RESOLUÇÃO DE PROBLEMAS UTILIZANDO A ARITMÉTICA MODULAR

Luciana Maria Dias de Ávila Rodrigues, Roberta Paula Brandão de Novais
Universidade de Brasília, Brasil
luavila@mat.unb.br, robertanovais7@gmail.com

Resumo

No trabalho que segue, mostraremos como utilizar uma ferramenta da teoria dos números, aritmética modular, como proposta didática a ser trabalhada tanto no ensino fundamental quanto no ensino médio como forma de motivação ao estudo de conteúdos, como: estudo das quatro operações aritméticas fundamentais, divisibilidade e o estudo de arcos côngruos aplicados no cotidiano da vida das pessoas. Os códigos numéricos de identificação, a criptografia, calendários e diversos fenômenos periódicos são assuntos que estão diretamente ligados ao tema, em que apresentaremos datas comemorativas, o cálculo dos dois últimos dígitos do CPF, e a leitura do código de barras brasileiro.

Introdução

Nos dias atuais, grande parte da metodologia de ensino de matemática se reduz a um modelo de aulas expositivas no qual o professor passa o conteúdo no quadro e o aluno tem um papel de mero expectador cujo seu maior esforço é, normalmente, na resolução de exercícios de fixação. Sendo este, na maioria das vezes um "copia e cola" resolvendo seguindo o passo a passo que o professor passou no quadro, sem ao menos se questionar o porquê de determinado raciocínio para tal resolução.

A metodologia de resolução de problemas (Saldanha) permite ao aluno ser um agente ativo de seu aprendizado e, mais do que isso, proporciona ao aluno aprender. Ou seja, antes de formalizar determinado conteúdo, trazer um problema e permitir que os alunos utilizem de seus conhecimentos prévios para tentar resolver tal desafio proposto pelo professor é um caminho que segundo Schroeder e Lester (1989), citado por Onuchic e Allevato(2015,p.4) "torna o ato de resolver problemas uma parte integrante da aprendizagem de Matemática, isto é, os alunos aprendem Matemática enquanto estão resolvendo problemas." (Onuchic & Allevato,2015, p.4)

Nesse sentido, apresentamos neste trabalho tanto ao professor quanto ao aluno mais uma forma de ensino-aprendizagem, fazendo o uso de situações problemas do cotidiano que utiliza a congruência entre os números para a decodificação de códigos bem como um controle de segurança.

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Uma congruência é uma relação entre dois números que, divididos por um terceiro – chamado módulo de congruência – deixam o mesmo resto.

Por exemplo, o número 9 é congruente ao número 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2 \pmod 7$.

Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros. O que não é muito comum é o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas.

Baseados nestes relatos, trazemos três atividades motivacionais (verificação dos dois últimos dígitos do CPF de uma pessoa, descobrir o dia em que a pessoa nasceu e encontrar o dígito de controle dos códigos de barras) que podem ser exploradas já nas classes do Ensino Fundamental como oportunidades de contextualização no processo de ensino / aprendizagem de matemática.

Desenvolvimento

Segue abaixo as aplicações de congruência como propostas de atividades a serem trabalhadas na Educação Básica:

Atividade 1 - Verificação dos dois dígitos de controle do CPF de uma pessoa

O número do Cadastro de Pessoa Física (CPF) de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são os dígitos de controle ou de verificação. A determinação desses dois dígitos de controle é também feita através da congruência aritmética, módulo 11, semelhante às que mostramos anteriormente.

No caso do CPF, o décimo dígito (que é o *primeiro dígito verificador*) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Se $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base {1, 2, 3, 4, 5, 6, 7, 8, 9} e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número S - a_{10} deve ser múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \pmod{11}$. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Atividade 2 - Criptografia e calendários: Em que dia da semana você nasceu?

O procedimento que escolhemos funciona para datas entre 1900 e 2399 (devido a uma particularidade dos anos bissextos terminados em “00”). Com algumas modificações, contudo, pode ser adaptado para atender quaisquer datas.

1) Calcule quantos anos se passaram desde 1900 até o ano em que você nasceu. Por exemplo, se você nasceu em 1980, irá anotar 80. Vamos chamar essa quantidade de A.
2) Calcule quantos 29 de fevereiro existiram depois de 1900. Para isso, basta dividir por 4 o valor A, sem considerar o resto da divisão. Vamos chamar essa nova quantidade de B.
3) Considerando o mês do nascimento, obtenha o número associado a ele, que está na tabela logo abaixo. Procure o mês e anote o número que está ao lado dele. Vamos chamar esse número de C.

