias de ensino de congruência modular no ensino básico.

Assim, o estudo justifica-se pela tentativa de elucidar a importância das aplicações de congruência modular para a sociedade e atrair a atenção para as aplicações da própria matemática no dia a dia. Sobretudo, o desenvolvimento de estudos nessa área pode suscitar, em momento oportuno, o interesse em aprimorar as metodologias de ensino da aritmética na educação básica e possibilite criar um ambiente favorável ao ensino da matemática.

Material e métodos

Os estudos foram iniciados em fevereiro de 2016, com a busca por monografias e artigos científicos nas bases Google Acadêmico, Anais da Associação Brasileira de Educação Matemática (SBEM) e Banco de dissertações do Mestrado Profissional de Matemática em Rede Nacional (PROFMAT), bem como livros de matemática que abordem aplicações de congruência modular. Os critérios utilizados na seleção tangem à explicitação do estudo de aplicações de congruência modular, estudo ou relato de experiência enfatizando o uso de congruência modular como metodologia de ensino para a educação básica.

Após a seleção da bibliografia, foram feitos levantamentos de aspectos históricos da construção da teoria dos números com ênfase no estudo de congruências, bem como fatores relevantes acerca das aplicações de congruência modular no desenvolvimento de sistemas de identificação e criptografia, com vistas a pensar em metodologias inovadoras para o ensino de aritmética na educação básica.

Em seguida, procedeu-se a proposição de oficinas para o ensino de matemática utilizando as aplicações de aritmética modular.

10^o

FEPEG FÓRUM

ENSINO · PESQUISA
EXTENSÃO · GESTÃO
RESPONSABILIDADE SOCIAL: INDISSOCIABILIDADE
ENSINO, PESQUISA E EXTENSÃO UNIVERSITÁRIA



ISSN 1806-549 X

Resultados e discussão

Foram analisadas dez publicações, sendo quatro dissertações de mestrado, todos com abordagem específica das aplicações de congruência modular em sistemas de identificação, criptografia e no ensino de divisibilidade na educação básica.

Identificou-se três estudiosos no campo da aritmética modular, que propuseram a utilização desse conteúdo como ferramenta para o ensino de divisibilidade e aplicações de matemática no cotidiano, reforçando a importância da matemática na produção de soluções para problemas relevantes do cotidiano [3, 6, 7].

A congruência modular tem sido utilizada para gerar um número de controle da veracidade de códigos. Esse número verificador possibilita constatar se um código de barras, um número padrão internacional de livro (ISBN), um número de passaporte, ou o número de Cadastro de Pessoa Física (CPF) estão corretos, já que todos os algarismos que compõem o número original são utilizados no método de geração do código verificador.

No caso da criptografia, a congruência modular é empregada na recodificação de mensagens e senhas, criando nova estrutura de códigos e impossibilitando que as pessoas, ou sistemas não detentores das chaves de decodificação façam uso do conteúdo em sua essência.

Foram propostas três oficinas de ensino de aritmética modular.

A primeira oficina propõe que os alunos apliquem a congruência modular na confirmação de validade de números de CPF, onde os mesmos terão a oportunidade de conhecerem a estrutura numérica do documento e certificarem-se do uso de aritmética na sua composição.

A segunda oficina sugere o ensino de aritmética através do uso de congruência modular para identificar a composição de códigos de barras impressos em embalagens de produtos diversos e, ainda, identificarem o país de origem do produto através da análise da estrutura numérica dos códigos.

A terceira oficina proposta pretende levar os alunos a aplicarem a congruência modular na criptografia de mensagens.

Conclusão/Conclusões/Considerações finais

A congruência modular foi amplamente discutida, ressaltando a sua aplicação tanto para a composição dos sistemas de identificação, quanto para a criptografia de códigos de segurança e em outras aplicações.

Procurou-se apresentar as principais aplicações de congruência modular abordadas no conjunto de referências bibliográficas selecionadas, enfatizando as que abrangem os sistemas de identificação, códigos de barras e criptografia.

