UNIVERSIDADE ESTADUAL DE GOIÁS
UNIDADE UNIVERSITÁRIA CORA CORALINA
CURSO DE MATEMÁTICA

APRESENTAÇÃO DE CONGRUÊNCIA MODULAR NO ENSINO MÉDIO POR MEIO DA ARITMÉTICA

Jackelyne de Souza Medrado

GOIÁS
2009

JACKELYNE DE SOUZA MEDRADO

APRESENTAÇÃO DE CONGRUÊNCIA MODULAR NO ENSINO MÉDIO POR MEIO DA ARITMÉTICA

Monografia apresentada ao curso de Matemática da Universidade Estadual de Goiás – UEG, Unidade Universitária Cora Coralina, como um dos requisitos para a obtenção do grau de licenciatura plena em Matemática.

Orientador: Profº Ms. Rosemberg Pereira Serrano

GOIÁS
2009

UNIVERSIDADE ESTADUAL DE GOIÁS
UNIDADE UNIVERSITÁRIA CORA CORALINA
COORDENAÇÃO DE MATEMÁTICA

APRESENTAÇÃO DE CONGRUÊNCIA MODULAR NO ENSINO MÉDIO POR MEIO DA ARITMÉTICA

Jackelyne de Souza Medrado

Trabalho de Conclusão de Curso apresentado a Coordenação de Matemática da Unidade Universitária Cora Coralina da Universidade Estadual de Goiás, como parte dos requisitos para obtenção do grau de:

Licenciado em Matemática

03 de dezembro de 2009

Comissão Examinadora:

____

Prof. Ms. Rosemberg Pereira Serrano – UnUCC/UEG
(Orientador)

____

Prof. Ms. Luciano Feliciano de Lima – UnUCC/UEG
(Convidado)

____

Prof. Esp. Silvano Reis – UnUCC/UEG
(Convidado)

A meus pais, meus irmãos, meu noivo, amigos e professores, pois sem eles não teria conseguido finalizar esta jornada.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter iluminado meu caminho e me dado força para percorrer os 360 km diários nas idas e vindas de Aruanã a Cidade de Goiás.

A meus pais, Jaime da Silva Medrado e Maria Rita de Souza Medrado, que estiveram presentes nos momentos tristes e felizes, sempre de prontidão para me amparar.

A meus irmãos, Joannes de S. Medrado e Annysuhlyva de S. Medrado, meu noivo, Carlos Henrique A. de Novais e minha tia Lucinéia que sempre me apoiaram e me incentivaram a correr atrás dos meus objetivos.

A meus professores do Ensino Médio que acreditaram em mim e me incentivaram a continuar com meus estudos.

A meus professores do curso de matemática que contribuíram com o meu crescimento pessoal e intelectual.

Ao orientador, Professor Rosemberg P. Serrano, que me auxiliou na elaboração deste trabalho.

As minhas grandes mestras, Shirlei Serconek e Kênia Calaça, pelos ensinamentos transmitidos.

Aos meus amigos e companheiros de estrada, em especial, meu amigo Alexandre Álvares Farias Alves.

Aos meus colegas de curso, em especial meu amigo Wender da Rocha Silva e minha amiga Maisa Alves da Silva pelo companheirismo.

Aos motoristas dos ônibus das cidades de Mozarlândia, Araguapaz e Aruanã, em especial, o motorista e amigo Edson Pereira Maia, que nunca nos deixou desamparados nas estradas.

A todos os meus amigos que, de alguma forma, fizeram parte desta luta diária e me ajudaram a vencer os obstáculos encontrados no meu caminho.

A matemática é a rainha das ciências, e a teoria dos números e a rainha das matemáticas.

GAUSS

RESUMO

Este trabalho tem como objetivo mostrar a congruência modular no ensino médio utilizando conceitos da aritmética e situações vividas diariamente pelos alunos a fim de promover uma relação do conteúdo com situações práticas. A pesquisa foi aplicada na cidade de Aruanã-GO no Colégio Estadual "Dom Cândido Penso" na 3ª série do ensino médio. As análises didático-pedagógicas estão baseadas em estudiosos da educação e da educação matemática como D'Ambrósio, Skovsmose, Paulo Freire e norteada nos Parâmetros Curriculares Nacionais para o Ensino Médio. O método utilizado fortalece uma práxis educacional contextualizada, concreta e lúdica, pois na aplicação do mesmo foi proposta a extração de informações com objetos concretos do cotidiano como livros, revistas, produtos, cartões de identificação, onde possuem códigos específicos que caracterizam cada item citado acima, os quais são elaborados seguindo rigorosamente uma relação com a congruência modular, a qual verifica a veracidade de tais códigos. Além de atividades sobre fenômenos periódicos e jogos envolvendo a criptografia, ambos trabalhados sobre o ponto de vista da congruência modular. Este é um tema raramente trabalhado na educação básica apesar de ser muito rico, dinâmico e prazeroso que oferece excelentes oportunidades para o aluno obter uma assimilação do conteúdo e adquirir uma aprendizagem significativa.

Palavras chave: Congruência modular. Códigos de identificação. Dígito verificador. Criptografia. Contextualização.

ABSTRACT

This study to have how aims to show the congruence modular high school using concepts of arithmetic and situations experienced daily by students to promote a relationship of content to practical situations. The research was conducted in the city of Aruanã - GO in State College "Dom Cândido Penso" in the 3rd grade of high school. Analysis didactic and pedagogical scholars are based on education and mathematics education as D'Ambrosio, Skovsmose, Paulo Freire and guided in the national curriculum standards for high school. The method develops an educational praxis contextualized, practical and playful, as in its application was proposed to extract information with concrete everyday objects such as books, magazines, products, identification cards, which have specific codes that distinguish each item mentioned above , which are produced strictly in relationship with the congruence modular, which verifies the existence of such codes. In addition to periodic phenomena on activities and games involving encryption, both worked on the standpoint of matching modular. This is a topic rarely worked in basic education despite being very rich, dynamic and pleasant, which offers excellent opportunities for students to obtain an assimilation of content and develop a meaningful learning.

Key words: Congruence modular. Identification codes. Check digit. Encryption. Contextualization.

SUMÁRIO

1 INTRODUÇÃO

Atualmente vivemos em uma sociedade moldada com a evolução das tecnologias onde temos que lidar com muitas linguagens diferentes. Uma dessas linguagens é a linguagem numérica, que comumente chamamos de códigos de identificação. Estes códigos servem para identificar algo ou alguém, como por exemplo, o Cadastro de Pessoa Física (CPF) que é utilizado para reconhecer cada indivíduo da sociedade brasileira. Outro exemplo é o International Standard Book Number (ISBN) de catalogação de livros, CD-Roms e publicações em braile, que foi criado em 1967, que especifica informações do local de publicação, editora e o objeto catalogado. Assim como estes códigos temos ainda códigos de barras, Registro Geral (RG), Cadastro Nacional de Pessoa Jurídica (CNPJ), International Standard Serial Number (ISSN) e a Criptografia que requer conhecimentos matemáticos mais avançados.

Tratamos com essas informações diariamente, mas alguém já se perguntou como são formados esses códigos? Qual processo utilizado? Quem os criou?

Com intuito de responder essas curiosidades e entendermos melhor os mecanismos que utilizamos em nosso cotidiano, buscamos neste trabalho compreender a formação destes códigos de identificação, a relação da aritmética modular com os mesmos e aplicá-los no contexto da educação básica.

Para isso recorreremos à aritmética modular e ao conceito de congruência. A aritmética modular é uma das ferramentas mais importantes da Teoria de Números, a partir de seu conceito é possível trabalhar com os diferentes tipos de códigos numéricos de identificação, como os citados acima, e diversos fenômenos periódicos.

O trabalho em questão foi aplicado na 3ª série do Ensino médio, por meio de atividades que revelou ao aluno as aplicações da aritmética modular em ações que os mesmos executam corriqueiramente ou em situações curiosas, como por exemplo, saber em que dia da semana você nasceu, ou em que dia da semana dará seu aniversário daqui a cinquenta anos. Outro exemplo é a identificação de dados sobre um determinado produto quando se tem apenas códigos de numeração.

Estas são algumas situações que exemplificam o desenvolvimento deste e o quanto é interessante entendermos essa linguagem.

O principal objetivo deste trabalho é apresentar para os alunos da educação básica, especificamente alunos do ensino médio, as aplicações da congruência modular no seu cotidiano. Além disso, definir o conceito de congruência, verificar o processo de formação dos diferentes códigos numéricos de identificação, identificar algoritmos utilizados para obtenção dos códigos e listar exemplos de situações que necessitam da aritmética modular.

O problema em questão é como podemos utilizar a aritmética modular no ensino médio para promover uma aprendizagem significativa.

A aritmética modular é utilizada frequentemente, inclusive por alunos da educação básica, porém não se usa esta aplicabilidade para desenvolver conteúdos matemáticos nas escolas, os quais se tornariam riquíssimos e promoveria aulas lúdicas e contextualizadas, consequentemente tornando o ambiente de sala de aula um local de produção de conhecimentos mais agradável.

O presente trabalho monográfico é divido em quatro capítulos, onde inicia-se com reflexões sobre o ensino de matemática fundamentado em vários teóricos da educação e da educação matemática como Skovsmose, D'Ambrósio, Freire e nos Parâmetros Curriculares Nacionais para o Ensino médio. Neste primeiro capítulo é frisada a importância do diálogo, os meios para proporcionar uma aprendizagem significativa, a relevância da matemática crítica para os dias atuais e a necessidade de se pensar em um ensino dialético, reflexão-ação, levando o aluno a notar a relação do conhecimento com seu meio. Nos três capítulos seguintes trabalha-se a congruência propriamente dita, suas aplicações no cotidiano e a aplicação deste na sala de aula, respectivamente, os quais foram elaborados considerando as reflexões sobre o ensino relatadas no primeiro capítulo.

Também estão presentes neste trabalho nos itens apêndice e anexos, alguns conteúdos que especificam melhor termos utilizados em seu desenvolvimento, além de fotos e depoimentos da aplicação do trabalho.

2 REFLEXÕES SOBRE O ENSINO DE MATEMÁTICA

2.1 O ensino de matemática e os PCN

Os Parâmetros Curriculares Nacionais (PCN), para o ensino médio representam um documento curricular oficial de referência para a organização de propostas curriculares das secretarias de educação estaduais, que tem como objetivo apresentar um conjunto de reflexões para servir de orientação à prática docente. Na área de Ciências da Natureza, Matemática e suas tecnologias, especificamente no Conhecimento de Matemática, pretende-se

> Contemplar a necessidade de sua adequação para o desenvolvimento e promoção dos alunos, com diferentes motivações, interesses e capacidades, criando condições para sua inserção num mundo em mudanças e contribuindo para desenvolver as capacidades que deles serão exigidas em sua vida social e profissional. (PCN, 2000, p. 40)

De acordo com os PCN (2000), a matemática no ensino médio possui caráter formativo e instrumental. Formativo por que ajuda a estruturar o pensamento e o raciocínio dedutivo do aluno e instrumental por que é uma ferramenta que serve para a vida cotidiana e para várias tarefas específicas em quase todas as atividades humanas.

Além dos caráteres especificados acima, devemos perceber a matemática no ensino médio como uma ciência, com suas características estruturais que busca desenvolver no aluno uma autonomia para que possa continuar aprendendo e assim continuar-se aperfeiçoando ao longo da vida.

Assegurado na Lei de Diretrizes e Bases da Educação Nacional (LDB - nº 9.394/96), o ensino médio tem como objetivos principais, além da consolidação e o aprofundamento adquirido no ensino fundamental, o aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico.

De acordo com a LDB (nº. 9.394/96) não é coerente que as escolas sejam conteudistas e fiquem restritas ao ensino obsoleto sem perspectivas para o desenvolvimento do aluno. O ensino das disciplinas, em nosso caso particular da matemática, deve contribuir para que os alunos desenvolvam habilidades relacionadas à compreensão, análise, comunicação, criação, reflexão, investigação e também a contextualização sociocultural.

Os PCN (1997) dizem que o estudo deve possibilitar aos alunos o desenvolvimento da capacidade de resolver problemas práticos do cotidiano, mas não é isso que temos vivenciado na realidade escolar. Pelo contrário, os alunos que vão à escola frequentemente criam uma barreira entre o que é aprendido e o que se vivencia fora dela. Não conseguem ter uma visão das relações existentes entre essas duas realidades.

Percebe-se isto no exemplo citado por Moysés (1997) que trata do confronto entre a forma que um mestre-de-obras e estudantes de 8º ano do Ensino Fundamental realizam cálculos de proporções.

> [...] foram mostradas aos sujeitos quatro plantas de interiores, cada uma desenhada em uma escala diferente, sem explicitar, no entanto, qual escala estava sendo utilizada. A primeira tarefa que lhes foi solicitada consistia em, dada uma medida na planta, em uma determinada escala, e outra medida correspondente à parede real, descobrir qual era a escala utilizada. A segunda tarefa consistia em medir uma parede no desenho e, com base na escala usada, determinar a sua medida real na construção. [...] Os resultados mostraram a superioridade do mestre-de-obras em relação aos estudantes, em geral. (MOYSÉS, 1997, p. 65-66)

A autora ainda deixa claro que isto não implica que se deve ignorar a aprendizagem através dos algoritmos matemáticos, mas é necessário sempre estabelecer uma relação, uma contextualização, uma vez que é preciso pensar numa educação para a vida.

Segundo os PCN (2000) o ensino deve proporcionar oportunidades para que os alunos percebam as aplicações da matemática em variadas situações, o que transmite a idéia de um ensino contextualizado, além de propor aos alunos que desenvolvam análises e julgamentos, de resolução de problemas, de comunicação e representação, o que corresponde a uma visão de aprendizagem como construção de competências.

Contudo, devemos ter clara a idéia de que os PCN não são regras para serem cumpridas e sim norteadores no processo de ensino e aprendizagem.

2.2 A importância do diálogo na sala de aula

Uma das ferramentas fundamentais para haver uma interação entre professor e aluno é o diálogo, é ele quem possibilita a mediação do professor para com o aluno para promover a aprendizagem do aluno. Esta idéia fica muito clara nas palavras de Alro & Skovsmose:

> Aprender é uma experiência pessoal, mas ela ocorre em contextos sociais repletos de relações interpessoais. E, por conseguinte, a aprendizagem depende da qualidade do contato nas relações interpessoais que se manifesta durante a comunicação entre os participantes. Em outras palavras, o contexto em que se dá a comunicação afeta a aprendizagem dos envolvidos no processo. (ALRO; SKOVSMOSE, 2006, p. 12)

Quando se fala em diálogo, não se pensa apenas no seu sentido próprio, fala entre duas ou mais pessoas, conversação, colóquio, mas num sentido amplo, onde as pessoas que estão participando do diálogo almejam o mesmo objetivo e participam efetivamente para chegar a este objetivo comum. Assim havendo diálogo entre professor e os alunos, estes últimos, não serão apenas ouvintes, mas estarão construindo conhecimento.

Existem diversas formas de comunicação na sala de aula, porém geralmente não se presencia comunicação alguma entre professor e aluno e sim um monólogo onde apenas o professor fala e os alunos "acatam". Este fenômeno é constante nas aulas de Matemática, talvez por que o professor não possui a formação apropriada para ministrar aulas de matemática ou não se interessa em buscar novos métodos que, de fato, promovem uma aprendizagem significativa. Por esta razão, Alro & Skovsmose (2006, p. 22) denominaram esta ação como "Absolutismo burocrático, que estabelece em termos absolutos o que é certo e o que é errado sem explicitar os critérios que orientam tais decisões.".