Tabela dos meses			
Janeiro	0	Julho	6
Fevereiro	3	Agosto	2
Março	3	Setembro	5
Abril	6	Outubro	0
Maio	1	Novembro	3
Junho	4	Dezembro	5

4) Considere o dia do nascimento (x). Calcule x – 1, que vamos chamar de D.
5) Some agora os quatro números que você obteve nas etapas anteriores (A + B + C + D). Divida essa soma obtida por sete (7) e verifique o valor do resto dessa divisão.
6) Finalmente, procure esse resto na tabela a seguir. Você terá o dia da semana do seu nascimento ou de qualquer outra pessoa que queira descobrir.

SEGUNDA-FEIRA	0	SEXTA-FEIRA	4
TERÇA-FEIRA	1	SÁBADO	5
QUARTA-FEIRA	2	DOMINGO	6
QUINTA-FEIRA	3		

Finalizaremos abordando os conceitos básicos da congruência módulo k.

Se os inteiros a e b dão o mesmo resto quando divididos pelo inteiro k (k > 0) então podemos dizer que a e b são côngruos, módulo k e podemos representar: $a \equiv b \bmod k$;

Uma maneira equivalente de dizer isso é afirmar que a diferença (a – b) ou (b – a) é divisível por k, ou que k é divisor dessa diferença.

Atividade 3- Leitura dos códigos de barras brasileiros

A leitura do código de barras também utiliza a divisibilidade para encontrar o dígito verificador. Podemos dizer que esse dígito em específico consegue identificar se houve algum erro na sequência numérica.

O código de barras usado nos mercados brasileiros é o European Article Number (EAN-13), com 13 dígitos, onde os três primeiros dígitos correspondem ao país de fabricação e os nove dígitos seguintes ao produto do fabricante. O último dígito é o de controle, sendo escolhido de modo que <c, v>= 0 em Z_{10} , em que *v* é o vetor código dado, e *c* o vetor de controle sendo igual a [1,3,1,3,1,3,1,3,1,3,1,3,1] pertencente ao Z_{10}^{13} .

Essas atividades têm sido aplicadas junto a professores da Secretaria de Educação do Distrito Federal (SEEDF) e têm apresentado excelentes resultados.

Conclusão

Há objetivos diferentes com relação a professores e alunos. Relacionado ao primeiro, procurou-se mostrar que aritmética modular é uma forte ferramenta no ensino da matemática, pois permite aos alunos ampliar o raciocínio matemático devido a possibilidade de melhorar o raciocínio lógico, mostrando que determinados conteúdos não são difíceis de aprender por aqueles que não têm domínio ou mesmo conhecimento sobre tal. Quanto aos alunos, é esperado que, por meio de tal conteúdo motivador e intrigante das atividades propostas, seja possível promover o *desenvolvimento de um pensamento sistêmico e do estabelecimento de conexões entre conhecimentos prévios e habilidades necessárias à sua formação.*

Tais atividades já foram aplicadas em oficinas que vão desde um público de alunos de educação básica, do ensino superior, como também professores de diversas áreas da educação. O público partilhou que determinadas atividades estimulam o raciocínio matemático bem como a curiosidade de se aprender está matéria considerada por muitas pessoas uma matéria abstrata e difícil. Comprovando assim, o alcance dos objetivos das atividades propostas.

Mostra-se então para os professores e alunos mais um método de ensino e aprendizagem, fazendo uso de situações problemas para a aritmética modular.

Referências bibliográficas

Brasil, RPM. *Revista do Professor de Matemática*. Volumes 12 e 45. Sociedade Brasileira de Matemática.

Buchmann, J. (2002). *Introdução à Criptografia*. São Paulo: Berkeley.

Burnett, S., & Paine, S. (2002*). Criptografia e Segurança: o Guia Oficial RSA*. São Paulo: Campus.

Crato, N,. (2001).*Alice e Bob. Expresso* / Revista, 22 de Setembro, pp. 118-120.

Martini, R. (2001). *Criptografia e Cidadania Digital*. Rio de Janeiro: Ciência Moderna.

Onuchic, L.R.de la, & Allevato, N.S.G.(2015,novembro). *Proporcionalidade Através da Resolução de Problemas no Curso Superior de Licenciatura em Matemática*. Anais do VI Seminário Internacional de Pesquisa em Educação Matemática, Pirinópolis, GO, Brasil.

Singh, S. (2001). *O Livro dos Códigos*. São Paulo: Record.

Terada, R. (2000). *Segurança de Dados: Criptografia em Redes de Computadores*. São Paulo: Edgard Blucher. Disponível em: http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf