UNIVERSIDADE ESTADUAL DO CEARÁ – UECE

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA – PRPGPq

CENTRO DE CIÊNCIAS E TECNOLOGIA – CCT

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

RAFAEL NOGUEIRA DE MOURA

CONGRUÊNCIAS MODULARES E ALGUMAS APLICAÇÕES PARA A EDUCAÇÃO BÁSICA

FORTALEZA – CEARÁ
2015

RAFAEL NOGUEIRA DE MOURA

CONGRUÊNCIAS MODULARES E ALGUMAS APLICAÇÕES PARA A EDUCAÇÃO BÁSICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Orientador: Prof. Dr. João Montenegro de Miranda

FORTALEZA – CEARÁ
2015

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Moura, Rafael Nogueira de.
Congruências modulares e algumas aplicações para a educação básica [recurso eletrônico] / Rafael Nogueira de Moura. – 2015.
1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 55 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) – Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2015.
Área de concentração: Matemática.
Orientação: Prof. Dr. João Montenegro de Miranda.

1. Congruência. 2. Critérios de divisibilidades. 3. Dígito de verificação. 4. Criptografia. I. Título.

RAFAEL NOGUEIRA DE MOURA

CONGRUÊNCIAS MODULARES E ALGUMAS APLICAÇÕES PARA A EDUCAÇÃO BÁSICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Aprovada em: 26 de agosto de 2015.

AVALIAÇÃO

Prof. Dr. João Montenegro de Miranda

(Orientador)

Universidade Estadual do Ceará – UECE

Prof. Dr. João Marques Pereira

Universidade Estadual do Ceará – UECE

Prof. Dr. José Robério Rogério

Universidade Federal do Ceará – UFC

Aos meus pais, José Jaime (*in memoriam*) e Regina Elizabeth que desde criança me ensinaram os valores da educação e que trilharam meu caminho me fazendo crescer pessoalmente, quanto profissionalmente.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dada essa oportunidade de realizar mais um sonho e por me dar forças nessa trajetória para alcançar mais essa vitória.

À minha esposa Alexsandra, pelo apoio e compreensão durante esse período de pouco mais de dois anos em que dediquei a fundo a esse projeto, me privando de momentos que poderia estar ao seu lado.

À minha família pelo amor e incentivo aos estudos. Em especial, meus pais José Jaime (*in memoriam*) e Regina Elizabeth e minhas irmãs Andréa e Valéria que sempre apoiaram e vibraram com as minhas conquistas, sendo um verdadeiro combustível para a realização desse sonho.

Ao meu professor e orientador Prof. Dr. João Montenegro, que me ensinou muito durante o curso e que esteve sempre me acompanhando no desenvolvimento desse trabalho, apesar do seu tempo corrido, esteve sempre presente com as devidas correções que engrandeceram o trabalho.

A todos os professores e coordenador do PROFMAT na UECE, pela dedicação e entusiasmo durante as disciplinas ministradas.

Aos meus colegas de mestrado na UECE, que sempre estiveram juntos auxiliando com trocas de informações e principalmente nos momentos de angustia, dano forças para continuar.

Ao programa PROFMAT, pela a oportunidade concedida aos professores para crescimento no ensino da matemática.

A CAPES, pelo incentivo financeiro, essencial para o desenvolvimento dos nossos estudos.

"O propósito dos modelos matemáticos não é
acomodar os dados, mas aperfeiçoar as perguntas."
(Samuel Karlin)

RESUMO

Este trabalho pretende mostrar que a congruência modular é um tema de grande aplicabilidade e presente no cotidiano, podendo ser introduzido no ensino básico, por meio de aplicações que causem interesse como, os critérios de divisibilidade, o dígito de verificação, a criptografia e as resoluções de problemas. Faz-se uma fundamentação teórica sobre a teoria dos números, especificamente, divisibilidade, divisão Euclidiana e números primos, para ser feita a introdução do assunto principal do trabalho que é congruência modular. As aplicações apresentadas servirão como propostas motivadoras para que os professores tenham como apoio metodológico no ensino da matemática assuntos da atualidade. O intuito principal, é que o leitor perceba que congruência modular é uma ferramenta que traz agilidade e simplicidade nas resoluções de problemas e além do mais está presente no seu cotidiano de uma forma simples de ser compreendida. Para facilitar o aprendizado, a teoria apresentada é sempre acompanhada de exemplos e resoluções de problemas.

Palavras chave: Congruência. Critérios de divisibilidade. Dígito de verificação. Criptografia.

ABSTRACT

This work aims to show that the modular congruence is a topic of great applicability and present in daily life and can be introduced in primary education, through applications that cause interest as the divisibility criteria, the check digit, encryption and resolutions problems. It makes up a theoretical foundation on the theory of numbers, specifically, divisibility, Euclidean division and prime numbers to be made to introduce the main subject of the work that is modular congruence. The submitted applications will serve as motivating proposals for teachers to have as methodological support in math current affairs education. The main objective is that the reader realize that modular congruence is a tool that brings speed and simplicity in problem solving and what's more is present in their daily lives in a simple to understand. To facilitate learning, the theory presented is always accompanied by examples and troubleshooting.

Keywords: Congruence. Divisibility’s Criteria. Check Digit. Encryption.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Neste trabalho apresentaremos alguns tópicos da Teoria dos Números, tais como divisibilidade, divisão euclidiana, congruência modular e algumas aplicações sobre congruências modulares. Abordaremos critérios de divisibilidade, digito de verificação e criptografias com uso de chaves públicas.

Ao fazer uma revisão bibliográfica encontramos vários trabalhos relacionados com o tema. Barbosa Junior (2013) faz uma explanação bem estruturada sobre conceitos básicos à teoria dos números, como divisibilidade, divisão euclidiana, máximo divisor comum, mínimo múltiplo comum, análise de restos e congruência modular, com aplicações: Teorema chinês do restos e Partilha de senhas. Seu objetivo apresentar congruência modular aos alunos do ensino básico.

O trabalho realizado por Santos (2013), traz uma preocupação com o rendimento apresentado pelos alunos de escolas públicas que participam da OBMEP, através de dados extraídos pelo próprio site da instituição, mostra um baixo índice de aproveitamento. Com essa preocupação, é feito toda uma sequência didática, para poder ser apresentado o conteúdo de congruência modular e equações diofantinas lineares, com atenção especial para divisão euclidiana, a fim de dotar o estudante da capacidade de resolver problemas de repetições periódicas de eventos.

Sant'Anna (2013) traz essa abordagem de divisibilidade, com mais ênfase e preocupação com as demonstrações desses critérios, através da aritmética modular, com intuito de gerar no aluno, um novo olhar investigativo, não ficando preso apenas ao que o professor repassa.

Esquinca (2013) traz uma preocupação no desenvolvimento dos professores de matemática em suas aulas para o ensino básico. Com o intuito de melhorar as aulas, são apresentadas algumas aplicações de congruência modular no dia-a-dia, com foco principal sobre o código de barras e a aritmética modular que está presente.

Uma das aplicações de congruência bastante interessante na atualidade é sobre a criptografia. No trabalho de Marques (2013) é apresentada a evolução da criptografia até os dias atuais e toda a matemática que aparece por trás. Uma das criptografias bastante interessante é a troca de chaves de Diffie-Hellman que utiliza a congruência modular no processo.

O tema congruência modular e suas aplicações é assunto bem interessante e com bastante utilidade, daí o interesse em aprofundar a pesquisa na área das aplicações que causam interesse aos leitores.

Ao me deparar com o conteúdo de congruências modulares nas disciplinas ministradas no mestrado, despertou-me um grande interesse, pelo fato de nunca ter tido contado e também pelo fato da facilidade de compreender o tema, antes nunca visto. Daí sempre ficava me questionando porque este assunto não era visto nas turmas de ensino básico.

