9º FEPEG FÓRUM DE ENSINO, PESQUISA, EXTENSÃO E GESTÃO
TRABALHOS CIENTÍFICOS APRESENTAÇÕES ARTÍSTICAS E CULTURAIS DEBATES MINICURSOS E PALESTRAS
23 A 26 SETEMBRO DE 2015
Campus Universitário Professor Darcy Ribeiro
ISSN 1806-549X
A HUMANIZAÇÃO NA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Relato de Experiência no Programa de Iniciação Científica Júnior (PIC) da OBMEP no Estudo de Tópicos de Aritmética e Criptografia Com o Grupo 4 – Pólo Montes Claros

Leidiane Cequeira Santos, Karoline Oliveira de Jesus, Marise Fagundes Silveira

Introdução

A Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) é um importante programa implementado pelo Instituto de Matemática Pura e Aplicada (IMPA) e pela Sociedade Brasileira de Matemática (SBM), incentivado pelo Governo Federal, no intuito de favorecer o interesse pela matemática nos estudantes de escolas públicas.

A prova da OBMEP é dividida em três níveis e realizada em duas fases. Os níveis 1 e 2 são aplicados para os alunos do Ensino Fundamental, para o 6º e 7º anos (Nível 1) e 8º e 9º anos (Nível 2). Já o nível 3 é aplicado para os alunos do Ensino Médio. Na primeira fase, participam todos os alunos inscritos pela escola, e as provas são compostas de questões de múltipla escolha, passando para a segunda fase 5% dos alunos inscritos em cada escola. As provas da segunda fase são compostas por questões discursivas que envolvem a resolução de problemas.

Os alunos da segunda fase que obtêm um melhor desempenho são premiados com medalhas e menções honrosas, além disso, os medalhistas podem participam do Programa de Iniciação Científica Jr. (PIC) no ano seguinte e se estiverem matriculados em escola pública são contemplados com uma bolsa de estudo financiada pelo Conselho Nacional de Pesquisa (CNPq).

As atividades realizadas no PIC são compostas de encontros presenciais e virtuais, discussões virtuais no fórum da OBMEP, denominado Hotel de Hilbert (HH), e tarefas para serem executadas em casa e no Fórum. Nos encontros presenciais os alunos são organizados por grupos de acordo com a quantidade de vezes que foram medalhistas e cada grupo possui um planejamento com os temas (Módulos) a serem estudados. Para o Grupo 4 (G4) - tema deste trabalho os encontros são organizados em 4 módulos:

MÓDULO I – ARITMÉTICA E CRIPTOGRAFIA
MÓDULO II – GEOMETRIA
MÓDULO III – COMBINATÓRIA
MÓDULO IV – INDUÇÃO MATEMÁTICA

No presente trabalho será abordado apenas o tema do Módulo I: Aritmética e Criptografia. A palavra aritmética é a denominação de uma ciência, que provêm do vocábulo *arithmos*, que significa número. Os números naturais foram se formando pela prática diária de contagens. Isto é, antigamente o homem conhecia de forma intuitiva conceitos que aplicava em sua vida e desta forma chegou a formalizar a representação de quantidades.

Os números foram inventados pela humanidade pela necessidade da contagem de bens, no registro de tempo ou de inventários de terras. Estima-se que a primeira função estabelecida para os números foi a de quantificar, ou seja, de atribuir uma determinada quantidade a conjuntos específicos atendendo a uma necessidade na prática, dando inicio assim a necessidade do estudo a aritmética [1].

A aritmética é considerada um ramo da Matemática a qual lida com os números e com as operações possíveis entre eles, desta forma é considerada as ciências dos números [2].

Conforme os Parâmetros Curriculares Nacional (PCNs) o sistema de numeração decimal, juntamente com suas operações, faz parte da aritmética, que se constitui em uma das principais disciplinas nos currículos da Educação Básica [3].

A Criptografia (do grego kryptós, “escondido”, e gráphein, “escrita”) é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. É um ramo da Matemática, parte da criptologia [4].

Um dos métodos de criptografia mais utilizado atualmente é chamado de RSA (nome que surgiu através da união do nome dos seus criadores – R.L.Rivest, A. Shamir e L.Adleman). O mesmo foi inventado em 1978, quando os três trabalhavam no Massachussets Instute of Technology (M.I.T). Neste tipo de criptografia os números primos são bastante utilizados.

Este trabalho objetiva relatar a experiência vivida pelos alunos do Grupo 4 (G4) – pólo Montes Claros no estudo do Módulo I – Aritmética e Criptografia obtida através do PIC, que foi criado para estimular a melhoria da qualidade do ensino na escola básica e o apreço pelo estudo da matemática.

Materiais e Métodos

O estudo do Módulo I - Aritmética e Criptografia foi realizado nos três primeiros encontros do PIC, e organizado de acordo com o Quadro 1. Foram adotadas as apostilas *Iniciação à Aritmética*, de Abramo Hefez, e *Criptografia*, de Severino Collier Coutinho. No primeiro encontro foram estudadas as propriedades aritméticas dos números inteiros, no segundo encontro foram estudados os temas Aritmética Modular, Inversos Modulares e Algoritmo Chinês do Resto, e no terceiro encontro, Potência e Criptografia. Ao final de cada encontro presencial (exceto o primeiro) foi feita uma avaliação a cerca do conteúdo estudado.

No primeiro encontro, foram trabalhados os conteúdos Divisão Euclidiana, Paridade, Resto da Divisão, Mínimo Múltiplo Comum, Máximo Divisor Comum, Aplicações da Relação de Bèzout e Equações Diofantinas Lineares. Os problemas propostos inicialmente, em sua maioria, são aplicações numéricas ou demonstrações matemáticas, mas conforme se avança nos assuntos, os problemas começam a ser mais abundantemente aplicados ao cotidiano e se percebe a conexão dos teoremas estudados anteriormente. Por exemplo: De que maneira podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?"[5] Para não resolvê-lo após inúmeras tentativas é preciso saber o conteúdo citado acima.

No segundo encontro, foi trabalhado a Aritmética Modular e suas Propriedades, Congruência Modular, Critérios de Divisibilidade Modular, Inversos Modulares (Definição, Existência, Inexistência), Algoritmo Chinês do Resto e Teorema Chinês do Resto, que são utilizados, entre outros, a resolver problemas do tipo: "Três fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Um certo ano cada um deles foi a um mercado diferente vender o seu arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era 87 kg. Ele vendeu tudo o que podia e voltou para casa com 18 kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 170 kg e voltou para casa com 58 kg. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 143 kg e voltou (ao mesmo tempo que os outros dois) com 40 kg. Qual a quantidade mínima de arroz que eles podem ter cultivado, no total?"[4]

Seguindo o planejamento acadêmico do PIC, no terceiro encontro foram abordados Restos de Potências, Potências Modulares, Ordem de um Inteiro Modular, O Teorema de Fermat, Potências, Módulos Primos e Módulos Compostos, que possibilita agregar novos conhecimentos para a resolução de desafios matemáticos que se tornariam mais complicados sem esse saber. Esse estudo facilita desde a definição de restos de grandes potências até a resolução de problemas básicos do cotidiano. E, para finalizar o Módulo I, é visto o tema Criptografia RSA. Após explicar que esse conteúdo depende do cálculo de resíduos de potências, o capítulo é dividido em Pré-codificação, Codificando e Decodificando uma Mensagem e uma explicação de por que o método funciona.

Resultados e Discussão

Embora os conteúdos sejam interessantes e possuam bastantes aplicações, os alunos do G4 tiveram dificuldade considerável para aprendê-los, visto que estes temas geralmente não são ensinados na educação básica e, quando são, o são com pouco rigor matemático e aprofundamento. Por isso, o número de encontros destinados para esse fim não foi o bastante para que o aluno assimile tamanha quantidade de conteúdos novos e mais elaborados que o de costume.

A estrutura do programa ameniza bastante essa dificuldade: os estudantes podem acessar o fórum Hotel de Hilbert para pedir ajuda e compartilhar idéias, além de contar com os monitores e um professor para sanar suas dúvidas, mas ainda assim o processo de aprendizado deve ser rápido para que o aluno não fique prejudicado, o que afeta sua individualidade, aprendizado pleno e desempenho nas avaliações.

Conclusão

Através da participação no PIC, os alunos do G4 – pólo Montes Claros tiveram a oportunidade de aprofundar seu conhecimento com maior rigor matemático, neste trabalho, em especial em relação aos conteúdos de aritmética e criptografia, assuntos estes que geralmente não são abordados desta maneira na educação básica. Tiveram também a oportunidade de resolver problemas que não conseguiriam resolver com os conhecimentos adquiridos na escola básica.

ISSN 1806-549X

Além da aprendizagem nos encontros presenciais com colegas, monitor e professor, a participação do aluno no Fórum do site do PIC (Hotel de Hilbert - HH) possibilitou que os mesmos desenvolvessem também habilidades de aprender por conta própria ou em colaboração com os demais colegas.

Referências Bibliográficas

[1] IFRAH, G. Os números: história de uma grande invenção. 3.ed. Traduzido por Stella M. Freitas Senra. São Paulo: Globo, 1985.
[2] BAÑUELOS, A. T.; VELÁZQUEZ. P. A. La historia de las disciplinas escolares, una contribución esencial al conocimiento de la escuela. El caso de la Aritmética. Revista complutense de educación, Espanha: Oviedo, vol10, n.1, p. 305-33, 1999.
[3] BRASIL. Ministério da Educação. Secretária de Educação Fundamental. Parâmetros curriculares nacionais: terceiro e quarto ciclos do ensino fundamental: introdução aos parâmetros curriculares nacionais. Secretaria de Educação Fundamental Brasília: MEC/SEF, 1998.
[4] COUTINHO.S.C - Números Inteiros e Criptografia RSA - Rio de Janeiro - IMPA – 2014.
[5] HEFEZ, Abramo. Iniciação à aritmética. - Rio de Janeiro - IMPA – 2014.

Quadro1. Planejamento de Estudo do Módulo I

MÓDULO I – ARITMÉTICA E CRIPTOGRAFIA			
Encontro	**Objetivos**	**Assuntos**	**Material**
1	Estudar as propriedades aritméticas dos números inteiros.	Algoritmo da Divisão. Algoritmo do mdc de Euclides. Aplicações da Relação de Bèzout. Equações Diofantinas Lineares.	**Apostila 1:** *Iniciação à Aritmética*, de Abramo Hefez.
2	Apresentar o conceito de congruência de números inteiros e algumas de suas aplicações.	Congruências. Teorema Chinês do Resto.	**Apostila 7** *Criptografia*, de Severino Collier Coutinho
3	Aplicar propriedades de congruências à criptografia RSA.	Criptografia RSA.	**Apostila 7** *Criptografia*, de Severino Collier Coutinho.