Infelizmente este absolutismo burocrático faz parte da vida de muitos estudantes de matemática, taxando ainda mais a mesma como uma disciplina que "aponta erros e corrigi-os", deixando de lado uma reflexão sobre determinado problema. Tem-se que desmistificar esta idéia errônea sobre a matemática. O professor deve perceber que, como todas as disciplinas, a matemática é uma disciplina que exige que haja uma reflexão sobre os assuntos abordados, para encontrar a melhor maneira de trabalhá-la. Da mesma forma que os alunos aprendem a ler, escrever e interpretar diversos contextos sociais eles devem aprender manipular as operações matemáticas relacionando-as também criticamente com o contexto social.

Para que haja uma ação-reflexão-ação na educação matemática, precisamos diversificar os métodos utilizados em sala de aula, saindo um pouco do método tradicional, onde o professor explica um assunto novo, passa alguns exemplos e aplica uma lista enorme de exercícios mecanizados, nos quais os alunos não irão desenvolver um raciocino lógico para conseguir respondê-los, apenas seguirão os mesmos passos dos exemplos dados. Em aulas como essa, não é necessário um diálogo, pois os alunos apenas seguem os passos desenhados pelo professor.

O diálogo também não pode ser entendido como uma tática, uma técnica, pois assim perderia seu verdadeiro sentido. Deve ser compreendido como parte integrante da natureza histórica dos seres humanos, é por meio do diálogo que os seres humanos, passam por várias transformações e se tornam cada vez mais seres críticos e comunicativos. Segundo Shor & Freire,

> Ao nos comunicarmos, no processo de conhecimento da realidade que transformamos, comunicamos e sabemos *socialmente*, apesar de o processo de comunicação, de conhecimento, de mudança, ter uma dimensão individual. Mas aspecto individual não é suficiente para explicar o processo. Conhecer é um evento social, ainda que com dimensões individuais. O que é o diálogo, neste momento de comunicação, de conhecimento e de transformação social? O diálogo *sela* o relacionamento entre os sujeitos cognitivos, podemos, a seguir, atuar criticamente pra transformar a realidade. (SHOR; FREIRE, 1986, p.65)

A educação dialógica, já possui certa problematização permitindo que se obtenha a consciência dos indivíduos sobre os temas abordados, assim quando o indivíduo participa na investigação do seu mundo temático ele se torna vulnerável a admirações, e esta por sua vez, possibilita a capacidade de criticá-lo e transformá-lo.

Vários pesquisadores tentam identificar os padrões de comunicação no ensino de matemática tradicional, como por exemplo, Alro & Skovsmose dão atenção a um aspecto singular a este ensino, “o paradigma do exercício”:

> Esse paradigma tem grande influência na Educação Matemática no que diz respeito à organização das aulas, aos padrões de comunicação entre professor e alunos, bem como ao papel que a Matemática desempenha na sociedade como um todo, por exemplo, com uma função fiscalizadora (exercícios de matemática encaixam-se

> perfeitamente em processos de seleção). [...] Nem o professor, nem os alunos participam da elaboração dos exercícios. (ALRO; SKOVSMOSE, 2006, p.52)

Como estes exercícios aplicados no ensino de matemática tradicional contribuirão com o desenvolvimento do aluno se nem mesmo o professor está presente na sua elaboração? Certamente é um assunto bastante contraditório, pois quem conhece e vivencia a realidade social não tem participação alguma na elaboração destes exercícios rotineiros propostos no livro didático. É preciso repensar estes métodos tradicionais da matemática para que se possa desenvolver aulas em que exista uma comunicação entre professor e aluno.

É necessário sair destes exercícios mecanizados para adentrar nos “cenários de investigação”.

> Podemos tentar abandonar o paradigma do exercício para entrar em um ambiente de aprendizagem diferente, que chamamos cenários para investigação. Eles são, por natureza, abertos. Cenários podem substituir exercícios. Os alunos podem formular questões e planejar linhas de investigação de forma diversificada. Eles podem participar do processo de investigação. Num cenário para investigação, a fala “O que acontece se...?” deixa de pertencer apenas ao professor e passa a poder ser dita pelo aluno também. E outra fala do professor, “Por que é dessa forma...?”, pode desencadear a fala do aluno “Sim, por que é dessa forma...?”. (ALRO; SKOVSMOSE, 2006, p. 55-56)

Quando se trabalha nos cenários de investigação, deixa-se de apenas imaginar situações com exercícios surreais, hipotéticos, isto é, exercícios que situam-se numa semi-realidade dentro de paradigma de exercícios, e passa-se a vivenciar uma realidade no desenrolar do exercício, o que permite ao aluno opinar, perceber se determinada solução é conveniente e, o que é mais significativo, verificar que existem diversas maneiras de pensar e resolver um problema.

> Exercícios baseados em dados da vida real abrem uma brecha no ensino tradicional de Matemática e desafiam o absolutismo burocrático. Por exemplo, torna-se difícil manter a premissa de que uma-e-somente-uma-resposta-está-certa à medida que se torna relevante questionar as informações contidas no exercício. A metafísica que impera no ensino tradicional de Matemática começa a ruir. (Idem, 2006, p. 55)

O professor deve refletir, agir e refletir novamente sua ação para conseguir levar suas aulas para um cenário de investigação, e consequêntemente, levar os alunos a uma produção de significados, através de convites para um cenário para investigação, onde os alunos são condutores e participantes ativos do processo de investigação.

Alro & Skovsmose (2006) denominam este modelo de aula como "cooperação investigativa", onde o aluno estabelece contato com o tema proposto, percebe, reconhece, posiciona, pensa alto, reformula, desafia e avalia, por meio da comunicação com o professor.

Um dos obstáculos que encontramos na Educação Matemática para o estabelecimento desta "cooperação investigativa" é que, por mais que o professor desenvolva todo um planejamento com atividades voltadas para situações reais, para um cenário investigativo, acaba apresentando a resposta certa ou a maneira certa de fazer o exercício e este fato contraria o sentido de uma investigação, uma vez que não foi o aluno que encontrou o caminho mediado pelo professor.

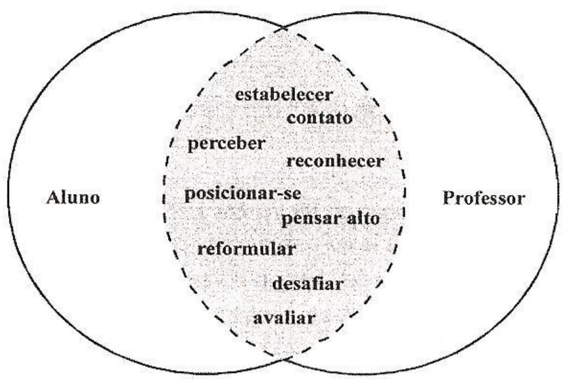


Figura 1 - O Modelo de Cooperação Investigativa
Fonte: ALRO; SKOVSMOSE, 2001, p.69.

Uma forma de se fixar o diálogo nas aulas de Matemática é abandonar o paradigma dos exercícios caminhando para os cenários de investigação, assim modifica-se o ambiente de aprendizagem, conseguindo-se efetuar uma aprendizagem significativa.

Com base no que foi exposto e nas idéias de Skovsmose, percebe-se que o ensino dialógico promove uma educação matemática crítica, onde educação matemática e democracia estão inter-relacionadas.

> A relação entre Educação Matemática e democracia é crítica. E se a Educação Matemática deve ser organizada para apoiar ideais democráticos, então se torna essencial rever e refazer todos os aspectos da Educação Matemática. Especificamente, torna-se essencial estudar o que se passa em sala de aula, na medida em que a sala de aula representa uma microssociedade, e não podemos imaginar uma educação para a democracia sem que valores democráticos básicos sejam aplicados de verdade em sala de aula. Isso significa que devemos examinar as relações entre professor e alunos, bem como a natureza do processo investigativo que eles vivenciam. (ALRO; SKOVSMOSE, 2006, p.142)

Os autores consideram que as qualidades de comunicação associados ao diálogo constituem uma aprendizagem crítica da Matemática, onde o aluno aprende a fazer uma “leitura crítica” do meio em que vive. Alro & Skovsmose fazem uma adaptação do termo literacia, utilizado por Paulo Freire para identificar essa leitura crítica que o aluno faz, denominando “matemacia”.

Segundo Alro & Skovsmose (2006), “Empregamos matemácia para designar uma competência ainda não muito bem específica que inclui leitura crítica do contexto sociopolítico”. Então quando há referência à matemática crítica, não basta que o aluno faça determinados cálculos. Além dos cálculos ele tem que compreendê-los e trazê-los para o seu cotidiano, ao refletir sobre os mesmos, estaremos trabalhando com a Matemacia.

2.3 As vertentes no Ensino de Matemática

2.3.1 Educação Matemática e Educação Crítica

Muito se tem falado sobre a educação matemática e os processos utilizados para tal firmar-se como educação, o estudo de matemática crítica é recente, mas já mostrou-se bastante eficiente para o ensino-aprendizagem.

Hoje a educação não é pensada apenas para formar mão-de-obra para nossa sociedade capitalista, ela almeja a formação de pessoas críticas que possuam a capacidade de relacionar, refletir, criar, agir, enfim, serem ativas e contribuírem com o desenvolvimento da sociedade. E para atingir estes objetivos faz-se necessário valer-se da Educação Crítica.

Com a educação matemática crítica, trabalha-se a realidade com o aluno e leva-se o mesmo a possuir uma opinião crítica a respeito desta realidade trabalhada. Obviamente está fora do ensino tradicional de matemática trabalhar com a educação crítica, pois segundo Skovsmose,

> Na educação Crítica, é essencial que os problemas se relacionem com situações e conflitos sociais fundamentais, e é importante que os estudantes possam reconhecer os problemas como "seus próprios problemas", de acordo com ambos os critérios subjetivo e objetivo da identificação do problema na Educação Crítica. Problemas não devem pertencer a "realidade de faz-de-conta" sem nenhuma significação exceto como ilustração da matemática como ciência das situações hipotéticas. (2001, p. 24)

Hoje é comum que os alunos que estão saindo do ensino médio encontrem uma dificuldade tremenda no ensino superior, pois não tiveram uma preparação adequada durante sua vida escolar. Isso se deve ao fato de ainda se trabalhar educação matemática de forma tradicional, onde os alunos aprendem apenas mecanicamente, e não conseguem refletir, aliás, são forçados a não fazer tais reflexões perante um determinado problema. Assim há menos possibilidade de formular, criticar e desenvolver maneiras de entender o problema, nas palavras de Skovsmose (2001), "os alunos não são convidados a matematizar".

É importante ressaltar que a educação crítica não é trabalhada sem o auxílio da educação matemática, e vice-versa, elas não sobrevivem sem uma integração. Pois nada adianta trabalhar a educação matemática sem relacioná-la com a vida, do mesmo modo, trabalhar com educação crítica sem ter um princípio educativo que se pretenda alcançar.

Contudo, deve-se tomar a educação crítica como base na aprendizagem, pois assim pode-se aprimorá-la identificando suas falhas e, se possível, corrigindo para melhorar o ensino na educação matemática. Não é possível deixar esta visão de ensino porque nela encontra-se uma aprendizagem através de reflexões, isto é, um conhecimento reflexivo.

Vale abrir um parêntese aqui para entender melhor a importância deste conhecimento reflexivo. Para isso vale considerar um exemplo citado por Skovsmose (2001) sobre o uso de carros: uma pessoa quando vai comprar um carro antes se prepara para estar apto a dirigi-lo e compreender alguns aspectos mecânicos (pelo menos na teoria é assim, há algumas exceções na prática). Então o compra e passa a usá-lo, um ato mecânico comum a todos, mas onde fica a reflexão sobre as conseqüências econômicas e sociais do uso de carros? A maioria das pessoas não pensa nisso, mesmo vivenciando algumas de suas conseqüências como o aquecimento global, esta diversificação climática que estamos vivendo e que tende a piorar, se preocupam apenas em “usar carros”.

Para poder entender e discutir determinadas implicações sociais, econômicas, política, entre outras, é necessário conhecer os princípios básicos e as condições que estão por trás de tal fenômeno. Como no caso desta pesquisa, a utilização de sistemas de identificação, não se pode ter apenas uma atitude mecânica para usá-los, principalmente nesta sociedade tecnológica em que se vive hoje, onde é muito fácil fraudar estes sistemas de identificação para tirar proveitos sem arcar com as conseqüências. Para evitar tais fraudes é preciso entender o processo de construção dos sistemas de identificação e aprender a usá-los de modo seguro. Quando busca-se estas ações está se praticando um conhecimento reflexivo.

Em resumo, não se pode apenas entender o conhecimento tecnológico, deve-se fazer uma reflexão sobre este conhecimento. Nas palavras de Skovsmose, “A tese fundamental em relação ao conhecimento tecnológico e reflexivo é a de que o conhecimento tecnológico, em si, é incapaz de predizer e analisar os resultados de sua própria produção; reflexões são necessárias” (2001, p.85).

2.3.2 Como Enxergar a Educação Matemática

Quem nunca ouviu alguém dizendo: “Eu odeio matemática, não sei pra que estudar matemática, não a utilizo mesmo?” É comum se ouvir esta frase, é raro encontrar uma pessoa que se interesse pela matemática. Contudo, estas pessoas que disseminam estas frases nunca pararam para refletir o que estão dizendo, será mesmo que não precisam da matemática?

Nem sempre a culpa é da pessoa que esta falando isso e sim de sua formação escolar, particularmente a educação matemática que teve. Com certeza, pessoas que possuem este pensamento da matemática tiveram aulas tradicionais, onde não aprendiam fazer nenhuma contextualização para mostrar o quanto o ensino da matemática é importante para suas vidas. Não se deve enxergar o ensino da matemática somente como aquele aprendido dentro de uma sala de aula direcionado por livros-textos com uma infinidade de exercícios mecanizados que não exigem esforço mental algum. Tais ensinamentos são amplos e continuam fora dos limites impostos por uma sala de aula.

A matemática está presente, em praticamente, todos os lugares, desde o momento de efetuar pequenos cálculos, analisar medidas, comprimentos, entre outros fatos corriqueiros dentro das residências, até ações fora dela. Como fazer compras em supermercados, analisar preços nas lojas, identificar a melhor opção de compra, executar transações bancárias, observar o processo de leitura dos códigos de barras de produtos, fazer compras pela internet, utilizar cartões de créditos, em diversos programas de computadores, fazer financiamentos, analisar as probabilidades existentes em eleições, aumento de preços de produtos, partidas de futebol, etc. São múltiplos e diversos os momentos em que a matemática está presente, inclusive em sistemas utilizados para identificação.

Toda essa diversidade enumerada é matemática. Consequentemente quando se coloca em ação estes itens, se está também praticando a educação matemática. O que já nos permite retornar ao questionamento inicial: Como é possível odiar a matemática se ela é necessária para desenvolver todas essas tarefas? E mais: O que faz crer que não se vai utilizá-la no cotidiano? É necessário revermos o conceito sobre educação matemática e procurar enxergá-la como ferramenta fundamental para o desenvolvimento de ações na sociedade tecnológica que vivemos.

Skovsmose esclarece a idéia do que vem a ser a educação matemática e onde ela ocorre:

> Educação matemática pode ocorrer em quaisquer situações. Eu uso a palavra educação matemática quando eu desejo me referir a situações onde os processos de aprender e ensinar matemática estão ocorrendo. Assim, educação matemática torna-se um rótulo que cobre tudo e eu desejo ignorar as conotações que indicam apenas os processos de ensino e aprendizagem que ocorrem na escola. Educação matemática ocorre em todo lugar. (SKOVSMOSE, 2007, p. 49)

.