Devido a sua grande aplicabilidade e facilidade de compreensão gerou um interesse em levar esse conteúdo para ser trabalhado nas turmas de ensino básico, com o enfoque nas resoluções de alguns problemas. O objetivo principal deste trabalho é de levar através de conceitos e aplicações simples o entendimento de congruências modulares e como se torna prático o seu uso nas resoluções de algumas situações problemas, onde seria quase impossível de ser resolvido sem tal conhecimento.

Tendo também o intuito nesse trabalho de melhorar o nível de aprendizado em matemática dos alunos no âmbito de problemas que envolvam repetição periódica, divisão e contas com restos, através de aplicações que criem curiosidades ao aluno.

Encontramos sempre relatos de professores e de alunos que sentem dificuldade com a operação da divisão, e de problemas onde o uso dela é necessário. Será que através de aplicações que chamem a atenção do aluno, ele irá ter mais vontade de aprender e querer entender o significado? É com essa perspectiva, que procuramos uma melhora no ensino de matemática na educação básica.

É através dessas dificuldades de aprendizado, que me interessei pelo tema de congruência modular e suas aplicações, pois congruência é uma relação presente na divisão, que pode facilitar no entendimento e nas resoluções de problemas que envolvam divisão de uma maneira mais fácil de ser compreendida.

Demonstraremos critérios de divisibilidade, que muitas vezes são apenas repassados aos alunos sem que eles tenham conhecimento, gerando uma serie de perguntas: por que vale aquele critério, de onde veio e se existe para outros números. Com demonstrações simples, verá que é possível formular outros critérios.

A criptografia é um assunto importante e interessante no contexto atual, onde vivemos cercados de tecnologia e informações. Acreditando que seu uso em sala de aula possa ser um fator que motive os alunos. Com a inserção da criptografia associaremos conteúdos de matemática, fazendo o aluno ter uma motivação no momento de aprender ou aplicar tal conteúdo.

O objetivo geral é apresentar métodos mais prazerosos e inovadores de serem trabalhados no ensino da matemática no ensino básico, para que desperte o interesse dos estudantes, principalmente na parte da divisão, operação que sentem mais dificuldade. No primeiro capítulo através de uma pesquisa bibliográfica, faz-se uma revisão da Teoria dos Números com finalidade de identificar conteúdos como, divisibilidade e as suas propriedades, com uma preocupação para as demonstrações de uma maneira clara, sempre apoiada em exemplos, para facilitar a compreensão, seguida da divisão euclidiana e sua importância nas resoluções de problemas apresentados e concluindo o primeiro capítulo com números primos.

No segundo capítulo apresenta-se a definição e as propriedades da congruência modular, com o uso de questões problemas para podermos fazer a comprovação da utilidade desse conteúdo para resoluções de determinados problemas. No último capítulo apresentaremos as aplicações da congruência modular. Iremos descrever processos que irão tornar o processo de ensino aprendizagem mais encantador e motivador, pois estarão diante de assuntos da atualidade e presentes no cotidiano.

2 DIVISIBILIDADE

Neste capítulo estudaremos divisibilidade nos números naturais e suas propriedades. Apresentaremos o algoritmo de Euclides, a importância do resto e os números primos.

Definição: Dados dois números naturais a e b, com $a \neq 0$, a divide b, quando existe um número natural q, de tal modo que $b = a \cdot q$. Neste caso diz-se também que a é um divisor de b e que b é um múltiplo de a. Ou ainda que b é divisível por a. Indicamos por $a|b$ o fato que a divide b.

Quando a não divide b, escrevemos $a \nmid b$, que significa que não existe nenhum número natural q, de tal modo que $b = a \cdot q$.

Por exemplo: $7|28$ pois $28 = 7 \cdot 4$;

$1|a$ pois $a = 1 \cdot a$;

$a|0$ pois $0 = a \cdot 0$;

$a|a$ pois $a = a \cdot 1$, para todo a natural.

2.1 PROPRIEDADES DA DIVISIBILIDADE

Considerando os números naturais a, b e c, com $a \neq 0$, temos:

i) Se $a|b$ e $b|c$, então $a|c$;

ii) Se $a|b$ e $a|c$, então $a|(b + c)$; e se $b \geq c$, então $a|(b - c)$

Demonstração:

i) Se $a|b$ então, existe um número natural q, de tal modo que $b = a \cdot q$. Se $b|c$ então, existe um número natural p, de tal modo que $c = b \cdot p$. Substituindo o valor de b da primeira igualdade na segunda igualdade, obtemos:

$$c = b \cdot p = (a \cdot q) \cdot p = a \cdot (q \cdot p).$$

Logo $a|c$. ■

ii) Se $a|b$ então, existe um número natural q, de tal modo que $b = a \cdot q$. Se $a|c$ então, existe um número natural p, de tal modo que $c = a \cdot p$. Somando as duas igualdades, temos que:

$$b \pm c = (a \cdot q) \pm (a \cdot p) = a \cdot (q \pm p).$$

Logo $a|(b \pm c)$. ■

iii) Sejam a, b, c e d números naturais, com $a \neq 0$ e $c \neq 0$, então se $a|b$ e $c|d \Longrightarrow a \cdot c|b \cdot d$;

Demonstração:

iii) Se $a|b$ então, existe um número natural q, de tal modo que $b = a \cdot q$ e da mesma forma se $c|d$ então, existe um número natural p, de tal modo que $d = c \cdot p$. Temos, que:

$$b \cdot d = (a \cdot q) \cdot (c \cdot p) = (a \cdot c) \cdot (q \cdot p).$$

Logo $a \cdot c|q \cdot p$. ■

iv) Sejam a, b e c números naturais, com $a \neq 0$, tais que $a|(b + c)$, então $a|b \Leftrightarrow a|c$; e se $b \geq c$ tal que $a|(b – c)$, então $a|b \Leftrightarrow a|c$;

v) Sejam a e b números naturais diferentes de zero, temos que, se $a|b$, então $b \geq a$;

Demonstração:

iv) Se $a|b$ então, existe um número natural q, de tal modo que $b = a \cdot q$ e como a e b são ambos diferentes de zero, temos que $q \geq 1$, segue-se que $a \leq a \cdot q = b$, o que implica $a \leq b$ ou $b \geq a$. ■

Exemplo 2.1.1: O número $21 \cdot 10^3$ é divisível por 6?

Solução: Note que $21 \cdot 10^3 = (3 \cdot 7) \cdot (2^3 \cdot 5^3) = 3 \cdot 2 \cdot (7 \cdot 2^2 \cdot 5^3) = 6 \cdot 350$.

Portanto 6 divide $21 \cdot 10^3$.

2.2 EUCLIDES

O grande matemático Euclides, conhecido também como Euclides de Alexandria, terra para onde foi chamado para ensinar matemática. Euclides nasceu por volta de 330 a.c, durante essa época foi o autor do texto de matemática mais bem sucedido de todos os tempos, esta obra recebeu o nome de *Os Elementos* (em grego, *Stoichia*).

Figura 1 – Representação artística de Euclides.

Fonte: Wikipédia (2015)

Os Elementos estão divididos em treze livros, dos quais os seis primeiros são sobre geometria, os três seguintes sobre teoria dos números, o décimo sobre os números incomensuráveis e os três últimos sobre a geometria no espaço. Essas obras constituem as mais antigas e importantes obras gregas a termos contato. Calcula-se que pelo menos mil edições já foram publicadas. Talvez nenhum livro além da Bíblia, possua tantas edições. Devido a sua grande contribuição para a área da geometria, Euclides ficou conhecido como "Pai da Geometria".

O algoritmo que é mencionado em *Os Elementos*, porém sem explicitar, o fato que é sempre possível efetuar uma divisão de b por a, com "resto" ou sobra. Devido este fato, ficou conhecido como Divisão Euclidiana.

2.3 DIVISÃO EUCLIDIANA

Imaginemos a seguinte situação: Desejamos dividir 14 bolinhas de gude entre 3 crianças. Com quantas bolinhas de gude cada criança ficará? Como 3 não divide 14. Teríamos a seguinte situação: separando as 14 bolinhas de gude em 3 partes iguais, ficaria cada uma das crianças com 4 bolinhas de gude e sobraria 2 bolinhas de gude, que seria o resto da divisão de 14 por 3.