Procurou-se apresentar propostas de trabalho com alunos do ensino fundamental e médio, onde os mesmos são convidados a experimentarem as aplicações da congruência modular nas situações destacadas, com o intuito de provocar a inovação do processo de ensino, promovendo melhores condições para a aprendizagem.

Isso chama a atenção para a necessidade de implementar metodologias de ensino que reforcem a aplicação da matemática no dia a dia. Demonstrar as aplicações da matemática é essencial para motivar os alunos a estabelecerem processos de investigação nesse campo, bem como de valorização dessa disciplina como conteúdo curricular.

Agradecimentos

À Universidade Federal de São João Del Rei (UFSJ), pela oportunidade de desenvolvimento deste estudo.

Referências bibliográficas

- [1] CARVALHO, A. L. de; RODRIGUES, D. V. M; ARAUJO, L. H. R. **Aplicações da aritmética modular na criptografia**. 2015. Disponível em: <<https://periodicos.set.edu.br/index.php/cadernoexatas/article/view/2157>> Acesso em: 04 março 2016.
- [2] CASTRO, Jânio Kléo de Souza. **Teoria dos números**: introdução à teoria dos números. Fortaleza: UAB/IFCE, 2010.
- [3] ESQUINCA, J. C. P. **Aritmética**: códigos de barras e outras aplicações de congruências. Dissertação de mestrado. Disponível em: <<http://repositorio.cbc.ufms.br:8080/jspui/handle/123456789/1746>>. Acesso em: 04 março 2016.
- [4] HEFEZ, Abramo. **Elementos de aritmética**. 2. ed. Rio de Janeiro: SBM. 2011.

10^o

FEPEG FÓRUM

ENSINO • PESQUISA
EXTENSÃO • GESTÃO

RESPONSABILIDADE SOCIAL: INDISSOCIABILIDADE
ENSINO, PESQUISA E EXTENSÃO UNIVERSITÁRIA



Realização:



Apoio:



ISSN 1806-549 X

- [5] LOPES, J. V.; ÁVILA, J. A. J. **Limitação de qualquer fator primo de um número perfeito ímpar**. Disponível em: <http://www.ufsj.edu.br/portal2-repositorio/File/profmat/TCC_09_Jaqueline.pdf> Acesso em: 11 março 2016.
- [6] LOURENÇO, P. J. P. **Aplicações da aritmética modular**. Dissertação de mestrado. Universidade de Coimbra. Julho de 2011. Disponível em: <<http://sistemaidentificacao.n.o.sapo.pt/ficheiros/Relatorioarit%20Modular.pdf>>. Acesso em: 04 março 2016.
- [7] OLIVEIRA, Maycon Costa de. **Aritmética**: criptografia e outras aplicações de congruências. Dissertação de mestrado. Disponível em: <<http://repositorio.cbc.ufms.br:8080/jspui/bitstream/123456789/2160/1/MAYKON%20COSTA%20DE%20OLIVEIRA.pdf>>. Acesso em: 11 março 2016.
- [8] PICADO, Jorge. **A álgebra dos sistemas de identificação**: da aritmética modular aos grupos diedrais. Disponível em: <<http://www.mat.uc.pt/~picado/SistIdent/isbn2.pdf>>. Acesso em 04/03/2016. Acesso em: 04 março 2016.
- [9] SÁ, Ilydio Pereira de. **Aritmética modular e algumas de suas aplicações**. Disponível em: <<http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf>>. Acesso em: 11 março 2016.
- [10] SANT'ANNA, I. K. de. **A aritmética modular como ferramenta para as séries finais do ensino fundamental**. Dissertação de mestrado. Disponível em: <http://wwwimpa.br/opencms/pt/ensino/downloads/PROFMAT/trabalho_conclusao_curso2013/iury_kersnowsky.pdf>. Acesso em: 11 março 2016.