Dando ênfase a educação matemática no ensino médio observa-se que a educação escolar teve um ganho muito importante com a inovação da LDB, onde estabelece o ensino médio como parte da educação básica, afirmando a necessidade de universalização desse nível de ensino. O ensino médio deve oferecer formação geral, ficando a profissionalização para cursos concomitantes ou posteriores ao ensino médio. E ainda propôs a flexibilidade na organização curricular, nas formas de pensar o tempo na escola e a trajetória escolar do aluno.

Apesar de todas essas inovações no ensino médio é necessário definir o rumo e objetivos do trabalho a ser desenvolvido para que haja uma aprendizagem significativa para que deixe de ser apenas uma sombra do Ensino Fundamental.

> A aprendizagem é uma relação dialética reflexão-ação, cujo resultado é um permanente modificar da realidade. E nesse ciclo realidade-reflexão-ação-realidade que reside o búsilis na nossa busca de desvendar comportamento individual, comportamento social e comportamento cultural. (D'AMBRÓSIO, 1986, p.49)

Como o autor destaca, a realidade é uma relação dialética reflexão-ação, os alunos do ensino médio têm que compreender esta relação e atuar nela para poder interferir na realidade e contribuir com este ciclo, para, consequentemente, contribuir com o desenvolvimento social e cultural da sociedade em comunidade ou grupo em que está inserido.

A matemática, assim como outras disciplinas, possui um papel fundamental na efetivação dessa relação dialética, deve-se apenas encontrar o caminho certo na educação escolar para tal efetivação.

3 ARITMÉTICA MODULAR

Iniciaremos este capítulo trabalhando alguns conceitos preliminares e propriedades, para poder chegar então ao conceito de congruência e assim permitir ao leitor que compreenda os passos utilizados no desenvolvimento deste trabalho.

3.1 Conceitos preliminares

Para compreender o conceito de congruência, é necessário antes possuir noções de múltiplos e divisores, divisão euclidiana, e familiaridade com máximo divisor comum e mínimo divisor comum, pois utilizaremos estes conceitos na próxima seção a fim de facilitar os cálculos.

Iniciaremos conceituando múltiplos e divisores.

Diz-se que um número inteiro a divide um inteiro b se $b = ac$ para algum c pertencente ($\in$) aos inteiros ($\mathbb{Z}$). Quando isto acontece também se diz que a é divisor de b ou que b é múltiplo de a (ou divisível por a). Em $\mathbb{Z}$ o conjunto dos múltiplos de um dado elemento a será também indicado por $M_a = \{0, \pm a, \pm 2a, \ldots\} = M_{(-a)}$.

Veremos a seguir um teorema muito importante na matemática, em particular, na congruência modular, conhecido como algoritmo de Euclides[1].

Teorema: Para quaisquer $a, b \in Z, b > 0$, existe um único par de inteiros q e r, de maneira que $a = bq + r$, onde $0 \leq r < b$.

Na igualdade que expressa o teorema, os elementos a, b, q e r são chamados respectivamente dividendo, divisor, quociente e resto na divisão euclidiana de a por b.

Exemplo: Apliquemos o algoritmo aos números $a = -38$ e $b = 8$. Observemos que o primeiro múltiplo de 8 que supera -38 é -32. Ou seja: $-32 = (q + 1) \, . \, 8$, o que implica $q = -5$. Daí: $r = a - qb = -38 - (-5) \, . \, 8 = 2$

---

[1] ver demonstrações em: DOMINGUES, Hygino. **Fundamentos da Aritméica.** São Paulo: Atual, 1991.

Assim: *-38 = 8 . (-5) + 2,* onde *-5* é o quociente e *2* o resto.

Utiliza-se o algoritmo de Euclides também no cálculo do máximo divisor comum (mdc)[2], o qual se define a seguir:

Sejam *a* e *b* números inteiros quaisquer. Entendemos por máximo divisor comum de *a* e *b* e indicamos por *mdc (a,b)* o número inteiro positivo definido por: $mdc(a,b) = mdc(|a|,|b|)$ (lê-se: máximo divisor comum de módulo da *a* e módulo de *b*), onde o segundo membro indica, obviamente, o máximo divisor comum de $|a|$ e $|b|$ nos Naturais ($\mathbb{N}$).

Vejamos um exemplo de como calcular o *mdc* dos inteiros 30 e 60.

Os divisores positivos de 60 são: 1, 2, 3, 4, 6, 10, 15, 20, 30, 60.

Os divisores positivos de 30 são: 1, 2, 3, 5, 6, 10, 15, 30.

Os divisores comuns são, portanto: 1, 2 3, 6, 10, 15, 30.

Portanto, o máximo divisor comum é igual a 30 e, indicamos: $mdc(60,30) = 30$.

Na prática, para calcularmos o *mdc* de números maiores utiliza-se a fatoração em números primos.

A seguir definiremos o mínimo múltiplo comum:

Dados a, b $\in Z$, existe e é único o mínimo múltiplo comum de $|a|$ e $|b|$ em $\mathbb{N}$. O número m é chamado também mínimo múltiplo comum de a e b. Notação: *m* = *mmc* (a, b).

Vejamos um exemplo de como calcular o *mmc* dos inteiros 40 e 30.

Os múltiplo positivos de 40 são: 0, 40, 80, 120, 160, 200, 240,...

Os múltiplos positivos de 30 são: 0, 30, 60, 90, 120, 150,...

Portanto, o mínimo múltiplo comum é igual a 120 e, indicamos: $mmc(40,30) = 120$.

Assim como no *mdc*, para calcularmos o *mmc* de números grandes utiliza-se o uso da decomposição em fatores primos dos números.

3.2 Congruências

---

[2] Ver SILVA, Valdir Vilmar da. **Números: construção e propriedades**. Goiânia, Ed. da UFG, 2003, p. 64-63.

O conceito de congruência, bem como a notação através da qual se torna um dos instrumentos mais fortes da Teoria de Números, foi introduzido por Karl Friedrich Gauss (1777 – 1855) em sua *Disquisitiones Arith*meticae de 1801. Foi a partir desta obra que se desenvolveu essa teoria.

Antes de apresentarmos as definições e propriedades relacionadas à congruência, vamos desenvolver um exemplo e diversas perguntas, para familiarizarmos com o tema.

O exemplo que segue foi elaborado por Sá (2006) e aplicado em sala de aula durante o desenvolvimento da aplicação desta pesquisa:

A seguir temos uma seqüência de números naturais agrupados em 6 linhas horizontais e seguindo a uma determinada ordenação. Observe:

0	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
1	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91
2	8	14	20	26	32	38	44	50	56	62	68	74	80	86	92
3	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93
4	10	16	22	28	34	40	46	52	58	64	70	76	82	88	94
5	11	17	23	29	35	41	47	53	59	65	71	77	83	89	95

É claro que poderíamos estender esta sequência, que fizemos até 95, o quanto desejássemos.

1. Em qual linha horizontal você acha que estaria localizado:

   a) O número 124?

   b) O número 327?

   c) O número 440?

   d) O número 12345658?

2. Qual o número imediatamente à direita do 23? E do 34? E do 45? E do 623? E do número natural *n*?

3. Qual o número imediatamente à esquerda do 65? E do 92? E do 400? E do 234 786? E do número natural *p*?

4. Como você poderia descrever todos os números que estão na mesma linha que o zero? E na linha do 1? E na linha do 2? E na linha do 3? E na linha do 4?
5. Como você poderia descrever todos os números que estão na mesma linha que o número 5?
6. Se você somar dois números quaisquer que estão na linha do zero, em qual linha vai estar o resultado dessa soma?
7. Se você subtrair dois números quaisquer que estão na mesma linha, em qual linha vai estar o resultado dessa subtração?

O exemplo acima é um caso que chamamos de congruência, módulo 6.

O número 13, por exemplo, é congruente ao número 37, módulo 6, e isso significa que esses dois números deixam o mesmo resto quando divididos por 6 (verifique que ambos estão na mesma linha que o número 1). Verificando:

$$13 = 6 \times 2 + 1$$

$$37 = 6 \times 6 + 1$$

Simbolicamente, poderemos escrever: $13 \equiv 37$ (mod 6)

De acordo com o exemplo acima podemos formalizar o conceito de congruência modular: Sejam *a*, *b* e *m* números inteiros, *m* > 0. Dizemos que *a* é côngruo a *b*, módulo *m*, se *m* divide *(a – b)*. Indicado por: $a \equiv b(\text{mod}\, m)$.

Por exemplo: $7 \equiv 15(\text{mod}8)$, pois 8 divide (-8);

De modo geral, $a \equiv a\ (\text{mod}\, m)$, para todo $a \in Z$ e para todo $m > 0$, já que $a - a = 0$ e *m* divide 0.

O conceito de congruência estabelece uma relação sobre Z para a qual valem as propriedades a seguir:

Propriedade 1. Para todo $m > 0$, a relação $\equiv$ é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência:

i. $a \in Z \Rightarrow a \equiv a \pmod{m}$

ii. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

iii. $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Prova de *iii*: por hipótese *m* divide *(a – b)* e *m* divide *(b – c)*, temos uma propriedade que nos diz se *a* divide *b* e *a* divide *c*, então *a* divide *(bx +cy)*, para todo *x*, $y \in Z$, daí *m* divide *[(a – b) + (b – c)]*, ou seja, *m* divide *(a – c)*. Donde $a \equiv c \pmod{m}$.

Nota: sempre que $a \equiv b$ (mod *k*) pode-se dizer que *a* e *b* são côngruos entre si (ou côngruos, apenas) modulo *k*. Se *a* e *b* não são côngruos diremos que são incôngruos módulo *k* e escreveremos $a \not\equiv b \ (mod\ k)$.

Propriedade 2. Para quaisquer *a*, *b* ∈ Z $a \equiv b \pmod{m}$ se, e somente se, *a* e *b* fornecem mesmo resto na divisão euclidiana por *m*.

Prova:

($\Rightarrow$) Por hipótese $a = b + km$, para algum $k \in Z$. Supondo que a divisão euclidiana de *b* por *m* se expresse por $b = mq + r \ (0 \le r < m)$, então $a = b + km = mq + r + km = m(k + q) + r$. Como $(0 \le r < m)$, então *r* é o resto na divisão euclidiana de *a* por *m*.

($\Leftarrow$) Se $a = mq_1 + r$ e $b = mq_2 + r$ (0 < r < m), então $a – b = mq_1 – mq_2 = m(q_1 – q_2)$ o que implica $a \equiv b \pmod{m}$.

Propriedade 3. Se $a \equiv b \pmod{m}$, então $a \pm c \equiv b \pm c \pmod{m}$ e $ac \equiv bc \pmod{m}$, para todo $c \in Z$.

Prova da segunda afirmação: por hipótese $a – b = mq$, $q \in Z$, logo $ac – bc = m(qc)$ e isto significa que $ac \equiv bc \pmod{m}$.

Propriedade 4. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então $a \pm c \equiv b \pm d \pmod{m}$ e $ac \equiv bd \pmod{m}$

Prova da segunda afirmação: das hipóteses e da propriedade 3, decorre que $ac \equiv bc \pmod{m}$ e $cb \equiv db \pmod{m}$. Logo, pela transitividade: $ac \equiv bd \pmod{m}$.

Propriedade 5. Se $a \equiv b \,(\bmod m)$, então $ra \equiv rb \,(\bmod m)$ e $a^r \equiv b^r \,(\bmod m)$, para todo inteiro $r \geq 1$.

O exemplo a seguir ilustra algumas das propriedades listadas acima.

Exemplo: Mostremos que $10^{200} - 1$ é divisível por 11. Como $10 \equiv -1 \,(\bmod 11)$; então $10^{200} \equiv (-1)^{200} \equiv 1 \,(\bmod 11)$. Portanto $10^{200} - 1 \equiv 0 \,(\bmod 11)$ e daí se conclui que: $11 \big/ (10^{200} - 1)$

Propriedade 6: Se $ca \equiv cb \,(\bmod m)$ e $mdc(m,c) = d > 0$, então:

$$a \equiv b \left(\bmod \frac{m}{d} \right)$$

Prova: Por hipótese $c(a-b) = mk$, para algum $k \in Z$. Daí:

$\frac{c}{d}(a-b) = \frac{m}{d}k$ onde $mdc\left(\frac{c}{d}, \frac{m}{d}\right) = 1$. Donde $\frac{m}{d}$ divide *(a – b)* e, portanto $a \equiv b \left(\bmod \frac{m}{d} \right)$.

Corolário 1 Se $ca \equiv cb \,(\bmod m)$ e $mdc(c,m) = 1$, então $a \equiv b \,(\bmod m)$.

O exemplo a seguir ilustrará este resultado.

Exemplo: tomemos *c = 3, a = 6, b = 4* e *m = 2,* logo teremos que $3 \times 6 \equiv 3 \times 4 \,(\bmod 2) = 18 \equiv 12 (\bmod 2)$. Calculemos agora o *mdc* (2, 3):

Divisores de 2 são: 1, 2

Divisores de 3 são: 1, 3

Logo, *mdc* (2, 3) = 1

Portanto, pelo corolário 1, temos que $6 \equiv 4 \,(\bmod 2)$

Corolário 2 Se $ca \equiv cb \pmod{p}$, onde p é primo e p não divide c, então $a \equiv b \pmod{p}$.

Neste caso, basta observar que o fato de p não dividir c, implica que $mdc\ (p,\ c) = 1$, então caímos no caso do corolário 1, logo teremos que $a \equiv b \pmod{p}$.

4 ALGUMAS APLICAÇÕES DA ARITMÉTICA MODULAR NO COTIDIANO

4.1 Fenômenos Periódicos e a Congruência

Quando pensamos em fenômenos periódicos vem a idéia de repetição, de ciclo, esta é a sua caracterização, são fatos que se repetem com regularidade. Assim podemos caracterizar como fenômeno periódico o giro que a Terra faz nos seus períodos de rotação, translação e evolução, as horas do relógio, os dias da semana, do mês, do ano, as passagens da lua, os horários escolares, entre outros. O tempo que passa para completar o ciclo de cada um desses fenômenos periódicos são chamados de período, logo o período de rotação da Terra é 24 horas, as horas marcadas por um relógio analógico possui um período de 12 horas, os dias da semana possui um período de 7 dias, assim por diante.