Teorema (Divisão Euclidiana): Sejam a e b dois números naturais, com $a \neq 0$ e $a < b$. Existem dois únicos números naturais q e r, tais que $\boldsymbol{b = a \cdot q + r}$, com $r < a$.

Usualmente chamamos b de dividendo (número que será dividido), a de divisor (número que divide), q de quociente (resultado da divisão) e r de resto (o que sobra).

Primeiramente precisaremos do Princípio da Boa Ordenação (PBO): Todo conjunto não vazio de naturais, possui um menor elemento.

Demonstração: (Existência) Vamos supor que $a < b$ e considerar o conjunto $S = \{b - n\,a \,/\, n \in \mathbb{N} \text{ e } b - n\,a \geq 0\}$.

Pelo Princípio da Boa Ordenação, o conjunto S tem um menor elemento r, tal que $r = b - q\,a$ que equivale $b = a\,q + r$.

Vamos provar que $r < a$. Primeiramente se $a|b$, então $r = 0$ e não temos o que provar. Caso $a \nmid b$, então $r \neq a$, basta mostrar que não pode acontecer $r > a$. Caso ocorresse isto, existiria um número natural $c < r$ tal que $r = c + a \Longrightarrow r = c + a = b - q\,a$, daí teríamos:

$c = b - (q + 1) \cdot a$, pertencente ao conjunto S, com $c < r$; contradição pelo fato de r ser o menor elemento de S.

(Unicidade) Suponhamos que existam q' e r', tais que $b = a\,q' + r'$ com $0 \leq r' < a$. Comparando com $b = a\,q + r$, temos:

$a\,q + r = b = a\,q' + r' \Longrightarrow a\,q - a\,q' = r' - r \Longrightarrow a \cdot (q - q') = r' - r$, logo a divide $r' - r$.

Como $r' < a$ e $r < a$, temos $|r' - r| < a$ e, portanto, como a divide $r' - r$, deve-se ter $r' - r = 0$, ou seja, $r' = r$.

Desta forma, $a\,q = a\,q'$, por hipótese $a \neq 0$, temos $q = q'$. ■

Por exemplo, para determinarmos o quociente e o resto da divisão:

a) 26 por 5.

Observe as equivalências a seguir:

$26 = 5 \cdot 1 + 21$;

$26 = 5 \cdot 2 + 16$;

$26 = 5 \cdot 3 + 11$;

$26 = 5 \cdot 4 + 6$;

$26 = 5 \cdot 5 + 1$.

Note que os números 21, 16, 11 e 6 eram todos maiores que o divisor 5. Portanto, temos que 26 divido por 5 é da forma $26 = 5 \cdot 5 + 1$. Onde o quociente é 5 e o resto é 1.

b) 58 por 7.

De maneira direta note que, $58 = 7 \cdot 8 + 2$. Como 2 é menor que o divisor 7, temos que o quociente é 8 e o resto é 2.

> O professor não deve confundir o ensino do algoritmo da divisão com a construção das ideias e dos significados dessa operação. É recomendável que o algoritmo da divisão seja sistematizado apenas quando o professor tiver certeza de que alunos compreenderam o sentido da divisão e conseguem associar as ideias envolvidas na divisão a situações problema. (BIGODE, 2009, p. 43).

A divisão euclidiana é usualmente utilizada através do algoritmo que mostraremos a seguir devido a sua praticidade no calculo da divisão.

Observe o modelo abaixo, onde definimos o local do dividendo, divisor, quociente e resto:

Dividendo	Divisor
Resto	Quociente

Por exemplo, utilizando o algoritmo para efetuar a divisão de 37 por 8. Primeiramente procuramos um número (quociente) que multiplicado pelo divisor de igual ao dividendo ou menor mais próximo, daí temos que, $8 \cdot 4 < 37 < 8 \cdot 5$, logo o quociente é 4. Como $8 \cdot 4 = 32$, temos que o resto é 5, pois é o que sobra de 37 .

Ficando assim no algoritmo:

37	8
-32	4
5	

A explicação para o uso desse algoritmo é a praticidade de se obter o quociente e o resto de uma maneira clara.

Observação 2.3.1: Na divisão de um número natural n por 2, temos apenas dois possíveis restos, 0 ou 1. Quando resto for igual a 0 temos que $n = 2q$, onde chamamos esse n de par. Se o resto for igual a 1 temos que $n = 2q + 1$, onde chamamos esse n de ímpar.

Exemplo 2.3.1: Verifique a paridade da diferença de dois números naturais ímpares.

Solução: Sejam $n_1 = 2q_1 + 1$ e $n_2 = 2q_2 + 1$, dois números ímpares, com $n_1 > n_2$. Daí:

$n_1 - n_2 = 2q_1 + 1 - (2q_2 + 1) = 2 \cdot (q_1 - q_2) + 0$. Portanto a diferença de dois números naturais ímpares é sempre par.

Observação 2.3.2: Fixado um número natural $m \geq 2$, pode-se sempre escrever um número natural qualquer n, de modo único, segundo a divisão euclidiana, na forma $n = mk + r$, onde k e r pertencente aos naturais e $r < m$.

Por exemplo, todo número natural n pode ser escrito em uma, e somente uma, das seguintes formas: $5k$, $5k + 1$, $5k + 2$, $5k + 3$ ou $5k + 4$.

Exemplo 2.3.2: (ENC-2001) Seja N um número natural; prove que a divisão de N^2 por 6 nunca deixa resto 2.

Solução: Pela a observação 2.3.2, o número N pode ser escrito em uma, e somente uma, das seguintes formas: $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$ ou $6k + 5$, com k natural.

Se $N = 6k \Longrightarrow N^2 = 36k^2 = 6 \cdot (6k^2)$;

Se $N = 6k + 1 \Longrightarrow N^2 = 36k^2 + 12k + 1 = 6 \cdot (6k^2 + 2k) + 1$;

Se $N = 6k + 2 \Longrightarrow N^2 = 36k^2 + 24k + 4 = 6 \cdot (6k^2 + 4k) + 4$;

Se $N = 6k + 3 \Longrightarrow N^2 = 36k^2 + 36k + 9 = 6 \cdot (6k^2 + 6k + 1) + 3$;

Se $N = 6k + 4 \Longrightarrow N^2 = 36k^2 + 48k + 16 = 6 \cdot (6k^2 + 8k + 2) + 4$;

Se $N = 6k + 5 \Longrightarrow N^2 = 36k^2 + 60k + 25 = 6 \cdot (6k^2 + 10k + 4) + 1$;

Observe que os restos possíveis de N^2 quando dividido por 6 são 0, 1, 3 e 4. Portanto N^2 divido por 6 nunca deixa resto 2.

Exemplo 2.3.3: Prove que todo quadrado perfeito, quando dividido por 3 deixa resto 0 ou 1.

Solução: Seja n um número inteiro dito quadrado perfeito, então $n = q^2$, para um q inteiro.

Pela a observação 2.3.2, o número q pode ser escrito em uma, e somente uma, das seguintes formas: $3k$, $3k + 1$ ou $3k + 2$, com k natural.

Se $q = 3k \Longrightarrow q^2 = 3 \cdot 3k^2$;

Se $q = 3k + 1 \Longrightarrow q^2 = 3 \cdot (3k^2 + 2k) + 1$;

Se $q = 3k + 2 \Longrightarrow q^2 = 3 \cdot (3k^2 + 4k + 1) + 1$;

Observe que os restos possíveis q^2 quando dividido por 3 são 0 e 1. Portanto todo quadrado perfeito quando dividido por 3 deixa resto 0 ou 1.

2.4 TRABALHANDO COM OS RESTOS

A motivação dessa seção é mostrar que o resto de uma divisão euclidiana traz significados mais importantes além de uma simples sobra de uma divisão. Iremos trabalhar com alguns problemas que apresentam repetições periódicas e a resolução é feita através de uma analise dos seus possíveis restos.

Problemas que envolvem restos na divisão são muito comuns, o que iremos mostrar agora são algumas técnicas que podem facilitar as resoluções desses problemas.

Imagine o seguinte problema: (CESPE/UnB – SEDUC/CE – 2013) Por apresentar problemas técnicos, uma impressora imprimiu, seguidamente, sem espaços entre os caracteres, a palavra CANETA em uma página de papel em branco, de forma que o início da impressão era CANETACANETACANETACANETACANETA. Nessa situação, se a impressão foi interrompida no instante que a impressora imprimiu o caractere de número 1.043, então, esse último caractere impresso foi à letra?

Uma das maneiras de ser resolvido este problema é construindo uma tabela, constando as letras da palavra CANETA e o número do caractere que representa cada letra.

C	**A**	**N**	**E**	**T**	**A**
1	2	3	4	5	6
7	8	9	10	11	12

É fácil perceber se continuasse a completar essa tabela, descobriremos a letra que representa o número 1.043, porém levaria um bom tempo. Então vamos analisar por outro ponto de vista.

Como a palavra CANETA tem 6 letras, repare que cada letra se repete a cada 6 números, com atenção especial para letra A que aparece duas vezes na palavra CANETA, Por exemplo, os números que representam a letra C, são: 1, 7, 13, 19, ..., que pode ser representado da forma 6k +1, com k natural, ou seja, que deixam resto 1 quando divido por 6. Desta forma cada letra pode ser representada por uma forma, equivalente ao seu resto na divisão por 6, como já visto na observação 2.3.2.

$C \rightarrow 6k + 1$

$A \rightarrow 6k + 2$

$N \rightarrow 6k + 3$

$E \rightarrow 6k + 4$

$T \rightarrow 6k + 5$

$A \rightarrow 6k$

Agora basta dividirmos 1.043 por 6 e ver o resto que vai dar, assim saberemos que letra ele vai representar. Pela divisão euclidiana temos que $1.043 = 6 \cdot 173 + 5$, logo 1.043 é da forma $6k + 5$, portanto o último caractere é a letra T.

Verificamos que para resolver este problema, observamos a repetição periódica que acontecia, para podermos então, analisar os restos da divisão por 6 que no caso foi pela periodicidade da palavra CANETA, que se repetia a cada 6 caracteres.

Esses tipos de problemas são bem comuns, basta ter uma repetição bem ordenada, como são alguns casos presente no cotidiano: os dias que se repetem a cada 24 horas, as horas que se repetem a cada 60 minutos, os dias da semana que se repetem a cada 7 dias, os dias no ano que se repetem a cada 365 dias, as fases da lua e etc.

Proposição 2.4.1: "O resto na divisão de uma soma por um dado número é o mesmo que a soma dos restos da divisão das parcelas por este número". Exceto quando a soma dos restos for maior ou igual ao divisor; quando isto ocorrer, devemos dividir novamente ai sim obteremos o mesmo resto.

Demonstração: Consideramos dois números naturais N_1 e N_2, tais que a soma $N_1 + N_2$, quando divida por m, deixa resto s, com $0 \leq s < m$, ou seja, $N_1 + N_2 = mq + s$, com q natural. Agora quando divididos suas parcelas por m, deixam restos r_1 e r_2, com $0 \leq r_1, r_2 < m$, tais que $N_1 = m \cdot q_1 + r_1$ e $N_2 = m \cdot q_2 + r_2$, com q_1 e q_2 números naturais. Assim temos:

$$N_1 + N_2 = m \cdot q_1 + r_1 + m \cdot q_2 + r_2 = m \cdot (q_1 + q_2) + (r_1 + r_2).$$

Podemos escrever $r_1 + r_2 = mq' + r'$ e $q_1 + q_2 = q''$, com $0 \leq r' < m$. Daí, temos: $N_1 + N_2 = m \cdot (q_1 + q_2) + (r_1 + r_2) = mq'' + mq' + r' = m \cdot (q'' + q') + r'$. Logo pela unicidade dos restos, temos que $s = r'$. ■

Exemplo 2.4.1: Qual o resto da divisão de (504 + 253) por 10?

Solução: Vejamos as duas formas de solucionar este problema.

1ª Forma: Temos que $504 + 253 = 757 = 10 \cdot 75 + 7$, o que deixa resto 7;

2ª Forma: Temos que $504 = 10 \cdot 50 + 4$ e $253 = 10 \cdot 25 + 3$, somando os restos temos $4 + 3 = 7$, portanto o resto obtido é 7;

Observe que obtemos o mesmo resto de duas formas diferentes.

Exemplo 2.4.2: Qual o resto da divisão de (44 + 23) por 5?

Solução: Vejamos duas formas de solucionar este problema.

1ª Forma: Temos que $44 + 23 = 67 = 5 \cdot 13 + 2$, o que deixa resto 2;

2ª Forma: Temos que $44 = 5 \cdot 8 + 4$ e $23 = 5 \cdot 4 + 3$, somando os restos temos $4 + 3 = 7$, mais $7 = 5 \cdot 1 + 2$, portanto deixa resto 2;
Observe que obtemos o mesmo resto de duas formas diferentes.

Proposição 2.4.2: "O resto na divisão de um produto por um dado número é o mesmo que o produto dos restos da divisão dos fatores por este número". Exceto quando o produto dos restos for maior ou igual ao divisor; quando isto ocorrer, devemos dividir novamente ai sim obteremos o mesmo resto.

A demonstração segue de maneira análoga que foi vista na proposição 2.4.1 e é facilmente verificada.

Exemplo 2.4.3: Qual o resto da divisão $(23 \cdot 50)$ por 7?
Solução: Vejamos duas formas de solucionar este problema.
1ª Forma: $23 \cdot 50 = 1150 = 7 \cdot 164 + 2$, deixando resto igual a 2;
2ª Forma: $23 = 7 \cdot 3 + 2$ e $50 = 7 \cdot 7 + 1$, multiplicando os restos temos $2 \cdot 1 = 2$, deixando resto igual a 2;
Observe que obtemos o mesmo resto de duas formas diferentes.

(A vantagem é que a 2ª forma é bem mais pratica e simples, podendo ser feita mentalmente dependo dos números).

Exemplo 2.4.4: Qual o resto da divisão de 12^{2015} por 11?
Solução: Para efetuar essa potência 12^{2015}, seria praticamente impossível com uma calculadora normal. Sabemos que 12^{2015} apresentam 2015 fatores iguais a 12, daí basta calcular o resto da divisão de 12 por 11 e elevá-lo a 2015. Como o resto da divisão de 12 por 11 é 1 e como $1^{2015} = 1$, temos que o resto da divisão de 12^{2015} por 11 é 1.

Exemplo 2.4.5: Qual o resto da divisão de $(25 \cdot 45 + 76 \cdot 90)$ por 6?
Solução: Efetuando as divisões de 25, 45, 76 e 90 por 6, obtemos os seguintes restos 1, 3, 4 e 0. Agora substituindo os valores dos restos obtidos na expressão, temos $(1 \cdot 3 + 4 \cdot 0) = 3$, portanto do resto da divisão é 3.

Exemplo 2.4.6: Prove que $n^5 + 4n$ é divisível por 5 qualquer que seja o número natural n.
Solução: Temos que os possíveis restos de n por 5, são 0, 1, 2, 3 e 4, ou seja podemos escrever n nas seguintes formas: $5k$, $5k + 1$, $5k + 2$, $5k + 3$ e $5k + 4$, com k natural, para

facilitar usaremos a tabela abaixo para assim poder fazer uma melhor analise dos resultados, analisando separadamente os restos da divisão $n^5 + 4n$ por 5:

n	n^5	$4n$	$n^5 + 4n$
$5k$	$5k$	$5k$	$5k$
$5k + 1$	$5k + 1$	$5k + 4$	$5k + 5 = 5\ (k + 1)$
$5k + 2$	$5k + 32 = 5\ (k + 6) + 2$	$5k + 8 = 5\ (k + 1) + 3$	$5k + 5 = 5\ (k + 1)$
$5k + 3$	$5k + 243 = 5\ (k + 48) + 3$	$5k + 12 = 5\ (k + 2) + 2$	$5k + 5 = 5\ (k + 1)$
$5k + 4$	$5k + 1024 = 5\ (k + 204) + 4$	$5k + 16 = 5\ (k + 3) + 1$	$5k + 5 = 5\ (k + 1)$

Nosso principal objetivo é mostrar que a divisão de $n^5 + 4n$ por 5 deixa resto 0, portanto vamos priorizar analisar os restos. Observe que na primeira coluna analisamos os possíveis restos de n por 5, na segunda coluna os possíveis restos de n^5 por 5, na terceira coluna os possíveis restos de $4n$ por 5 e na última coluna somamos os resultados das segunda e terceira colunas e percebemos que em todos os casos obteve um múltiplo de 5, provando que $n^5 + 4n$ é divisível por 5.

O objetivo de apresentar essas propriedades da soma e do produto dos restos é que em muitos casos podem facilitar ou até mesmo ser a única solução para um problema apresentado.

2.5 NÚMEROS PRIMOS

Um número natural maior do que 1, cujo os únicos divisores positivos são 1 e ele próprio, esse número é chamado de número primo.

Dados dois números primos p e q e um número natural a qualquer, obtém-se:

i) Se $p|q$, então $p = q$.

Como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, ou seja, p deve ser maior do que 1, logo $p = q$.

ii) Se $p \nmid a$, então o máximo divisor comum de p e a é 1.

Se o máximo divisor comum de p e a for d, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e consequentemente, $d = 1$.

Um número natural maior do que 1 e que não é primo é chamado de composto.

Por exemplo, 2, 3, 5, 7, 11, 13 e 17 são números primos, enquanto que, 4, 6, 8, 9, 10, 12 e 14 são compostos, de acordo com a definição acima.

Proposição 2.5.1: Sejam a,b e p números naturais, sendo p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração: Seja p primo tal que $p|ab$. Se $p|a$, nada temos a demonstrar. Suponha então que $p \nmid a$, nesta condição, o único divisor positivo comum desses números é 1, assim podemos escrever $p \cdot x + a \cdot y = 1$, com x e y inteiros. Multiplicando ambos os lados dessa igualdade por b e reagrupando temos, $p \cdot (x \cdot b) + (a \cdot b) \cdot y = b$. Como $p|p$ e, por hipótese, $p|ab$ vem que $p|[\ p \cdot (x \cdot b) + (a \cdot b) \cdot y]$, ou seja, $p|b$. ■

Corolário: Se p, p_1, ..., p_n são números primos e , se $p|p_1 \cdot \cdot \cdot p_n$, então $p = p_i$ para algum $i = 1$, ..., n.

Demonstração: Use a proposição 2.5.1, indução sobre n, e o fato de que, se $p|p_i$, então $p = p_i$.

■

Proposição 2.5.2: (Crivo de Eratóstenes) Se um número natural $n > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leq n$ ou $p \leq \sqrt{n}$. (Em outras palavras significa dizer que o maior número primo possível que compõem esse número n, corresponde à raiz quadrada de n arredondada para baixo).

Demonstração: Seja $n = a \cdot b$, com $1 < a \leq b$. Seja p um divisor primo de a, segue que $p|n$ e $p^2 \leq a^2 \leq a \cdot b = n$, donde $p^2 \leq n$ ou $p \leq \sqrt{n}$. ■

Exemplo 2.5.1: O número 163 é primo ou composto?

Solução: Utilizando o crivo de Eratóstenes, basta verificar se 163 é múltiplo de algum dos primos 2, 3, 5, 7 ou 11, já que o próximo primo é número 13, e $13^2 = 169 > 163$. Como 163 não é múltiplo de 2, 3, 5, 7 ou 11. Logo o número 163 é primo.

Exemplo 2.5.2: Verifique se o número 343 é primo ou composto. Caso seja composto, escreva na sua forma fatorada.

Solução: Utilizando o crivo de Eratóstenes, basta verificar se 343 é múltiplo dos primos 2, 3, 5, 7, 11, 13 ou 17, já que o próximo primo é o número 19, e $19^2 = 361 > 343$. Ao verificar,

temos que 7 é múltiplo de 343. Portanto é um número composto, e que pode ser escrito das seguintes formas:
$343 = 7 \cdot 49$ ou $343 = 7^3$.

Teorema 2.5.1: (Teorema Fundamental da Aritmética) Todo número natural maior que 1 ou é primo ou se escreve de modo único como um produto de fatores de números primos.
Demonstração: Se $n = 2$, o resultado é obviamente verificado.

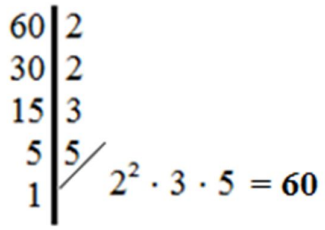
Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$.

(Unicidade) Suponha, agora, que $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_j e os q_j são números primos. Como $p_1 | q_1 \cdots q_s$, pelo corolário acima, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto, $p_2 \cdots p_r = q_2 \cdots q_s$.

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

Para realizar decomposição de um número composto, basta dividir o número pelo seu menor divisor diferente de 1, em seguida repetir esse procedimento com o quociente obtido, repetindo esse processo até que o quociente seja 1.

Figura 2 – Algoritmo da fatoração em números primos.



Fonte: Autor (2015)

No algoritmo que utilizamos na figura 2, tem a seguinte representação, na coluna da esquerda em cima fica o dividendo, o que vem logo abaixo dele é o quociente obtido da divisão e os demais são os próximos quocientes obtidos. Na coluna da direita são colocados

os seus respectivos menores divisores diferente de 1 do número que encontra-se a sua esquerda. (Por exemplo: o menor divisor de 15 é o 3, portanto colocamos o 3 a sua direita e o quociente obtido abaixo do 15).

Observação: como sabemos que o menor divisor diferente de 1 é um número primo. Logo podemos realizar essa fatoração utilizando como divisores qualquer número primo, que seja um divisor é claro.

Vejamos alguns exemplos de números naturais e suas respectivas decomposições em fatores primos:

a) $60 = 2^2 \cdot 3 \cdot 5$

b) $225 = 3^2 \cdot 5^2$

c) $112 = 2^4 \cdot 7$

Exemplo 2.5.3: O número 486 é divisível por 6?

Solução: Decompondo os números em fatores primos, temos: $486 = 2 \cdot 3^4$ e $6 = 2 \cdot 3$. Como o número 486 apresenta os fatores 2 e 3, logo o mesmo é divisível por 6.

Exemplo 2.5.4: Com quantos zeros termina o número $(375 \cdot 96)$?

Solução: Decompondo os números em fatores primos: $375 = 3 \cdot 5^3$ e $96 = 2^5 \cdot 3$.

Efetuando a multiplicação das igualdades, obtemos:

$$375 \cdot 96 = 3 \cdot 5^3 \cdot 2^5 \cdot 3 = 2^5 \cdot 3^2 \cdot 5^3$$

Como o que interessa é que termine com zero, basta verificar quantos fatores de 10 possuem. Assim, $2^5 \cdot 3^2 \cdot 5^3 = (2 \cdot 5)^3 \cdot 2^2 \cdot 3^2 = 10^3 \cdot 2^2 \cdot 3^2$. Portanto o número termina com 3 zeros.

3 CONGRUÊNCIA MODULAR

Neste capítulo apresentaremos o conceito de congruência modular, tal relação de extrema importância para as aplicações que apresentaremos no próximo capítulo, que é o assunto principal do nosso trabalho. Na próxima seção contaremos um pouco da história de Gauss, um dos propulsores da congruência modular.