Mas o que tem a ver a congruência modular com os fenômenos periódicos? Tem tudo a ver, o período estabelecido em cada fenômeno periódico é o modulo da congruência em questão, assim podemos, através da congruência modular, descobrir, por exemplo, em que dia da semana será um quarta-feira se transcorrer quarenta e cinco dias. Para uma melhor compreensão desta relação observemos o exemplo citado por Coutinho (2008) sobre horários escolares:

> Embora seja necessário descrever os horários de aula de cada matéria ao longo de todo o ano, simplificamos esta tarefa utilizando o fato destes horários se repetirem a cada sete dias. Assim, descrevendo a distribuição de aulas ao longo de uma semana, podemos estendê-la para todo o ano letivo, simplesmente repetindo o mesmo horário a cada semana. Por exemplo, imagine que sua mãe lhe pergunta se você terá aula de matemática no dia 23 de setembro. Para responder esta pergunta basta você descobrir em que dia da semana cai 23 de setembro e olhar o seu horário. Como hoje é segunda-feira 10 de setembro e como 23 - 10 = 13, o dia 23 está a 13 dias desta segunda. Por outro lado, 13 = 7 + 6. Só que, passado sete dias, estaremos de volta a uma segunda-feira e, a seis dias desta segunda temos um domingo; portanto, a resposta é que não há aula de matemática neste dia qualquer que seja o seu horário escolar. (p.38-39)

Façamos uma análise para compreender como foi usada a congruência modular. Primeiro temos que descobrir qual o período que está sendo usado, que é 7 dias, depois descobrir quanto tempo irá decorrer de hoje até o dia que queremos saber se vai ou não ter aula de matemática. Então, seja S o tempo decorrido, dividimos S por 7, período do fenômeno, teremos o quociente q e o resto r da divisão. Perceba que a cada sete dias caímos no mesmo dia que hoje. Logo, daqui a $S\text{-}r = 7.q$ dias terão passado q semanas e estaremos de volta a uma segunda feira. O dia da semana poderá ser analisado através do resto de divisão de S por 7, como mostra o esquema abaixo.

Resto →	0	1	2	3	4	5	6
Dia →	Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo

Voltando ao exemplo, o tempo decorrido foi 13 dias, como 13 divido por 7 deixa resto 6, o qual está correspondendo ao Domingo, então isso explica o fato.

Assim como este, existem outros exemplos interessantes que facilitam nossa compreensão de alguns fatos desde que saibamos enxergá-los pelo ponto de vista da congruência modular. Vejamos alguns exemplos elaborados por Ilydio de Sá envolvendo relógio e calendários.

4.1.1 Aritmética do relógio

Figura 2 - Relógio analógico
Fonte: www.brindmar.com/review/product/list/id/90/

Trata-se de um caso de congruência módulo 12 (nos relógios analógicos, é claro). Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1. 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5, e assim, sucessivamente.

$1 \equiv 13 \equiv 25 \equiv ..., \pmod{12}$

$5 \equiv 17 \equiv 29 \equiv ..., \pmod{12}$

Que horas um relógio analógico estará marcando se forem transcorridas 32 horas, depois das 3 horas?

Solução: Observe que 3 + 32 = 35 horas. Usando o algoritmo da divisão, dividindo 35 por 12, teremos:

$35 = 12 \times 2 + 11$. Pela propriedade 2, temos $35 \equiv 11 \pmod{12}$. O relógio estará marcando 11 horas.

Como se trata de um relógio analógico, se o horário citado,3 horas, fosse da manhã, a resposta seria 11 horas da manhã, se o horário citado, 3 horas, fosse da tarde, a resposta seria 11 horas da noite.

4.1.2 Calendários

Vamos supor que você saiba em qual dia da semana caiu o dia 1º de janeiro (em 2006) foi um domingo e deseja saber quando cairá outro dia qualquer (vale para qualquer ano). É só montar um quadro para essa primeira semana, que no caso será:

Domingo	**Segunda**	**Terça**	**Quarta**	**Quinta**	**Sexta**	**Sábado**
1	2	3	4	5	6	7

Verificamos aqui que estamos diante de um caso de congruência, módulo 7. Digamos que estivéssemos interessados em descobrir em que dia da semana se deu o dia 5 de julho de 2006 (e não temos um calendário em mãos, é claro). Primeiro precisamos ver quantos dias existem de 1 de janeiro até 5 de julho. Vejamos:

Meses	**Quantidade de dias**
Janeiro	31
Fevereiro	28
Março	31
Abril	30
Maio	31
Junho	30
Julho	5
Total	**186**

Observe que 2006 não é bissexto, logo fevereiro possui 28 dias.

Agora, é como se tivéssemos uma fila de 186 dias e estamos desejando saber, na congruência de módulo 7 (7 dias da semana) qual o correspondente ao 186.

Se dividirmos 186 por 7, usando o algoritmo de Euclides, teremos:

$186 = 26 \times 7 + 4$

Logo, o 186 é congruente a 4, módulo 7 ($186 \equiv 4 \pmod 7$). Como o dia 4 foi uma quarta-feira, o dia 186 também o será e, é claro, que todas as demais quarta-feiras deste ano foram representadas por números congruentes a 4, módulo 7.

4.2 Sistemas de Identificação

> Matemática é uma operação em muitos locais de trabalho, bancos, tapeçarias e em todas as lojas. Nós não estamos acostumados em pensar num caixa de supermercado como usando matemática. Entretanto, a leitura óptica do código de barra e o

> pagamento por cartão de crédito pressupõem que um gigantesco aparato matemático esteja em operação. (SKOVSMOSE, 2007, p.47-48)

Com a evolução dos tempos e o advento da tecnologia verifica-se a presença de números, particularmente da matemática, em quase todos os estágios da sociedade, onde geralmente são utilizados para identificação de objetos, empresas e até mesmo pessoas. Estes números são importantíssimos e carregam informações valiosas sobre os itens citados acima, um exemplo mais simples e freqüente se dá quando efetua-se compras em supermercados. Quem nunca se deparou com um problema de leitura do código de barra de um produto por meio daquelas máquinas de leituras em caixas de supermercado? Quando acontece um erro, a pessoa responsável pelo caixa digita o número do código de barra do produto num teclado para passar as informações sobre o produto e assim o cliente visualiza o preço do produto.

Se por um acaso, o caixa de supermercado digitar um número errado, e por coincidência digitar um código de outro produto mais caro, o cliente ficará no prejuízo? Certamente é difícil perceber um erro quando se trata de números. Já em um texto ortográfico, é fácil notar o erro, pois ou a palavra não faz parte do idioma ou não faz sentido com o contexto.

Para identificar erros cometidos ao transcrever um código numérico e também para minimizar fraudes, foram criados os chamados dígitos de verificação, como o próprio nome diz, eles servem para verificar se o código em questão está correto. Tais dígitos são normalmente formados estabelecendo uma relação de congruência.

Estes números de códigos de identificação estão presentes em diversos itens, como: códigos de barras, Cadastro de Pessoa Física (CPF), International Standard Serial Number (ISSN), International Standard Book Number (ISBN), Cadastro Nacional de Pessoa Jurídica (CNPJ), Registro Geral (RG), Titulo de Eleitor, Bilhete de Identidade (BI), Cartões de créditos, Nota Euro, Números de Identificação Bancária (NIB), Números de Identificação Fiscal (NIF), entre outros, mas abordaremos aqui só os cinco primeiros descritos, pois com eles teremos uma compreensão de como se aplica a congruências modular nestes sistemas de identificação, o procedimento para verificação dos restantes é análogo, variando em alguns casos a base considerada.

4.2.1 International Standard Book Number - ISBN

A Agência Brasileira do ISBN especifica-o como um sistema internacional padronizado que identifica numericamente os livros segundo o título, o autor, o país, a editora, individualizando-os inclusive por edição. Utilizado também para identificar software, seu sistema numérico é convertido em código de barras, o que elimina barreiras lingüísticas e facilita a sua circulação e comercialização. Criado em 1967 por editores ingleses, passou a ser amplamente empregado tanto pelos comerciantes de livros quanto pelas bibliotecas, até ser oficializado, em 1972, como norma internacional pela International Organization for Standardigation - ISO 2108 – 1972.

Em tal sistema, as publicações antes de 2007 são identificadas através de 10 algarismos, a partir de 01 de janeiro de 2007 passou-se a usar 13 dígitos, pois o crescente número de publicações estava esgotando a capacidade do sistema. Em ambos os casos o último número (dígito de verificação) é calculado através da aritmética modular envolvendo operações matemáticas com os outros dígitos. Esses dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

Vejamos como se processa o cálculo do dígito final do ISBN (verificação) no caso das publicações com 10 algarismos.

Representando por $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ a seqüência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base {10, 9, 8, 7, 6, 5, 4, 3, 2} e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser acrescentado à 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, $S + a_{10} \equiv 0 \ (mod\ 11)$.

Vejamos um exemplo:

Na contracapa do livro Números Inteiros e Criptografia RSA, da Série de Computação e Matemática, do IMPA, temos o seguinte código do ISBN: 85-24401-24-9. Vejamos o cálculo do dígito de verificação que, como estamos observando, é igual a 9.

Devemos primeiro pegar a seqüência formada pelos 9 primeiros dígitos e multiplicá-los, nessa ordem, pela base {10, 9, 8, 7, 6, 5, 4, 3, 2}, depois somar os produtos obtidos.

8 5 2 4 4 0 1 2 4 → código ISBN sem o dígito de verificação

10 9 8 7 6 5 4 3 2 → base

Efetuando as multiplicações correspondentes e somando os produtos obtidos, teremos:

$8 \times 10 + 5 \times 9 + 2 \times 8 + 4 \times 7 + 4 \times 6 + 0 \times 5 + 1 \times 4 + 2 \times 3 + 4 \times 2 =$

$= 80 + 45 + 16 + 28 + 24 + 0 + 4 + 6 + 8 = 211$

Dividindo o resultado por 11 teremos, usando o algoritmo de Euclides:

$211 = 19 \times 11 + 2$

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, ele terá que ser igual a 9, pois 11 – 2 = 9. O que confere o valor apresentado no código dado. Isso significa dizer que 211 + 9 = 220 é um múltiplo de 11, ou ainda, que $220 \equiv 0 \pmod{11}$.

No caso do ISBN com 13 algarismos o cálculo para a verificação do dígito de verificação é análogo ao código de barra European Article Numbering-13 (EAN-13), o qual será especificado na próxima subseção. Ao invés da base {10, 9, 8, 7, 6, 5, 4, 3, 2}, usa-se a base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3}.

As informações do ISBN são classificadas da seguinte forma:

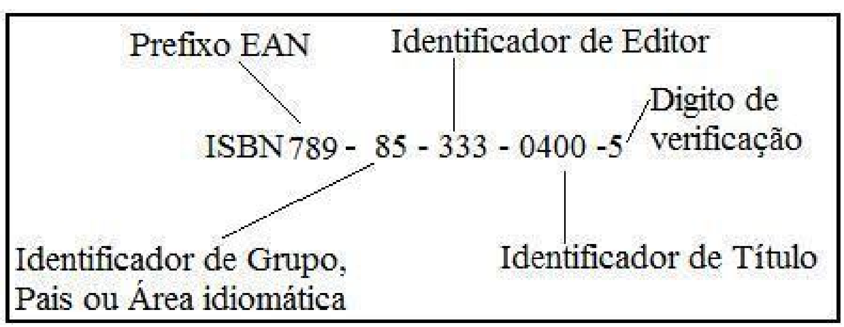


Figura 3 - ISBN 13 dígitos
Fonte: http://www.bn.br/portal/arquivos/jpg/ISBN.jpg

Como podemos observar na figura, quando se trata do ISBN com 13 algarismos, os três primeiros dígitos identificam o prefixo EAN que serve para identificar o país onde o produto foi fabricado, no exemplo acima o prefixo EAN identifica o Brasil. O primeiro grupo é o identificador de grupo, pais ou área idiomática, o grupo seguinte identifica o editor, o próximo grupo faz referência ao título da obra e por último tem-se o digito de verificação. No ISBN com 10 dígitos deve-se desconsiderar apenas o prefixo EAN.

4.2.2 Código de Barra EAN-13

Existem diversos códigos de barra[3] para a identificação de produtos em variadas categorias, como o código de barras 39 utilizado em inventário e não varejista, o código 25 utilizado, sobretudo em manuseio de inventários, em fichas de compensação bancária, na identificação de envelopes de acabamento de fotografias, em passagens aéreas, no manuseio de bagagens e cargas e em dezenas de outras aplicações, o código UCC-128 utilizado em aplicações logísticas e automação de vários setores produtivos e comerciais, UPC-A, UPC-E, EAN-8, EAN-13, todos com utilização em varejo, sendo que os dois últimos são adaptações européias dos dois primeiros. Existem também os códigos CODABAR, CODE-128, FIM, CMC7, ITF, ITF-14, JAN-8, JAN-13, MSI plessey, Pharmacode, POSTNET, cada uma com suas especificações.

Aqui abordaremos apenas o código de barra EAN-13, pois é o mais utilizado em todo mundo, desde aplicações de varejo até em publicações de livros e periódicos.

O EAN-13 é constituído de 13 algarismos sendo que o último é o digito de verificação, neste caso o módulo da congruência usada é 10, onde os fatores de multiplicação são os dígitos 1 e 3 que vão se repetindo da esquerda para a direita.

O cálculo para obtenção do dígito de verificação se dá da seguinte forma:

Se $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}$ a seqüência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{13} deve ser tal que ao ser somado com soma obtida, deve gerar um múltiplo de 10, isto é, se a soma obtida é S, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \ (mod\ 10)$.

Vejamos um exemplo:

Numa embalagem de caixa para bastonetes fabricada no Brasil temos o seguinte código de barra:

$$\boxed{789\text{-}6004\text{-}81416\text{-}2}$$

---

[3] Para detalhes sobre os códigos de barras citados, ver: tipos de códigos de barras. Disponível em:<http://br.geocities.com/dadosvariaveis/tipos.html>. Acesso em 05 de Jun 2009.

Vamos efetuar os cálculos para a determinação do dígito de verificação (que estamos vendo ser o dígito 2).

Devemos primeiro pegar a seqüência formada pelos 12 primeiros dígitos e multiplicá-los, nessa ordem, pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3}, depois somar os produtos obtidos.

7 8 9 6 0 0 4 8 1 4 1 6 → código de Barra sem o dígito de verificação

1 3 1 3 1 3 1 3 1 3 1 3 → base

Efetuando a soma dos produtos, teremos:

$7 + 24 + 9 + 18 + 0 + 0 + 4 + 24 +1 + 12 + 1 + 18 = 118$

Com o algoritmo de Euclides, podemos escrever $118 = 10\times 11 + 8$

Logo, o dígito de verificação será igual a 2, pois $10 - 8 = 2$. Note que $118 + 2 = 120$ (múltiplo de 10).

Daí temos que $120 \equiv 0 \pmod{10}$.

No código de barras com 13 algarismos, os três primeiros dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos 7, 8 e 9, que é o que identifica o país[4]); A GS1 BRASIL, órgão responsável pela emissão de códigos de barras, estabeleceu que os 4 ou 5 algarismo decimais seguintes representariam a empresa, ela utiliza 4 algarismo quando a empresa produz muitos produtos. Estão disponíveis no Brasil 6000 códigos de empresas nesta situação, estes códigos são numerados de 0000 a 5999. São utilizados 5 algarismos para empresas com menor número de produtos, neste caso, existem 40000 códigos, numerados de 60000 a 99999. Os dígitos seguintes, exceto o último, representam os códigos dos produtos produzidos, estes códigos são de responsabilidade da empresa, e deve ser informado à GS1 BRASIL os códigos escolhidos com a respectiva correspondência com o produto produzido. O último dígito, como já sabemos, é o dígito de verificação.

---

[4]Uma tabela completa, com os números identificatórios de cada país, pode ser encontrada na página da *Internet* <http://www.gs1.org/barcodes/support/prefix_list>. Acesso em: 09 de Nov. 2009.

4.2.3 International Standard Serial Number - ISSN

O ISSN, cujo significado é International Standard Serial Number possui uma semelhança com o ISBN, mas a função do ISSN é identificar publicações seriadas. Diferente dos outros códigos de identificação, o ISSN não tem significação em si e não contém em si todas as informações referentes à origem ou conteúdo da publicação. Seu uso é definido pela norma técnica internacional da ISO 3297.

Segundo o Instituto Brasileiro de Informação em Ciência e Tecnologia – IBICT, órgão responsável pela operacionalização do ISSN no Brasil,

> O ISSN identifica o título de uma publicação seriada em circulação, futura (pré-publicação) e encerrada, em qualquer idioma ou suporte físico utilizado (impresso, online, CD-ROM etc). O ISSN é composto por oito dígitos, incluindo o dígito verificador, e é representado em dois grupos de quatro dígitos cada um, ligados por hífen, precedido sempre por um espaço e a sigla ISSN. Exemplo: ISSN 1018-4783. (IBICT, 2005)

Com base no ISSN Manual – Cataloguing part, deve-se proceder da forma descrita abaixo para calcular o dígito de verificação.

Primeiro distribui-se o número do ISSN sem o dígito de verificação, depois deve-se multiplicar os números da direita para a esquerda pela base {2,3,4,5,6,7,8}, feita a multiplicação, então deve-se somar os resultados obtidos e dividir por 11, em seguida, deve-se peguar o resto da divisão e subtrair por 11, o resultado encontrado é o digito de verificação. Vejamos:

Exemplo: ISSN 0317-8471

Devemos multiplicar o código do ISSN com a base na ordem descrita abaixo e posteriormente somar os resultados.

0 3 1 7 8 4 7 → Código do ISSN

8 7 6 5 4 3 2 → base

Soma (Código do ISSN × base) = 0 + 21 + 6 + 35 + 32 + 12 + 14 = 120

Dividindo o resultado por 11 teremos, por meio do algoritmo de Euclides:

$120 = 10\times11 + 10$, isto é, $120 \equiv 10 \pmod{11}$.

Logo, confirmamos que o digito de verificação é 1, pois 11 – 10 = 1.

No caso em que o resultado da subtração for 10 devemos substituir pela letra X. Vejamos um caso, o código abaixo foi retirado da revista Prazeres da Mesa:

Figura 4 – Código ISSN

Fonte: PRAZERES DA MESA. A bíblia da gastronomia. São Paulo: 4 capas, Ano 6, nº 69, Abr. 2009.

ISSN 1678-958X

1 6 7 8 9 5 8 → Código do ISSN sem o dígito de verificação

8 7 6 5 4 3 2 → base

Soma (Código do ISSN × base) = 8 + 42 + 42 + 40 + 36 + 15 + 16 = 199

Dividindo o resultado por 11, com o algoritmo de Euclides, teremos:

$199 = 18 \times 11 + 1$, isto é, $199 \equiv 1 \pmod{11}$.

Logo, o dígito de verificação é X, pois 11 – 1 = 10.

4.2.3.1 Adaptação ISSN/EAN-13

Com o advento da codificação em barras como ferramenta de automação na venda e gestão de mercadorias, fez-se um acordo entre ISSN International Centre e EAN, integrando o código ISSN na codificação EAN-13, onde identifica publicações periódicas em qualquer lugar do mundo. Para as publicações feitas no Brasil utiliza-se o prefixo 977, assim como no caso do ISBN que é identificado pelo prefixo 978.

De acordo com a GS1 BRASIL, (Antiga ABAC - Associação Brasileira de Automação Comercial) deve-se seguir os seguintes passos para encontrar o dígito de verificação:

Deve-se desconsiderar o último dígito (o verificador) do código ISSN, passando de 8 para 7 posições;

À esquerda do código deve-se aplicar o prefixo EAN-977, somando 10 posições;

À direita acrescenta-se mais dois dígitos[5], totalizando 12 posições;

Com base nos 12 dígitos deve-se calcular o verificador. Para isso, enumere da direita para a esquerda a seqüência de 3 e 1, depois multiplique o número do código com o número da base correspondente e some os resultados obtidos. O resultado final deverá ser subtraído por um múltiplo de 10 maior que ele, o resultado da subtração é o digito de verificação procurado. Se acaso o resultado da subtração for um múltiplo de 10 o dígito será 0 (zero).

Vejamos um exemplo, o código do ISSN abaixo foi retirado da revista Recreio, do ano 10 e nº 494:

Figura 5 – Código ISSN

Fonte: RECREIO. São Paulo: Abril, Ano 10, nº 494, 27 de Ago. 2009.

Devemos primeiro efetuar as multiplicações do código do ISSN/EAN-13 pela base especificada na ordem que segue, depois somar os resultados obtidos.

9 7 7 1 5 1 7 7 4 6 0 0 → Código do ISSN/EAN-13 sem o dígito de verificação

1 3 1 3 1 3 1 3 1 3 1 3 → base

[5] Veja em anexo as formas de uso dos 2 dígitos acrescidos ao ISSN.

Soma (Código de ISSN/EAN-13 × base) = 9+21+7+3+5+3+7+21+4+18+0+0 = 98

O múltiplo de 10 maior que 98 é 100, logo, 100 – 98 = 2, que é o digito de verificação procurado.

4.2.4 Cadastro de Pessoa Física – CPF

O CPF no Brasil é composto por 11 dígitos, agrupados em dois blocos, sendo o primeiro com 9 algarismos e o segundo com 2 algarismos, cujos são, assim como no ISBN, ISSN, códigos de barras, os dígitos de verificação, os quais são calculados através da aritmética modular. O CPF difere em um aspecto dos sistemas de identificação trabalhados até agora, pois ele possui dois dígitos de verificação, mas isso não implicará diferenças nos procedimentos de verificação.

Para efetuarmos os cálculos para encontrar o dígito de verificação, devemos seguir os passos descritos abaixo:

Se $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ é a seqüência 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, $S - a_{10} \equiv 0 \ (mod\ 11)$. Note que tal número será o próprio resto da divisão por 11 da soma obtida. A determinação do segundo dígito de verificação é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9.

Vejamos um exemplo de como devemos fazer para obter os dois dígitos de verificação que estão faltando do CPF 024 778 431.

Escrevemos os nove primeiros dígitos da seqüência e multiplicamos, na ordem especificada abaixo, pela base {1, 2, 3, 4, 5, 6, 7, 8, 9}.

0 2 4 7 7 8 4 3 1 → os noves primeiros dígitos do CPF

1   2   3   4   5   6   7   8   9 → base

Efetuando as multiplicações correspondentes e adicionando os resultados, teremos:

$0 \times 1 + 2 \times 2 + 4 \times 3 + 7 \times 4 + 7 \times 5 + 8 \times 6 + 4 \times 7 + 3 \times 8 + 1 \times 9 = 188.$

Dividindo o número 188 por 11, utilizando o algoritmo de Euclides, teremos:

$188 = 17 \times 11 + 1$ isto é, $188 \equiv 1 \pmod{11}$

Dessa forma, o primeiro dígito de verificação será o algarismo 1.

Agora acrescentamos o primeiro dígito de verificação do CPF, e desenvolvemos os mesmos cálculos, mas agora considerando a base {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, vejamos:

0   2   4   7   7   8   4   3   1   1 → dígitos do CPF acrescidos do primeiro dígito de controle

0   1   2   3   4   5   6   7   8   9 → base

Efetuando as multiplicações e adicionando os resultados, teremos:

$0 \times 0 + 2 \times 1 + 4 \times 2 + 7 \times 3 + 7 \times 4 + 8 \times 5 + 4 \times 6 + 3 \times 7 + 1 \times 8 + 1 \times 9 = 161.$

Dividindo o número 161 por 11, teremos:

$161 = 14 \times 11 + 7$ isto é, $161 \equiv 7 \pmod{11}$

Logo, o segundo dígito de verificação é o 7.

Concluímos então que, no nosso exemplo, o CPF completo seria: 024 778 431 17.

Se acaso o resto da divisão fosse 10, isto é, se o número obtido fosse congruente a 10 módulo 11, usaríamos o dígito zero.

De acordo com dados fornecidos pelo senado, os dois últimos dígitos do CPF, como já especificamos, são números de verificação: seguem um algoritmo de módulo 11, baseado no valor dos outros dígitos, para possibilitar a verificação automática e prevenir erros de digitação, dígito anterior (isto é, o terceiro dígito da direita para a esquerda) revela a unidade federativa em que a pessoa registrou-se pela primeira vez, dado que é proibido (em condições normais) trocar de número e os primeiros oito dígitos são números bases.

Assim, basta observar o dígito final antes do traço para descobrir sua origem.

Exemplo: CPF XXX.XXX.XX"6"-YY

O número destacado em aspas indica que a origem deste CPF é Minas Gerais, cujo código é 6. Vejamos a seguir os códigos que representam as regiões fiscais brasileiras.

A Região Fiscal onde emitido o CPF (definida pelo nono dígito) tem a seguinte abrangência: 0 - Rio Grande do Sul; 1 - Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul e Tocantins; 2 - Amazonas, Pará, Roraima, Amapá, Acre e Rondônia; 3 - Ceará, Maranhão e Piauí; 4 - Paraíba, Pernambuco, Alagoas e Rio Grande do Norte; 5 - Bahia e Sergipe; 6 - Minas Gerais; 7 - Rio de Janeiro e Espírito Santo; 8 - São Paulo; 9 - Paraná e Santa Catarina.

4.2.5 Cadastro Nacional de Pessoa Jurídica – CNPJ

O CNPJ é um número composto de 14 algarismos, o qual tem como finalidade identificar uma pessoa jurídica perante a Secretaria da Receita Federal do Brasil. Possui a mesma idéia do CPF, porém é utilizado para empresas.

O formato do número do CNPJ é o seguinte: 00.000.000/0000-00, onde os dois primeiros dígitos formam a raiz, identificando a empresa cadastrada; os próximos quatro dígitos compõem o sufixo, que especifica qual a unidade de atuação da empresa e os dois últimos dígitos, assim como no CPF, formam os dígitos de verificação que são estabelecidos a partir de relações aritméticas (congruência modular) com os dígitos anteriores.

O cálculo para encontrar o dígito de verificação do CNPJ é da seguinte forma: Se a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12} é a seqüência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base {6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9} e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{13} é o resto da divisão da soma obtida (S) por 11, isto é, $S \equiv a_{13} \pmod{11}$. A determinação do segundo dígito de verificação é feita de modo similar, sendo que agora acrescentamos o décimo terceiro dígito (que é o que acabamos de calcular) e usamos a seguinte base de multiplicação {5, 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9}.

No caso de CNPJ temos que fazer uma segunda verificação, a verificação do oitavo dígito, considerando a congruência modulo 10. Para isso devemos pegar os primeiros sete dígitos e multiplicá-los pela base {2, 1, 2, 1, 2, 1, 2}, o resultado das multiplicações deverá ser avaliado na base 9, por exemplo, se tivermos 14 como resultado, $14 \equiv 5 \pmod 9$, logo consideraremos o resultado 5, depois devemos somar os produtos obtidos. O digito de verificação que está faltando corresponde ao número que faltar para inteirar múltiplo de 10.

Veja, abaixo, um exemplo do cálculo do dígito de verificação módulo 11 (o mais usado pelos bancos) e do dígito de verificação módulo 10, que serve para a verificação do oitavo dígito em relação aos anteriores, para o CNPJ nº 18781203/0001:

Primeiramente devemos pegar a seqüência formada pelos 12 primeiros dígitos e multiplicá-los pela base {6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9} na ordem descrita abaixo:

1 8 7 8 1 2 0 3 0 0 0 1 → os 12 primeiros dígitos do CNPJ

6 7 8 9 2 3 4 5 6 7 8 9 → base

Efetuando as multiplicações e somando os resultados, teremos:

$6 + 56 + 56 + 72 + 2 + 6 + 0 + 15 + 0 + 0 + 0 + 9 = 222$

Dividindo o número 222 por 11, com o algoritmo de Euclides, teremos:

$222 = 20 \times 11 + 2$, isto é, $222 \equiv 2 \pmod{11}$

Logo, o primeiro dígito de verificação é o 2. Para calcularmos o segundo dígito devemos acrescentar o primeiro dígito obtido e seguir os mesmos passos, mas com a seguinte base {5, 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9}

Fazendo o somatório da multiplicação de cada algarismo, na ordem descrita abaixo, teremos:

1 8 7 8 1 2 0 3 0 0 0 1 2 → dígitos do CNPJ acrescidos do primeiro dígito de controle

5 6 7 8 9 2 3 4 5 6 7 8 9 → base

Efetuando as multiplicações e somando em seguida, temos:

$5 + 48 + 49 + 64 + 9 + 4 + 0 + 12 + 0 + 0 + 0 + 8 + 18 = 217$

Dividindo o número 217 por 11, com o algoritmo de Euclides, teremos:

$217 = 19 \times 11 + 8$ isto é, $217 \equiv 8 \pmod{11}$

Portanto, CNPJ completo é 18781203/0001-28

Conferência do oitavo dígito:

Devemos pegar os primeiros sete dígitos e multiplicá-los pela base {2, 1, 2, 1, 2, 1, 2} na ordem descrita abaixo:

1 8 7 8 1 2 0 → os primeiros 7 dígitos do CNPJ

2 1 2 1 2 1 2 → base

Somando os resultados das multiplicações dos algarismos correspondentes, temos:

$2+ 8 + 14 + 8 + 2+ 2 + 0$

Considerando estes resultados na base 9, teremos:

$2+ 8+ 5+ 8 + 2 + 2 + 0$, pois $14 \equiv 5 \pmod{9}$. O resultado da soma é 27, para 30 faltam 3, logo o oitavo dígito é o 3.

4.3 Criptografia

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 (detentor da "chave secreta"), 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 (Criptologia é o campo que engloba a Criptografia e a Criptoanálise[6]).

Podemos dizer que o uso da criptografia é tão antigo quanto à necessidade do homem em esconder a informação. Muitos pesquisadores atribuem o uso mais antigo da criptografia conhecido aos hieróglifos usados em monumentos do Antigo Egito (cerca de 4500 anos atrás). Diversas técnicas de ocultar mensagens foram utilizadas pelos gregos e romanos.

A criptografia pré-computacional era formada por um conjunto de métodos de substituição e transposição dos caracteres de uma mensagem que pudessem ser executados manualmente (ou até mesmo mentalmente) pelo emissor e pelo destinatário da mensagem. O surgimento de máquinas especializadas e, posteriormente, dos computadores ocasionou uma significativa evolução das técnicas criptográficas.

A era da criptografia moderna começa realmente com Claude Shannon [1948?], possivelmente o pai da criptografia matemática.

Atualmente a criptografia existente no mercado é bem mais sofisticada e segura, até mesmo para seguir o padrão de conhecimento da sociedade. Neste trabalho abordaremos a criptografia como mera exemplificação de aplicação da congruência modular, isto é, não aprofundaremos o assunto, a intenção é apenas entender sua importância para o desenvolvimento social e sua relação com o tema proposto.

Nos prenderemos a criptografia Clássica, onde o processo de encriptação e desencriptação baseava-se em substituição de posições das letras do alfabeto, como exemplo o Código de César.

4.3.1 Código de César

Em criptografia, a Cifra de César, também conhecida como cifra de troca ou ainda código de César, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição em que cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de 3 posições, A

[6] Criptoanálise é o ramo da criptologia que estuda formas de descodificar ou decifrar uma mensagem sem conhecer a chave secreta.

seria substituído por D, B viraria E e assim por diante. O nome do método teve origem numa técnica semelhante usada por Júlio César para se comunicar com os seus generais.

Códigos como o de Júlio César, onde basea-se em substituições de letras do alfabeto são muito fáceis de serem quebrados, isto é, de decifrar o conteúdo da mensagem, uma vez que basta analisar a frequência que determinada letra aparece, mas não é tão fácil assim para mensagens muito curtas, pois esta análise de frequência de letras pode induzir ao erro. O caso é que códigos como estes não podem ser usados para guardar informações importantes na nossa sociedade atual.