3.1 FRIEDRICH GAUSS

Foi por volta de 1784, em Brunswick, Alemanha que ocorreu a história que é relatada por Paenza.

Uma professora de segundo ano do nível fundamental estava cansada da "confusão" que as crianças faziam, e para mantê-las um pouco quietos, deu-lhes o seguinte problema: "Calculem a soma dos primeiros cem números." A ideia era mantê-los calados durante um tempo. O fato é que o menino levantou a mão quase imediatamente, sem nem sequer dar tempo à professora para que terminasse de se acomodar na sua cadeira.

– Sim? – perguntou a professora, olhando para o menino.

– Já fiz, senhorita – respondeu o pequeno. – O resultado é 5050.

A professora não podia acreditar no que tinha ouvido, não porque a resposta fosse errada – o que não era –, mas porque estava desconcertada com a rapidez.

– Você a tinha feito antes? – perguntou.

– Não, acabei de fazer.

Enquanto isso, as outras crianças mal tinham chegado a escrever no papel os primeiros algarismos, e não entendiam a conversa entre o colega e a professora.

– Venha e conte a todos como fez

O jovenzinho se levantou do seu lugar e, sem sequer levar o papel que tinha diante de si, aproximou-se humildemente do quadro-negro e começou a escrever os números:

$1 + 2 + 3 + ... + 98 + 99 + 100$

– Bem – continuou o jovenzinho. O que fiz foi somar o primeiro e o último número (ou seja, o 1 e o 100). Essa soma dá 101.

Depois, continuei com o segundo e o penúltimo (o 2 e o 99). A soma novamente dá 101.

Dessa forma, ‘emparelhando’ os números assim e somando-os, tem-se cinquenta pares de números cuja soma dá 101. Logo, cinquenta vezes 101 resulta no número 5050, que é o que a senhorita queria.

A história termina aqui. O jovenzinho chamava-se Carl Friedrich Gauss. Nasceu em Brunswick, em 30 de abril de 1777, e morreu em 1855. Gauss é considerado o “príncipe da matemática”, e foi um dos melhores (se não o melhor) da história.

Figura 3 – Carl Friedrich Gauss.

Fonte: Wikipédia (2015)

Aos doze anos Gauss já olhava com desconfiança para os fundamentos da geometria euclidiana; aos dezesseis já tinha seu primeiro vislumbre de uma geometria diferente da de Euclides. Um ano mais tarde, começou uma busca critica das provas, na teoria dos números, que tinham sido aceitas por seus antecessores e tomou a decisão de preencher os vazios e completar o que tinha sido feito pela metade.

Foi Gauss que observou que usávamos com frequência frases do tipo “*a* da o mesmo resto que *b* quando dividido por *m*” e que essa relação tinha um comportamento semelhante com a igualdade. Foi em 1798, aos 21 anos que finalizou o seu livro *Disquisitiones Arithmeticae*, tornando assim publico a notação específica para este fato que conhecemos como Congruência Modular.

3.2 DEFINIÇÃO DE CONGRUÊNCIA MODULAR

Definição: Sejam a, b e m números naturais, com $m \neq 0$. Se os restos da sua divisão euclidiana por m são iguais, dizemos a e b são congruentes módulo m. Quando isso acontece usamos a simbologia:

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

Por exemplo, $26 \equiv 11 \pmod 5$, pois os restos da divisão de 26 e de 11 por 5, são iguais a 1. Portanto dizemos que 26 é congruente a 11 módulo 5.

Proposição 3.2.1: Sejam a, b e m números naturais, com $m \neq 0$ e $a > b$. Temos que:

$a \equiv b \pmod{m}$ se, e somente se, $m|a - b$.

Em outras palavras para verificar se dois números são congruentes módulo m, não é preciso efetuar a divisão euclidiana por m em ambos e depois verificar seus restos. Basta efetuar a diferença entre eles e verificar se é divisível por m.

Demonstração: Vejamos inicialmente que $a \equiv b \pmod{m}$ implica $m|a - b$.

Se $a \equiv b \pmod{m}$, pelo algoritmo euclidiano temos,

$a = q_1 \cdot m + r$

$b = q_2 \cdot m + r$; com q_1, q_2 e r números naturais.

Agora $a - b = (q_1 - q_2) \cdot m$

Logo $m|a - b$.

Reciprocamente, se $m|a - b$, então $a - b = q \cdot m$; com q natural.

Pelo algoritmo euclidiano temos,

$a = q_1 \cdot m + r_1$

$b = q_2 \cdot m + r_2$; com q_1, q_2, r_1 e r_2 números naturais e $0 \leq r_1, r_2 < m$.

Como $a - b = q \cdot m$

Então $q_1 \cdot m + r_1 - (q_2 \cdot m + r_2) = q \cdot m \Longrightarrow m|r_1 - r_2$

Como $0 \leq r_1, r_2 < m$

Daí $r_1 - r_2 = 0 \Longrightarrow r_1 = r_2$.

Logo $a \equiv b \pmod{m}$. ■

Observe no exemplo anterior que, $26 - 11 = 15$ e como $5|15$. Portanto pela proposição acima temos que $26 \equiv 11 \pmod 5$.

Agora caso o número a não seja congruente ao número b módulo m, usamos a seguinte simbologia:

$a \not\equiv b \pmod{m}$.

A teoria de congruência é muito importante para calcularmos o resto da divisão entre dois números. Note que todo número é congruente módulo m ao resto de sua divisão por m e, portanto, é congruente módulo m a um dos números 0, 1, 2, ..., m-1.

Por exemplo, 20 dividido por 3, deixa resto 2, pois $20 = 3 \cdot 6 + 2$.

Daí, podemos escrever que $20 \equiv 2 \pmod{3}$.

3.3 PROPRIEDADES DAS CONGRUÊNCIAS MODULARES

Nessa secção abordaremos as propriedades da congruência modular, propriedades essas de extrema relevância para o que veremos em seguida em resoluções de problemas e algumas aplicações.

Nas propriedades, não se utiliza o caso $m = 1$, pois se usássemos congruência módulo 1, obteríamos $a \equiv b \pmod{1}$ que é o mesmo que $1|a - b$, o que é sempre verdade para quaisquer a e b. Por isso excluímos essa possibilidade.

Sejam a, b, c, d e m números naturais, com $m > 1$. Valem as seguintes propriedades:

i) $a \equiv a \pmod{m}$.

ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

iv) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

v) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

vi) Se $a \equiv b \pmod{m}$, então $a + c \equiv b + c \pmod{m}$.

vii) Se $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{m}$.

viii) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$, para n natural.

ix) Se $a \equiv b \pmod{m}$ e $n|m$, então $a \equiv b \pmod{n}$.

Demonstração:

i) Como $m|0$, então $m|a - a$, o que os diz que $a \equiv a \pmod{m}$.

ii) Se $a \equiv b \pmod{m}$, temos que $m|a - b$, logo $a - b = mk$. Multiplicando essa última igualdade toda por (-1), temos que $-(a - b) = -mk$, assim $b - a = m(-k)$, logo $b \equiv a \pmod{m}$.

iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem inteiros k e k' tais que:
$a - b = mk$ e $b - c = mk'$. Somando membro a membro as duas igualdades anteriores, temos:
$(a - b) + (b - c) = mk + mk' \Longrightarrow a - c = m(k + k')$.
Logo temos que $m|(a - c)$, ou seja, $a \equiv b \pmod{m}$.

iv) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então existem inteiros k e k' tais que:
$a - b = mk$ e $c - d = mk'$. Somando membro a membro as duas igualdades anteriores, temos:
$(a - b) + (c - d) = mk + mk' \Longrightarrow (a + c) - (b + d) = m(k + k')$.
Logo temos que $m|[(a + c) - (b + d)]$, ou seja, $a + c \equiv b + d \pmod{m}$.

v) Demonstração é feita de maneira análoga ao item (iv).

vi) Se $a \equiv b \pmod{m}$, temos que $a - b = mk$. Somando e subtraindo c no primeiro membro da igualdade, temos: $a - b + c - c = mk \Longrightarrow (a + c) - (b + c) = mk$.
Assim temos que $a + c \equiv b + c \pmod{m}$.

vii) Se $a \equiv b \pmod{m}$, temos que $a - b = mk$. Multiplicando ambos os lados da igualdade por c, temos: $ac - bc = mkc$.
Assim temos que $ac \equiv bc \pmod{m}$.

viii) Se $a \equiv b \pmod{m}$, então $m|a - b$. Sabemos que:

$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$. Como $m|a - b$, então $m|a^n - b^n$.
Assim $a^n \equiv b^n \pmod{m}$.

ix) Se $a \equiv b \pmod{m}$, então $m|a - b$. Como $n|m$, então $n|a - b$. Logo $a \equiv b \pmod{n}$.