Júlio Cesar elaborou um esquema de enviar mensagens criptografadas para seus generais, através deste esquema, onde as letras eram trocadas pela terceira letra anterior no alfabeto. Desta forma, somente quem soubesse da regra conseguia desfazer o algoritmo e ler a mensagem original.

Veja como funcionava essa chave 3, de Julio César:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

A partir do esquema acima, temos que a letra A corresponde a X, a B corresponde a Y, assim sucessivamente até a letra Z que corresponde a W.

Ou seja, uma palavra simples como "ATACAR” seria codificada como "XQXZXO".

Você deve estar se perguntando: Mas onde está à relação com congruência modular? Vamos então á um exemplo mais completo que nos mostrará esta relação.

Considerando o esquema seguinte, usar a chave 4:

♡	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
14	15	16	17	18	19	20	21	22	23	24	25	26

Cada letra fica representada por um número que representa a sua posição no alfabeto. O espaço entre duas palavras será indicado pelo símbolo ♡, ao qual foi associado o número 0. Assim, para codificarmos uma mensagem teremos que somar com modulo 27 (pois no esquema temos uma seqüência com 27 elementos)

Com essa chave, ela fica substituída pela letra cujo número corresponde ao número original, aumentado de 4. Quando acontecer do resultado ser superior ao 26, voltamos ao início do alfabeto. Por exemplo, o número 28 corresponderá à letra A, pois $28 = 27 + 1$ e, como já sabemos $28 \equiv 1 \pmod{27}$.

Através da chave dada como no exemplo anterior (somar 4 ou $y = x + 4$), se a mensagem a ser enviada fosse CIDADE ♡ DE ♡ GOIÁS, o grupo emissor teria que criptografá-la como: G M H E H I D H I D K S M E W.

O grupo receptor da mensagem, sabendo que a chave foi "somar 4", teria agora que subtrair 4 unidades dos números que representam cada letra da mensagem criptografada, para obter a mensagem original, decifrando o código. Vejamos:

Mensagem codificada: G M H E H I D H I D K S M E W

Decodificando a mensagem: como a chave para codificação foi $y = x + 4$, então para decodificar deve-se aplicar o inverso da chave, isto é, $x = y – 4$. Fazendo os cálculos teremos: Para a primeira letra, no caso G, ela corresponde ao número 7, logo $7 – 4 = 3$, portanto a letra decodificada é C, a próxima letra é M, que é representada pelo número 13, dái $13 – 4 = 9$, o qual representa a letra I, continua-se com esse processo até obter a palavra decodificada.

Mensagem decodificada: C I D A D E ♡ D E ♡ G O I Á S.

5 A CONGRUÊNCIA MODULAR NO ENSINO MÉDIO

5.1 Por que ensinar Congruência Modular para alunos de Ensino médio?

Cada dia que passa os recursos tecnológicos vão se tornando mais comuns para as pessoas de todas as idades, principalmente para os mais jovens, talvez pela curiosidade de aprender o novo. Hoje em dia é normal ver crianças que mal sabem falar, manuseando máquinas como computadores, celulares, MP3, MP4, entre outros.

É correto supor que se sabem manusear é necessário também aprender o que está por trás de seu funcionamento; os riscos que podem correr utilizando algumas das vantagens destas novas tecnologias, como por exemplo, a internet.

Usa-se bastante a internet e nela, às vezes, colocam-se números de códigos de identificação como CPF, RG, CNPJ, ISBN, ISSN, códigos de barra, entre outros números de identificação para realizar algumas operações. Entretanto, na maioria das vezes não há uma compreensão de como os dados se manterão seguros e como são formados estes sistemas de identificação. Este é um assunto muito interessante e que deve ser trabalhado na educação básica. Todos os cidadãos possuem uma numeração que os identifica, assim como as empresas, os livros, revistas e todos os produtos que são comerciáveis. Sabemos que servem para identificar, mas como esses números são formados? Existe algum padrão? Como é possível identificar um produto, uma empresa e até pessoas com esses números? Estes códigos de identificação são passíveis de erros?

Estes questionamentos podem ser respondidos com o auxílio da Congruência Modular. Os sistemas de identificação como CPF, RG, CNPJ, ISBN, ISSN, códigos de barras, são mais um de suas inúmeras aplicações.

Outro item que usamos diariamente e que envolve conceitos da congruência modular é o relógio. Você já parou para pensar o mecanismo do relógio? Parece contar para sempre, embora conte para sempre nunca atinge quantidades grandes, mas tudo isso é tão familiar que muitas vezes passa despercebido. Por exemplo, cada vez que o número das horas chega aos 24, começa tudo de novo. Se forem 2 horas em ponto e aguardamos 24 horas, o relógio diz de novo 2 horas. Suponha agora que são 16 horas e que se quer saber que horas serão ao “adicionar” 10 horas, depressa deduz-se a resposta: 2 horas! Assim, do ponto de vista do relógio 16 + 10 = 2. Se por acaso um aluno fosse responder esta conta olhando pelo ponto de vista da Aritmética e não do relógio, certamente responderia 26 ao invés de 2. Como explicar este fato?

Nesse caso, foi utilizada a congruência modular, em particular o módulo é 24, ou seja, considera-se apenas o resto da divisão por esse número, logo 26 divido por 24 deixa resto 2, por isso o resultado 2 quando se está olhando sobre o ponto de vista do relógio.

Não é possível furtar-se de falar sobre mais um tópico que possui congruência modular em sua essência: a criptografia é uma de suas aplicações mais importantes, pois englobam vários aspectos deste mundo globalizado e com recursos altamente avançados. Inclusive os sistemas de identificação citados anteriormente são formas de criptografar informação, mesmo que seja indiretamente, pois por trás dos números existem várias especificidades do produto, empresa ou pessoa em questão.

Quase tudo que se almeje fazer hoje, é possível fazer através da internet. Desde estabelecer uma simples comunicação com alguém que está do outro lado do mundo até a compra de qualquer produto. Mas para que este sistema funcione sem prejudicar ninguém e mantenha as informações em sigilo é necessário que as mesmas sejam criptografadas. Assim, com a intervenção da criptografia cada vez mais nossa sociedade evolui, lembrando que esta evolução é no sentido de praticidade, rapidez com que se efetua algo, como por exemplo, fazer compras, fechar negócios, transmitir informações.

Existem vários estágios da Criptografia, a que será abordada aqui, é a criptografia simples de chave simétrica, é um exemplo mais adequado para alunos do Ensino médio e com ela se consegue trabalhar com mais uma aplicação de congruência modular.

É interessante deixar claro que esta criptografia simples não é muito usada na internet para proteger as informações por que são fáceis de serem quebradas. A criptografia que geralmente é utilizada para proteger essas informações é a Criptografia RSA[7], que se fortificam no tamanho dos números primos utilizados para criptografar uma mensagem, para quebrar tal mensagem criptografada com RSA é necessário fatorar o número que está protegendo a mensagem. E com números de mais de cem dígitos esta tarefa se torna muito difícil, e enquanto não se descobre como fatorar estes números muito extensos nossas informações ainda estão seguras.

---

[7] Ver criptografia RSA em: COUTINHO, Severino Colier. **Números Inteiros e Criptorafia RSA.** Série de Computação e Matemática. Instituto Nacional de Matemática Pura e Aplicada – IMPA. Rio de Janeiro, 2003.

Muitas vezes estes fatos são obscuros para os jovens que estão cursando o Ensino Básico. Eles lidam frequentemente com fenômenos periódicos, sistemas de identificação e criptografia, mas não os compreendem. Daí a necessidade de fazê-los conhecer esta outra Aritmética: a Aritmética Modular, focando o conceito de Congruência, pois é o conceito que se faz presente no cotidiano.

5.2 Como trabalhar com a Congruência Modular na sala de aula?

O desenvolvimento do trabalho foi feito com alunos do ensino médio. O principal objetivo foi relacionar conteúdos importantes da matemática com o cotidiano das pessoas, isto é, fazendo uma contextualização, apresentando apenas questões norteadoras para serem verificadas sem a preocupação de provas.

Esta pesquisa possui caráter qualitativo, não baseando em elementos numéricos, onde busca-se a melhor maneira de trabalhar a congruência modular a fim de conseguir fazer uma ligação entre conteúdo e realidade.

Para trabalhar qualquer conteúdo em qualquer nível escolar temos sempre que planejar, analisando os contra e os prós da execução do trabalho, com a congruência modular não é diferente.

O foco deste trabalho não é a congruência propriamente dita, mas sim suas aplicações em diversas áreas. Então o plano de atividades já tem que ser pensado numa contextualização. A questão é: como promover esta contextualização?

> A contextualização não pode ser feita de maneira ingênua, visto que ela será fundamental para as aprendizagens a serem realizadas – o professor precisa antecipar os conteúdos que são objetos de aprendizagem. Em outras palavras, a contextualização aparece não como uma forma de "ilustrar" o enunciado de um problema, mas como uma maneira de dar sentido ao conhecimento matemático na escola. (ORIENTAÇÕES CURRICULARES PARA O ENSINO MÉDIO, 2006, p.83)

Outro fator muito importante para o ensino e a aprendizagem dos alunos é promover atividades individuais e em grupo.

As Orientações Curriculares para o Ensino médio (2006), nos afirma que:

> As idéias socioconstrutivistas da aprendizagem partem do princípio de que a aprendizagem se realiza pela construção dos conceitos pelo próprio aluno, quando ele é colocado em situação de resolução de problemas. Essa idéia tem como premissa que a aprendizagem se realiza quando o aluno, ao confrontar suas concepções, constrói os conceitos pretendidos pelo professor. Dessa forma, caberia a este o papel de mediador, ou seja, de elemento gerador de situações que propiciem esse confronto de concepções, cabendo ao aluno o papel de construtor de seu próprio conhecimento matemático. (ORIENTAÇÕES CURRICULARES PARA O ENSINO MÉDIO, 2006, p.81)

Contudo, para atingirmos bons resultados é essencial buscar o aluno para a participação efetiva no desenvolvimento do trabalho, onde o mesmo terá contribuição desde o momento da escolha de ferramentas até o resultado da atividade.

Após a organização e análise dos dados, foi possível planejar e elaborar os procedimentos para o desenvolvimento da pesquisa.

Primeiramente acontecerá a construção do conceito de congruência em sala de aula por meio de um exemplo que necessitará de investigação e questionamentos por parte dos alunos. Após a familiarização do conteúdo, iniciaremos uma abordagem mais ampla com utilização de exemplos ainda no ambiente escolar, depois partiremos para a análise desse tema em situações do nosso cotidiano da seguinte forma:

Um tópico interessante dentro de aritmética modular que utiliza o conceito de congruência são os calendários e outros sistemas periódicos que vamos trabalhar mais em nível de curiosidade. Com os sistemas periódicos dentro da congruência poderemos descobrir quando determinado evento vai acontecer, qual o dia específico, por exemplo, que uma pessoa nasceu, ou qual o dia da semana que se deu o natal de 2000.

Pegar números de ISBN de alguns livros, CDs, monografias, entre outros e praticar o algoritmo de construção deste código de identificação para verificar se os resultados obtidos batem com os resultados fornecidos pelos livros, num outro momento executar este mesmo procedimento, mas sem a obra analisada a fim de descobrir a mesma. O mesmo será trabalhado com o ISSN

De modo semelhante analisar códigos de barras de diferentes produtos, destacando algumas diferenças nos cálculos utilizados para a verificação da origem do produto;

Agora numa situação um pouco mais particularizada, compreender a formação dos códigos de identificação em documentos, como CPF, percebendo o sentido de cada número e qual sua importância, isto é, o que é possível descobrir com a disposição desses números.

Ainda se tratando dos códigos de identificação trabalharemos com as técnicas de criptografia dentro de sala entre os próprios alunos com brincadeiras onde um aluno deverá mandar mensagem para outro sem que a mensagem seja lida por terceiros. Esse assunto, por ser mais complexo, exigirá um pouco mais de análise dos alunos e senso crítico, pois a criptografia é bastante utilizada em nosso meio mais no sentido de evitar fraudes, sendo então muito comum nas bases de dados de bancos e Internet que trabalham com informações pessoais importantes, que se usados por terceiros podem vir a causar grandes complicações. Sem contar que os métodos utilizados nos tópicos acima também se tratam de criptografar mensagens, pois atrás dos números existem informações sobre sua origem.

Com essa metodologia, espera-se que o ensino deixe de ser visto como transmissão de conhecimento e a aprendizagem como “mera recepção de conteúdo”, “acúmulo de conhecimentos”. E então o ensino-aprendizagem passe a ter um sentido intimamente voltado para a sistematização do novo conhecimento, onde o aluno tenha realmente uma aprendizagem significativa. Pois assim formarão pessoas preparadas para as situações problema enfrentadas diariamente, consciente de suas ações, de seus direitos e deveres, em especial, pessoas críticas e reflexivas.

5.3 Aplicação da pesquisa

A pesquisa foi aplicada na 3ª série “B” do Ensino médio do Colégio Estadual “Dom Cândido Penso”, sob o auxílio do Professor Alcino Tadeu dos Santos, no período noturno.

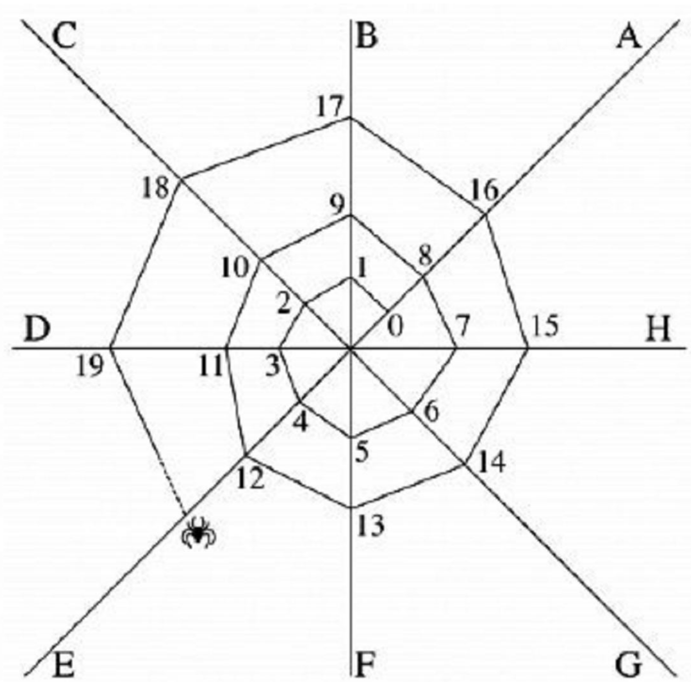
Há 53 alunos matriculados nesta sala, sendo que 40 desses alunos são freqüentes. A faixa etária dos alunos é de 20 a 30 anos. As dimensões da sala de aula são boas, mas mesmo assim se torna pequena para comportar uma grande quantidade de alunos, esta foi uma das dificuldades encontradas durante a aplicação do projeto. Foram necessárias cinco horas/aulas para aplicar o conteúdo proposto.

Os recursos utilizados durante a aplicação foram: Data show, quadro, giz, calendários, códigos de identificação de pessoas (CPF), de livros (ISBN), de revistas (ISSN), de produtos num geral (Códigos de Barra, especificamente EAN-13).

Primeiramente foi apresentado um exemplo (ver a seguir) para construirmos a idéia de aritmética modular, particularmente o conceito de congruência, depois trabalhamos com algumas propriedades de congruência. Nenhuma propriedade foi demonstrada, trabalhamos apenas casos particulares para percebemos a veracidade das propriedades, não convinha fazermos demonstrações por causa do tempo e pelo distanciamento do nosso foco: “As aplicações da Congruência Modular”.

Exemplo aplicado em sala

A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?



Fonte: Banco de Questões da OBMEP 2006, nível 2, 2ª lista.

Os alunos levantaram questionamentos importantíssimos que contribuíram para chegar à solução do exemplo e para a compreensão de congruência modular, como: que números estão sobre o fio A, B, C, D, E, F, G e H? Existe alguma semelhança entre eles? Quanto aumenta de um fio para o outro? Que relação podemos estabelecer em cada fio? É possível construir a teia até chegarmos ao fio desejado? E se fosse uma quantidade muito grande? Entre outros questionamentos que possibilitaram aos alunos chegar numa solução e formular uma regra básica para encontrar qualquer número solicitado, onde essa regra se fundamenta no conceito de congruência modular.

Depois que os alunos se familiarizaram com o conceito de congruência começamos a abordar suas aplicações. Primeiro trabalhamos com as aplicações de congruência nos sistemas periódicos como calendários, relógios, entre outros. Como atividade para esta questão utilizamos a periodicidade do calendário, pois é mais interessante e instiga mais a curiosidade do aluno e a determinação em participar da aula.

Na medida em que se aprofundava o conteúdo, principalmente as aplicações de aritmética modular, os alunos se mostravam mais interessados e maravilhados com o tema.

Um dos problemas propostos aos alunos em aula foi à identificação de erros nos códigos numéricos por meio da congruência modular. Esta atividade mostrou que eles necessitavam de mais conhecimentos de conceitos matemáticos.

Após o reforço sobre os conceitos matemáticos, retomamos o trabalho com as aplicações da congruência modular partindo para os códigos de identificação pessoal e comercial, como CPF, ISBN, ISSN e códigos de barras. Os alunos foram convidados a buscar esses códigos numéricos em objetos que eles possuíam para poderem compreender como interpretar os mesmos e sua importância no contexto social.

Um fato interessante que ocorreu quando iniciamos o trabalho com os sistemas de identificação, especificamente com o CPF, foi um levantamento de um aluno, “trabalhar com o nosso CPF é muito perigoso”, antes mesmo de ouvir a explicação da maneira que iríamos trabalhar, mas este levantamento serviu para mostrar que esta questão de segurança com os sistemas de identificação já não está tão afastada, as pessoas precisam apenas se informar mais para compreender como se processo e quais são as precauções que devermos ter à respeito destes sistemas de identificação. Este levantamento veio a calhar, pois a partir dele iniciou-se uma discussão que justificou ainda mais a relevância da aritmética modular em nossas vidas.

Foi proposto aos alunos um jogo, para fechar as aplicações de congruência modular, consistia em uma atividade em grupo sobre criptografia. Durante o jogo proposto os alunos estavam bastante eufóricos e se divertindo muito com a execução, se entusiasmaram com á técnica aprendida para criptografar/descriptografar mensagens.

Mesmo não tendo trabalhado com a teoria mais avançada da criptografia, como exemplo a criptografia RSA, dialogamos sobre sua importância sobre os sistemas de comunicação, principalmente na internet, pois é através da criptografia e de outros aparatos matemáticos que nossas informações estão asseguradas, isto se seguirmos as indicações de segurança, por isso é importante nos mantermos sempre bem informados. Esta criptografia possui a mesma essência da criptografia que trabalhamos, porém seu processo para descriptografar é muito mais complexo e exige equipamentos tecnológicos sofisticados, como computadores com programas específicos, e mesmo assim ainda é muito difícil alguém conseguir quebrar algum código.

5.4 Resultados alcançados

O objetivo mais relevante foi alcançado com o desenvolvimento das atividades, pois os alunos conseguiram perceber a presença da congruência na sociedade e em suas vidas e as facilidades que a mesma proporciona. Pode-se verificar isto com a aplicação de um questionário, onde foi proposto ao aluno que se manifestasse sobre a importância do assunto para sua formação e para a sociedade.

É possível perceber pelas falas[8] dos alunos que além de compreenderem, de fato, a importância das aplicações da aritmética modular, também aprenderam a desenvolver alguns algoritmos, usar as propriedades de congruência, verificar a validade dos códigos de identificação, entender o mecanismo utilizado para criptografar/descriptograr mensagens e a origem desses conceitos, por exemplo:

[8]Vide anexo A – Depoimento de alguns alunos que participaram da aplicação da pesquisa.

É interessante termos o conhecimento sobre congruência, pois através dela teremos consciência de como se processa vários mecanismos que utilizamos bastante em nossa vida, como CPF, ISBN, códigos de barra, criptografia.

A congruência é muito importante para nossa sociedade, principalmente nos dias atuais, com o avanço das tecnologias, servindo para diminuir as fraudes

Não só pra minha formação mais a congruência é fundamental para a sociedade onde ela analisa e codifica CPF, código de barras entre outros.

Desperta em modo geral, a curiosidade de entender o processo de funcionamento e aplicação das codificações, inclusive para identificar-mos.

O trabalho com as aplicações de congruência modular foi muito compensativo, pois notava-se nos alunos o entusiasmo ao descobrir os verdadeiros significados dos códigos numéricos, como exemplo, saber a unidade federativa que a pessoa registrou-se pela primeira vez por meio do número de CPF, informações de origem, de fabricação, especificidades de produtos diversos, além de certificar que determinado código é verdadeiro.

A idéia do trabalho e a forma proposta para desenvolver o mesmo cativaram os alunos e obteve vários resultados positivos, porém a grande quantidade de alunos tumultuou um pouco algumas atividades e alguns alunos não conseguiram desenvolver as atividades propostos em relação ao conceito de congruência, mas em relação às atividades voltadas para a aplicação da congruência todos tiveram uma boa participação e conseguiram desenvolver os problemas e enxergar os passos onde a congruência foi utilizada.

6 CONSIDERAÇÕES FINAIS

No início do projeto propusemos trabalhar com um tema prático que envolvesse conceitos da aritmética modular, pois é uma área fascinante e pouco divulgada para alunos da educação básica. Quando iniciamos a pesquisa para começar a desenvolver o trabalho nos surpreendemos com a variedade de aplicações contidas neste tema e com sua capacidade de cativar quem começa a estudá-la.

Fomos bastante felizes com o desenvolvimento deste. Pensar atividades desafiadoras e interessantes que promovem uma contextualização, permitindo o aluno vivenciar o que está sendo estudado, consequentemente, promovendo uma aprendizagem significativa, certamente acrescentou experiências importantíssimas que contribuirão para futuras atividades educativas.

Verificamos, por meio da aplicação, que trabalhar nos cenários para investigação realmente contribui com a melhoria do ensino, pois o aluno se torna participativo no processo de construção do conhecimento proporcionando uma assimilação e, por conseguinte, uma aprendizagem significativa.

Desenvolver este trabalho foi uma experiência sensacional, um grande desafio, até por que há poucos escritos que abordam este tema e poucas bibliografias acessíveis. Almejamos que esse trabalho sirva de alicerce para novas idéias que objetivem a melhoria da Educação Matemática.

Com a aplicação deste trabalho conseguimos alcançar nossos objetivos, principalmente apresentar para os alunos da educação básica, especificamente alunos do ensino médio, as aplicações da congruência modular no seu cotidiano, propondo uma metodologia interessante para se trabalhar congruência modular de forma simples e cativante, promovendo no leitor uma curiosidade de aprofundar neste tema e entender melhor os mecanismos que nos rodeiam nesta sociedade tecnológica e em constante evolução.

Dizem que não há glórias sem dificuldades, com este projeto tivemos esta certeza, pois conseguimos superar as expectativas depois de tantas vezes acreditarmos que não havia mais saídas e ao fim de todas essas dificuldades conseguimos propor uma maneira prazerosa de trabalhar a matemática na educação básica, com a aritmética modular.

REFERÊNCIAS

ALRO, Helle; SKOVSMOSE, Ole. **Diálogo e Aprendizagem em Educação Matemática**. Tradução de Orlando Figueiredo. Belo Horizonte: Autêntica, 2006.

ÁVILA, Geraldo. **O ensino de Matemática**. RPM 23. São Paulo: SBM, [2009]. 1 CD.

ÁVILA, Geraldo. **Os objetivos do Ensino de Matemátic**a. RPM 27. São Paulo: SBM, [2009]. 1 CD.

BRASIL. **Parâmetros Curriculares Nacionais** (PCN) para o ensino médio, Matemática. Brasília, DF: MEC/SEF, 1997.

BRASIL. **Parâmetros Curriculares Nacionais** (PCN) para o ensino médio, Matemática. Brasília, DF: MEC/SEF, 2000.

BRASIL. Ministério da educação. Secretaria de Educação Básica. **Orientações curriculares para o Ensino médio:** Ciências da natureza, matemática e suas tecnologias. Brasília, DF: MEC/SEF, 2008.

CAVALCANTE, A. L. B. **Teoria dos Números e Criptografia**. Revista Virtual, 2005, Disponível em: <http://www.upis.br/revistavirtual/Cavalcante_%20Teoria%20dos%20N%FAmeros%20e%2Criptografia_2005_UPIS.pdf>. Acesso em 14 de Jun. 2009.

COCUS, Mônica. **Você sabe realmente para que serve seu CPF?**. Secretaria de Recursos Humanos do Senado Federal. Jornal conversa pessoal. Disponível em:<http://www.senado.gov.br/sf/senado/portaldoservidor/jornal/jornal87/u. aspx>. Acesso em: 06 de Ago. 2009.

COUTINHO, Severino Colier. **Números Inteiros e Criptorafia RSA**. Instituto Nacional de Matemática Pura e Aplicada – IMPA. Rio de Janeiro: IMPA, 2003. (Série de Computação e Matemática).

DANTE, Luiz Roberto. **Restos, congruência e divisibilidade**. RPM 10. São Paulo: SBM, [2009]. 1 CD.

DOMINGUES, Hygino. **Fundamentos da Aritméica.** São Paula: Atual, 1991.

DRUCK, Suely. **A crise no Ensino de Matemática no Brasil**. RPM 53. São Paulo: SBM, [2009]. 1 CD.

D'AMBRÓSIO, Ubiratã. **Da realidade à ação**: reflexões sobre a educação e matemática. São Paulo: Ed. Da Universidade Estadual de Campinas, 1986.

D'AMBRÓSIO, Ubiratã. **Educação Matemática:** Da teoria à prática. 10 ed.Campinas, SP: Papirus, 2003 – (Perspectivas em Educação Matemática).

FERREIRA, William Alves. **A aplicação da matemática na criptografia para a transmissão de dados.** UNIMESP – Centro Universitário Metropolitano de São Paulo. Disponível em: <http://www.unimesp.edu.br/arquivos/mat/tcc06/Artigo_Willian_Alves_Ferreira.pdf>. Acesso em: 22 de Jun. 2008.

FREIRE, Benedito Tadeu Vasconcelos. **Congruências, Divisibilidades e Adivinhações**. RPM 22. São Paulo: SBM, [2009]. 1 CD.

GS1, The global language of business. Prefixo de Empresa GS1. Disponível em: <http://www.gs1.org/barcodes/support/prefix_list>. Acesso em: 09 de Nov. 2009.

HEFES, Abramo; VILLELA, Maria Lúcia T. **Códigos Corretores de Erros.** Instituto Nacional de Matemática Pura e Aplicada – IMPA. Rio de Janeiro: IMPA, 2008. (Série de Computação e Matemática).

IBICT, Instituto Brasileiro de Informação em Ciência e Tecnologia. **Centro brasileiro do ISSN.** Ministério da Ciência e Tecnologia. Disponível em: <www.ibict.br/secao.php?cat=issn>. Acesso em 05 de Jun. 2009.

ISSN, International centre. **ISSN Manual**. Disponível em: <www.issn.org/2-23364-issn-manual.php>. Acesso em: 06 de Jun. 2009.

LELLIS,Marcelo; IMENESES,Luiz Márcio. **A matemática e o novo ensino médio.** Disponível em: <http://www.somatematica.com.br/artigos/a4/p5.php>. Acesso em: 22 jun. 2008.

LINES, Malcom. **Pense num número**. Idéias, conceitos e problemas que desafiam a mente e deixam os especialistas perplexos. Tradução de José Luís Malaquias. Lisboa: Gradativa, 1993. (Aprender a fazer ciência).

LOPES, Alice Casimiro. **Os Parâmetros Curriculares nacionais para o ensino médio e a submissão ao mundo produtivo**: o caso do conceito de contextualização. Educ. Soc., set. 2002.

MARKARIAN, Roberto. **A matemática na escola. Alguns problemas e suas causas**. RPM 38. São Paulo: SBM, [2009]. 1 CD.

MELLO, José Luiz Patore. **Aritmética Modular e Sistemas de identificação**. RPM 48. São Paulo: SBM, [2009]. 1 CD.

MICOTTI, Maria Cecília de Oliveira. O Ensino e as Propostas Pedagógicas. In: **Pesquisa em educação matemática: concepções e perspectivas**. São Paulo: Editora UNESP, 1999 (Seminários e Debates).

MILIES, César Polcino. **A matemática dos códigos de barras**. RPM 65. São Paulo: SBM, [2009]. 1 CD.

MILIES, César Polcino. **A Matemática dos Códigos de Barras.** IME/USP - Departamento de Matemática, SP. Disponível em: <http://www.mat.ufg.br/bienal/2006/mini/polcino.pdf>. Acesso em: 22 de Jun. 2008.

MORGADO, Augusto César. **Em que dia cai?** RPM 24. São Paulo: SBM, [2009]. 1 CD.

MOYSÉS, Lúcia. **Aplicações de Vygotsky a educação matemática**. Campinas, SP: Papirus, 1997 – (Coleção Magistério: Formação e trabalho pedagógico)

PICADO, Jorge. **A algebra dos sistemas de identificação: da aritmética modular aos grupos diedrais**. Departamento de Matemática, Universidade de Coimbra. Disponível em: <http://www.mat.uc.pt/~picado/>. Acesso em: 22 de Jun. 2008.

POOLE, David. **Álgebra Linear.** Tradutoras técnicas Martha Salerno Monteiro (coord) [et. al.]. São Paulo: Thomson Learning, 2006.

PRAZERES DA MESA. A bíblia da gastronomia. São Paulo: 4 capas, Ano 6, nº 69, Abr. 2009.

RECREIO. São Paulo: Abril, Ano 10, nº 494, 27 de Ago. 2009.

SÁ, Ilydio Pereira de. **Aritmética Modular e Algumas de Suas Aplicações.** Disponível em: <http://magiadamatematica.com/wp-content/uploads/congruencia.pdf. Acesso em: 20 de Jun. 2008.

SÁ, Ilydio Pereira de. **Tratamento da Informação da Educação básica: aritmética modular e os códigos de identificação do cotidiano.** Disponível em: <www.sbem.com.br/files/ix_enem/.../MC26269805791T.rtf. Acesso em: 20 de Jun. 2008.

SHOR, Ira; FREIRE, Paulo. **Medo e Ousadia** – O Cotidiano do Professor. Tradução de Adriana Lopez. 8ª Ed. Rio de Janeiro: Paz e Terra, 1986. (coleção educação e comunicação, 18).

SKOVSMOSE, Ole. Matemática em Ação. In: BICUDO, Maria Aparecida Viggiani. **Educação Matemática: Pesquisa em Movimento**. São Paulo: Cortez, 2004, p.30-57.