3.4 ARITMÉTICA DOS RESTOS

Nesta seção colocaremos em prática através de situações problemas, exemplos da utilidade das propriedades da congruência modular nas resoluções de problemas que envolva a analise dos restos.

As propriedades de congruência modular facilitam o cálculo de alguns problemas, com a obtenção do resto de uma divisão. Por exemplo, qual o resto da divisão 17^{2014} por 13?

De fato não seria tarefa fácil apenas com os métodos que dispomos, sem o uso da congruência modular. Observe a solução como se torna mais prática com o uso de suas propriedades:

Temos que, $17 \equiv 4 \pmod{13}$.

Pela propriedade (viii) temos, $17^2 \equiv 4^2 \pmod{13} \Longrightarrow 17^2 \equiv 3 \pmod{13}$.

Pela propriedade (v) temos, $17 \cdot 17^2 \equiv 4 \cdot 3 \pmod{13} \Longrightarrow 17^3 \equiv -1 \pmod{13}$.

Como $17^{2014} = (17^3)^{671} \cdot 17$.

Temos, $17^{2014} \equiv (-1)^{671} \cdot 4 \pmod{13} \Longrightarrow 17^{2014} \equiv -4 \pmod{13}$

Assim $17^{2014} \equiv 9 \pmod{13}$.

Portanto o resto da divisão de 17^{2014} por 13 é 9.

Exemplo 3.4.1: Determine o resto da divisão de 50^{2015} por 7.

Solução: Como $50 = 7 \cdot 7 + 1$, temos que $50 \equiv 1 \pmod{7}$.

$50^{2015} \equiv 1^{50} \pmod{7} \Longrightarrow 50^{2015} \equiv 1 \pmod{7}$.

Portanto o resto na divisão de 50^{2015} por 7 é 1.

Veremos agora a praticidade da congruência modular que pode ser aplicada nas situações problemas já vistas na seção trabalhando com os restos.

No exemplo **(2.4.6):** Prove que $n^5 + 4n$ é divisível por 5 qualquer que seja o número natural n.

Solução: Note que $n^5 + 4n = n(n^4 + 4)$. Se $n \equiv 0 \pmod 5$, temos que $n^5 + 4n \equiv 0 \pmod 5$, portanto $5 | n^5 + 4n$.

Se $n \equiv 1 \pmod 5$, $n^4 + 4 \equiv 1 + 4 \equiv 0 \pmod 5$ $\therefore n^5 + 4n \equiv 0 \pmod 5$.

Se $n \equiv 2 \pmod 5$, $n^4 + 4 \equiv 16 + 4 \equiv 0 \pmod 5$ $\therefore n^5 + 4n \equiv 0 \pmod 5$.

Se $n \equiv 3 \pmod 5$, $n^2 \equiv 9 \equiv 4 \pmod 5$ daí, $n^4 + 4 \equiv 16 + 4 \equiv 0 \pmod 5$

$\therefore n^5 + 4n \equiv 0 \pmod 5$.

Finalmente se $n \equiv 4 \pmod 5$, $n^2 \equiv 16 \equiv 1 \pmod 5$ e $n^4 + 4 \equiv 1 + 4 \equiv 0 \pmod 5$

$\therefore n^5 + 4n \equiv 0 \pmod 5$.

Portanto $n^5 + 4n$ é divisível por 5.

Exemplo 3.4.2: Uma pessoa que comemorou seu aniversário numa terça-feira, sabendo que esse ano e o próximo não será ano bissexto, qual dia da semana ele irá comemorar seu aniversário no próximo ano?

Solução: Como os dias da semana se repetem a cada 7 dias, basta tomar os 365 dias de um ano e fazer congruência módulo 7. Vemos que $365 \equiv 1 \pmod 7$, ou seja, será um dia a frente na semana, no caso será uma quarta-feira.

Exemplo 3.4.3: Encontre o resto da divisão 7^{50} por 11.

Solução: Vamos analisar as congruências, 7^n módulo 11, com n natural:

$7^2 = 49 \equiv 5 \pmod{11}$

Usando a propriedade (vii), temos que:

$7^2 \cdot 7 \equiv 5 \cdot 7 \pmod{11} \Longrightarrow 7^3 \equiv 2 \pmod{11}$

$7^4 \equiv 14 \pmod{11} \Longrightarrow 7^4 \equiv 3 \pmod{11}$

$7^5 \equiv 21 \pmod{11} \Longrightarrow 7^5 \equiv -1 \pmod{11}$

$(7^5)^{10} \equiv (-1)^{10} \pmod{11} \Longrightarrow 7^{50} \equiv 1 \pmod{11}$.

Portanto o resto na divisão 7^{50} por 11 é 1.

Exemplo 3.4.4: Mostre que $2^{20} - 1$ é divisível por 41.

Solução: Sabemos que $2^{10} = 1024 = 41 \cdot 24 + 40$.

Logo $2^{10} \equiv -1 \pmod{41} \Longrightarrow (2^{10})^2 \equiv (-1)^2 \pmod{41} \Longrightarrow 2^{20} \equiv 1 \pmod{41}$.

Pela definição temos que, $41 | 2^{20} - 1$.

Exemplo 3.4.5: Qual o algarismo das unidades do número $7^{2015} + 4^{100?}$

Solução: Para encontrar o algarismo das unidades, devemos encontrar o resto da divisão desse número por 10.

Temos que, $7^2 \equiv -1 \pmod{10}$.

Pela propriedade (viii) temos $(7^2)^{1007} \equiv (-1)^{1007} \pmod{10} \Longrightarrow 7^{2014} \equiv -1 \pmod{10}$

Daí $7^{2015} \equiv -7 \pmod{10} \Longrightarrow 7^{2015} \equiv 3 \pmod{10}$. (1)

Agora,

$4^2 \equiv 6 \pmod{10}$

$4^3 \equiv 4 \pmod{10}$

$4^4 \equiv 6 \pmod{10}$

$4^5 \equiv 4 \pmod{10}$

Repare a regularidade que acontece com potência de base 4, quando o expoente é ímpar o algarismo das unidades é 4, já quando o expoente é par o algarismo das unidades é 6. Um caso de repetição periódica.

Daí então, $4^{100} \equiv 6 \pmod{10}$ (2)

Finalmente usando a propriedade (iv) nas congruências (1) e (2), temos:

$7^{2015} + 4^{100} \equiv 3 + 6 \pmod{10} \Longrightarrow 7^{2015} + 4^{100} \equiv 9 \pmod{10}$.

Portanto o algarismo das unidades é o 9.

É fácil perceber que a congruência modular é uma ferramenta matemática, de grande utilidade. Cálculos difíceis de ser solucionada, com o seu uso e as suas propriedades têm solução de maneira mais pratica e de fácil entendimento.

4 APLICAÇÕES DE CONGRUÊNCIAS

Apresentam-se nesse capítulo algumas aplicações de congruência modular. O objetivo é chamar a atenção do leitor para um campo da matemática bem interessante e ao mesmo tempo de difícil compreensão para alguns alunos da educação básica, que é a divisão. Fato percebido por experiência própria de professor, experiência de colegas professores e também mencionado por alunos.