SKOVSMOSE, Ole. **Educação crítica:** incerteza, matemática, responsabilidade. Tradução de Maria Aparecida Viggiani Bicudo. São Paulo: Cortez, 2007.

TERADA, Routo. **Criptografia e a importância de suas aplicações**. RPM 12. São Paulo: SBM, [2009]. 1 CD.

TAMAROZZI, Antônio Carlos. **Codificando e decifrando mensagens**. RPM 45. São Paulo: SBM, [2009]. 1 CD.

______________, **Tipos de códigos de barras**. Disponível em: <http://br.geocities.com/dadosvariaveis/tipos.html>. Acesso em: 09 de Jul. 2009.

VICKI, VOVÓ. **Aritmética Modular**. Disponível em:<http://www.numaboa.com/escolinha/matematica/171-modulo>. Acesso em: 04 de Abr. 2009.

VICKI, VOVÓ. **Introdução à Criptografia**. Disponível em:<http://www.numaboa.com/escolinha/matematica/171-criptografia>. Acesso em: 04 de Abr. 2009.

APÊNDICE

APÊNDICE A – PRODUTO ESCALAR

Apresentaremos aqui uma outra maneira de representar as operações envolvidas no cálculo do dígito verificador utilizando produto escalar.

Antes de apresentarmos um exemplo mostrando como poderíamos representar os algoritmos desenvolvidos no decorrer deste, vamos recordar o que é um produto escalar.

O produto escalar de $u = [u_1, u_2, u_3]$ e $v = [v_1, v_2, v_3]$ é o vetor $u \times v$ definido por

$$u \times v = [u_1 \times v_1 + u_2 \times v_2 + u_3 \times v_3]$$

Vamos considerar um exemplo dado no corpo do trabalho para apresentar esta outra forma de desenvolver o algoritmo que calcula o digito de verificação.

Na contracapa do livro Números Inteiros e Criptografia RSA, da Série de Computação e Matemática, do IMPA, têm o seguinte código do ISBN: 85-24401-24-9. Vejamos o cálculo do dígito de verificação que, como estamos observando, é igual a 9.

Chamemos de *b* o vetor que compõe o código do ISBN menos o digito de verificação, isto é, *b* = [8, 5, 2, 4, 4, 0, 1, 2, 4]. O vetor de checagem é o vetor c = [10, 9, 8, 7, 6, 5, 4, 3, 2]. A condição é que $(c \times b) + d \equiv 0 \pmod{11}$, onde *d* é o digito de verificação.

Fazendo o produto escalar, temos:

$$c \times b = 10 \times 8 + 9 \times 5 + 8 \times 2 + 7 \times 4 + 6 \times 4 + 5 \times 0 + 4 \times 1 + 3 \times 2 + 2 \times 4$$
$$c \times b = 80 + 45 + 16 + 28 + 24 + 0 + 4 + 6 + 8$$
$$c \times b = 211$$

Agora basta analisar o valor de *d*, ou seja, verificar qual número deve substituir o *d* para que o produto escalar acrescido de *d* seja congruente a zero módulo 11.

Dividindo o resultado por 11 teremos:

211 = 19×11 + 2

Para obtermos um múltiplo de 11, devemos subtrair o quociente da divisão acima pelo resto obtido, isto é, 11 – 2 = 9. O que confere o valor apresentado no código dado. Isso significa dizer que 211 + 9 = 220 é um múltiplo de 11, ou ainda, que $211 + 9 \equiv 0 \pmod{11}$.

ANEXOS

ANEXO A – DEPOIMENTOS DOS ALUNOS

Abaixo segue alguns depoimentos de alunos que participaram da aplicação da pesquisa.

É interessante termos o conhecimento sobre congruência, pois através dela teremos consciência de como se processa vários mecanismos que utilizamos bastante em nossa vida, como CPF, ISBN, códigos de barra, criptografia.

A congruência é muito importante para nossa sociedade, principalmente nos dias atuais, com o avanço das tecnologias, servindo para diminuir as fraudes.

Não só pra minha formação mais a congruencia é fundamental para a sociedade onde era analizar e codificar CPF codigo de barras entre outros.

Desperta em modo geral, a curiosidade de entender o processo de funcionamento e aplicação das codificações, inclusive para identificações.

ANEXO B - FORMAS DE USO DOS DOIS DÍGITOS ACRESCIDOS AO ISSN

ENCARTE TÉCNICO

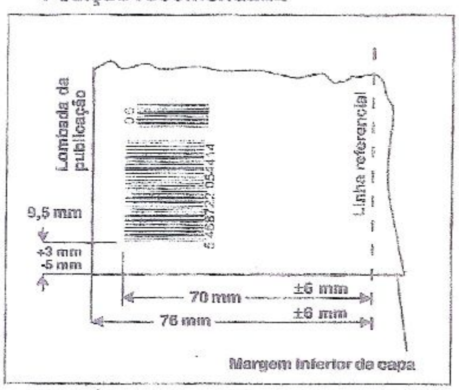
Nº 8 - FEV/94

Codificação de publicações periódicas

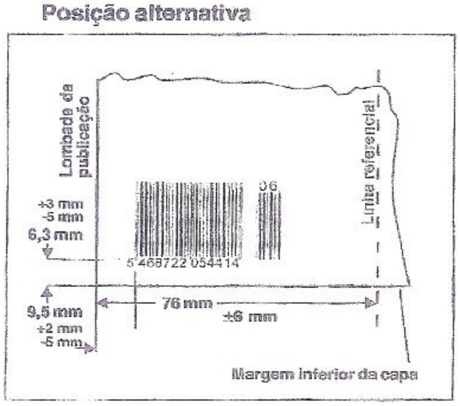
Localização do símbolo

Para que haja critérios ainda mais claros para a aplicação do ISSN/EAN-13, demonstramos abaixo as diretrizes voluntárias de localização do símbolo no periódico.

Posição recomendada



Posição alternativa



Formas de uso dos 2 dígitos acrescidos ao ISSN

A utilização destas duas posições no ISSN/EAN-13 podem ser variáveis dependendo da periodicidade da publicação.

Diários: as publicações de cada dia devem ser diferenciadas; portanto utiliza-se as duas posições da seguinte maneira:

01 - Domingo
02 - 2ª feira
03 - 3ª feira
04 - 4ª feira
05 - 5ª feira
06 - 6ª feira
07 - Sábado

A primeira posição destes dois dígitos pode ser modificada caso haja mudança de preço da publicação.

Semanários: 01 ao 53, significando o número de semana do ano.

Quinzenais: aplica-se alternadamente os números das semanas do ano.

02, 04, 06 ... 52
ou
01, 03, 05 ... 53

Mensais: identifica-se o número do mês do ano.

01 ao 12

Bimestrais: alterna-se os números do meses do ano

02, 04, 06 ... 12
ou
01, 03, 05 ... 11

Trimestrais: a mesma regra que para as publicações bimestrais.

Período pelas Estações do Ano:

- 1ª posição traz o último número do ano correspondente;
- 2ª posição traz o nº correspondente à estação do ano.

1 = Primavera 2 = Verão 3 = Outono 4 = Inverno

Período abrangendo duas Estações:

- 1ª posição traz o último número do ano correspondente;
- 2ª posição traz o nº correspondente à primeira estação das duas em questão.

Anual: - 1ª posição traz o último número do ano correspondente;
- 2ª posição traz sempre o número 5 (fixo).

Intervalos especiais: identificado por um nº de 01 a 99.

EAN Brasil
Alameda Santos, 2.441, 9º andar
CEP 01409-002 – São Paulo – SP
Tel.: (011) 3064-8772 Fax: (011) 3064-0821
Tel.: 0800-110789
E-mail: ean@eanbrasil.org.br
Site na Internet: http://www.eanbrasil.org.br

ANEXO C – PLANO DE AULA DA APLICAÇÃO DA PESQUISA

Plano de aula

Aplicação do Projeto de Monografia sobre **"Apresentação de Congruência Modular no Ensino Médio por meio da Aritmética"**

Escola: Col. Est. "Dom Cândido Penso" Duração: 4 aulas de 50 minutos

Data: 15-19/06/2009 Professor (a): Jackelyne de Souza Medrado

Série: 3º série EM

Objetivos

Geral:

Apresentar noções básicas e conceitos da Aritmética Modular, especificamente a congruência e mostrar onde lidamos com ela e em que facilita nas atividades em nosso dia-a-dia.

Específico:

- Entender o conceito de congruência;
- Verificar o processo de formação dos diferentes códigos numéricos de identificação;
- Identificar os algoritmos utilizados para obtenção dos resultados;
- Relacionar a Aritmética Modular com o cotidiano;

- Listar exemplos de situações que necessitam da Aritmética Modular;
- Perceber a importância da Aritmética Modular para o funcionamento da sociedade nesta era tecnológica;

Conteúdo

Congruência Modular presente nos códigos de identificação, nos fenômenos periódicos e na criptografia.

Metodologia

Aula investigativa, onde os alunos desenvolverão o conceito de Congruência Modular. Aula expositiva e lúdica com algumas aplicações de congruência modular.

Desenvolvimento

No primeiro momento será exposto um problema para os alunos analisarem e investigarem a fim de estabelecer algumas características especiais deste problema para chegarem ao conceito de congruência modular. Após esta investigação, formalizaremos o conceito de congruência e algumas de suas propriedades.

Depois que os alunos se familiarizarem com o conceito de congruência modular iniciaremos a abordagem de suas aplicações. Primeiro trabalharemos com as aplicações de congruência modular nos sistemas periódicos como calendários, relógios, entre outros. Como atividade para esta questão utilizaremos a periodicidade do calendário, onde os alunos aprenderão como encontrar o dia de determinada data sem ter um calendário em mãos, apenas utilizando a congruência modular.

Posteriormente trabalharemos com o CPF, onde os alunos deverão trazer seus números de CPF para trabalharmos com a aplicação da congruência. (Obs.: cada aluno trabalhará somente com seus números de documento para evitarmos maiores constrangimentos futuros, já que estamos atentados à questão de segurança dos sistemas de identificação.).

Logo em seguida iremos para a biblioteca da escola para os alunos escolherem alguns livros e revistas para retirarmos os números de ISBN e ISSN, respectivamente, e compreender como são formados, saber como é utilizada a congruência modular para sua fabricação.

Como a intenção é aplicação da congruência, novamente será proposto aos alunos que tragam algum objeto que possua código de barra para desenvolvermos estudos a respeito do mesmo e novamente entender o emprego da congruência modular. (lembrando que estes códigos de barra serão da forma EAN-13).

Por fim, formaremos alguns grupos na sala para desenvolver o jogo “cuidado com o espião”, onde estes grupos deverão mandar mensagens sigilosas para determinado grupo, para isso utilizarão a criptografia. Durante este processo o grupo deverá criptografar uma mensagem usando a criptografia simétrica, isto é, onde o remetente e o destinatário devem saber da chave utilizada, e depois o grupo receptor deverá tentar descriptografar a mensagem para compreender a mensagem original. Em todos os passos de criptografar e descriptografar, estaremos trabalhando com a congruência modular.

Recursos Didáticos

Calendários, CPF, revistas (ISSN), livros (ISBN), produtos com códigos de barra EAN-13, papel para recados, computador, data show, quadro e giz.

Avaliação

A avaliação será contínua, onde observarei se os objetivos estão sendo alcançados, principalmente se os alunos estão compreendendo a importância da Congruência Modular e sua relevância para a nossa sociedade.

Referências

JURKIEWICZ, Samuel. **Divisibilidade e Números Inteiros: Introdução à Aritmética Modular**. Disponível em <www.obmep.org.br>. Acesso em: 01 de Jun 2009.

LINES, Malcom. **Pense num número**. Idéias, conceitos e problemas que desafiam a mente e deixam os especialistas perplexos. Lisboa: Gradativa. 1993.

S. C. Coutinho. Números Inteiros e Criptografia RSA. 2.ed. Rio de Janeiro: IMPA, 2003.

SÁ, Ilydio Pereira de. **Tratamento da Informação na Educação Básica: Aritmética Modular e os Códigos de Identificação do Cotidiano.** Disponível em www.sbem.com.br/files/ix_enem/Minicurso/Trabalhos/MC26269805791T.rtf -. Acesso em: 01 de Jun 2009.

Anexos:

Atividades sobre as aplicações de Congruência Modular

1. Considerando o dia de hoje (quarta-feira, 17 de junho de 2009), sem utilizar o calendário, imagine que você queira saber em que dia da semana será o dia das crianças (12 de Outubro), como procederemos para encontrá-lo?

2. Escolha um livro qualquer, coloque informações sobre o mesmo (título do livro, autor, editora, entre outros), depois desenvolva o método para encontrar o dígito de controle do ISBN através da congruência.

3. Desenvolva o mesmo processo do exercício anterior utilizando uma revista e um produto que contenha um código de barra (lembrando que agora devemos considerar o ISSN no caso da revista).

Atividade em grupo

Jogo: "Cuidado com o espião"

Regras do Jogo: Forme 6 grupos, onde os grupo seguirão a seguinte correspondência (pode estabelecer outra correspondência se achar necessário):

1↔3 4↔6 2↔5

Ou seja, o grupo 1 irá criptografar um mensagem e enviar para o grupo 3 para descriptografá-la, o grupo 3 também irá criptografar um mensagem e deverá enviar para o grupo 1, onde os dois já terão comunicado a chave que irão utilizar, e assim sucessivamente.

Durante o envio da mensagem ela poderá ser extraviada e assim cair nas mãos de grupos errado, os quais tentarão decifrar a mensagem, se acaso conseguir quebrar o código antes que a mensagem chegue ao seu destino, o grupo que criptografou a mensagem perderá o jogo.

Todos os grupos se orientarão na tabela abaixo para criptografar sua mensagem, variando apenas a chave para criptografar e descriptografar a mensagem.

Note que o módulo adotado neste esquema é 27 (existem 27 elementos), isto é, utilizarão congruência com respeito ao modulo 27 para criptografar e descriptografar.

♡	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
14	15	16	17	18	19	20	21	22	23	24	25	26

De acordo com as regras do jogo descritas acima, especifique o número do seu grupo, coloque a mensagem que vocês irão criptografar e então criptografe-a para enviar para seu grupo correspondente. Depois que você receber a mensagem criptografada do outro grupo, já com posse da chave, descriptografe e escreva ela abaixo.

ANEXO D – QUESTIONÁRIO

Colégio Estadual “Dom Cândido Penso”

Projeto de Monografia: **“Apresentação de Congruência Modular no Ensino Médio por meio da Aritmética”.**

Acadêmica: Jackelyne de Souza Medrado / UEG-UNUCC.

Aruanã, ____ de ___________ de 2009.

Aluno (a): ____.

Questionário

Este questionário tem por objetivo avaliar a aplicação do projeto de Monografia: “Apresentação de Congruência Modular no Ensino Médio por meio da Aritmética”

1. Em sua vida escolar você já tinha estudado congruência modular?

   ____

2. Escreva umas poucas linhas sobre o assunto (Congruência)? Liste algumas aplicações usuais. Você já havia analisado este problema sobre este ângulo?

   ____

   ____

   ____

3. Como você classifica a idéia do projeto?

   ( )Ótima ( )Boa ( )Regular ( )Ruim

4. Diga algo sobre a importância do assunto para a sua formação. E para a sociedade.

   ____

   ____

5. O tempo e os recursos disponibilizados foram suficientes?

   ____

ANEXO E – FOTOS DA APLICAÇÃO DA PESQUISA