> Sabemos das dificuldades presentes no ensino da matemática, devemos procurar tornar as aulas mais atrativas, especialmente quando falamos dos atuais estudantes mais imediatistas e menos interessados em aulas apenas teóricas. Nessas condições, o que podemos tentar fazer é tornar nossas aulas as mais atrativas possíveis, aos olhos deles. (Melo, 2014, p.53).

O intuito é, através das aplicações que mostraremos aqui, fazer com que os alunos tenham mais interesse e curiosidade sobre essas aplicações e percebam que a matemática está presente no seu cotidiano, às vezes de maneira bem sutil e de fácil entendimento.

As aplicações que apresentaremos tem sua importância, seja nas soluções de problemas presentes na atualidade, seja facilitando nas soluções de problemas de matemática do ensino básico.

4.1 CRITÉRIOS DE DIVISIBILIDADE

No ensino nas escolas de educação básica é abordado alguns assuntos como critérios de divisibilidade, como sendo um conjunto de regras a serem memorizadas e aplicadas de maneira direta sem mesmo entender o porquê de se utilizá-las. É fato que tal conteúdo, que é considerado como “atalho” se mostra muito útil nas resoluções de problemas. Mais a maneira de como é inserida, prejudica a capacidade do aluno de desenvolver seu raciocínio lógico.

> A operação de divisão, por outro lado, envolve conhecimento além daquele relativo à obtenção de subconjuntos equivalentes quando se reparte. Como uma operação multiplicativa, requer a coordenação dos fatores envolvidos - dividendo, divisor e quociente - através do entendimento das relações que estes termos podem estabelecer entre si. (CORREA, 2000, p. 13).

Neste capítulo iremos estudar as demonstrações dos critérios de divisibilidade, usando o conceito de congruências modulares. A intenção é justificar tais critérios e proporcionar um estímulo para os alunos, para que eles tenham mais interesse e prazer pela disciplina da matemática, que anda cada vez com menos interesses pelos os alunos da educação básica.

Para realizarmos as demonstrações a seguir, vamos considerar sem perda de generalidade, um número natural $N = a_r...a_2a_1a_0$, com $r + 1$ algarismos, que pode ser escrito, na base 10, como $N = a_r \cdot 10^r + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Critérios de divisibilidade por 2.

"Um número é divisível por 2 se, e somente se, o último algarismo for par".

Demonstração: Sabemos que 10 pode decomposto, como $10 = 2 \cdot 5$, Assim um número natural N pode ser escrito na forma:

$N = a_r \cdot 2^r \cdot 5^r + ... + a_2 \cdot 2^2 \cdot 5^2 + a_1 \cdot 2 \cdot 5 + a_0 = 2 \cdot (a_r \cdot 2^{r-1} \cdot 5^r + ... + a_2 \cdot 2 \cdot 5^2 + a_1 \cdot 5) + a_0$

Como $2 \cdot (a_r \cdot 2^{r-1} \cdot 5^r + ... + a_2 \cdot 2 \cdot 5^2 + a_1 \cdot 5) \equiv 0 \pmod 2$, temos:

$N \equiv a_0 \pmod 2$.

Portanto N é divisível por 2 se, e somente se, $a_0 \equiv 0 \pmod 2$ se, e somente se, o último algarismo é par. ■

Critérios de divisibilidade por 5.

"Um número é divisível por 5 se, e somente se, o último algarismo for 0 ou 5".

Demonstração: Sabemos que 10 pode decomposto, como $10 = 2 \cdot 5$, assim um número N pode ser escrito na forma:

$N = a_r \cdot 2^r \cdot 5^r + ... + a_2 \cdot 2^2 \cdot 5^2 + a_1 \cdot 2 \cdot 5 + a_0 = 5 \cdot (a_r \cdot 2^r \cdot 5^{r-1} + ... + a_2 \cdot 2^2 \cdot 5 + a_1 \cdot 2) + a_0$

Como $5 \cdot (a_r \cdot 2^r \cdot 5^{r-1} + ... + a_2 \cdot 2^2 \cdot 5 + a_1 \cdot 2) \equiv 0 \pmod 5$, temos:

$N \equiv a_0 \pmod 5$.

Portanto N é divisível por 5 se, e somente se, $a_0 \equiv 0 \pmod 5$ se, e somente se, o último algarismo for 0 ou 5. ■

Critérios de divisibilidade por 3.

"Um número é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3".

Demonstração: Seja o número $N = a_r \cdot 10^r + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Sabemos que $10 \equiv 1 \pmod 3 \Longrightarrow 10^n \equiv 1^n \pmod 3 \Longrightarrow 10^n \equiv 1 \pmod 3$.

Substituindo esta congruência em N, temos:

$N \equiv (a_r \cdot 1 + ... + a_2 \cdot 1 + a_1 \cdot 1 + a_0) \bmod 3 \Longrightarrow N \equiv (a_r + ... + a_2 + a_1 + a_0) \bmod 3$

O que nos diz que N é divisível por 3 se, e somente se, $a_r + ... + a_2 + a_1 + a_0$ é divisível por 3.

■

Exemplo 4.1.1: (CFS) É divisível por 2, 3 e 5 simultaneamente o número:

a) 235 b) 520 c) 230 d) 510 e) 532

Solução: Para o número ser divisível por 2, 3 e 5 simultaneamente, ele deve obedecer aos três critérios.

1º Para ser divisível por 2, o último algarismos deve ser par, portanto o item a) está falso.

2º Para ser divisível por 5, o último algarismos deve ser 0 ou 5, portanto o item e) está falso.

3º Para ser divisível por 3, a soma dos algarismos deve ser divisível por 3, daí temos:

b) 5+2+0 = 7 c) 2+3+0 = 5 d) 5+1+0 = 6, portanto os itens b) e c) estão falsos.

Assim o número 520 é divisível por 2, 3 e 5 simultaneamente.

Critérios de divisibilidade por 9.

"Um número é divisível por 9 se, e somente se, a soma de seus algarismos for um número divisível por 9".

Demonstração: A demonstração pode ser feita de maneira análoga, a realizada por 3, pois temos, $10^n \equiv 1 \pmod 9$. ■

Exemplo 4.1.2: (EPCAr) Seja um número $m = 488a9b$ onde b é o algarismo das unidades e a o algarismo das centenas. Sabendo-se que m é divisível por 45, então $a + b$ é igual a:

Solução: Para que m seja divisível por 45 ele deve ser divisível por 5 e 9 simultaneamente, pois $45 = 9 \cdot 5$, para que isso ocorra, deve seguir as seguintes condições:

1º Para m ser divisível por 5, b deve ser 0 ou 5.

2º Para m ser divisível por 9, devemos ter a soma dos algarismos divisível por 9, para que isso ocorra $(4 + 8 + 8 + a + 9 + b) = (29 + a + b)$ deve ser divisível por 9.

Pelas condições teríamos duas opções para o valor de b:

Primeira opção, para $b = 0$, temos $a = 7$.

Segunda opção, para $b = 5$, não temos valor para a que satisfaça a 2º condição.

Portanto $a + b = 7$.

Critérios de divisibilidade por 11.

"Um número é divisível por 11 se, e somente se, a soma dos algarismos de ordem ímpar, subtraída da soma dos algarismos de ordem par, forma um número divisível por 11".

Demonstração: Seja $N = a_r \cdot 10^r + ... + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Sabemos que $10 \equiv -1 \pmod{11} \Longrightarrow 10^n \equiv (-1)^n \bmod 11$, daí temos:

$$\begin{cases} 10^n \equiv 1\ (mod\ 11), se\ n\ for\ par. \\ 10^n \equiv -1\ (mod\ 11), se\ n\ for\ ímpar \end{cases}$$

Agora substituindo essa congruência em N, temos:

$N \equiv (a_r \cdot (-1)^n + ... - a_3 + a_2 - a_1 + a_0) \bmod 11$

$N \equiv [(a_0 + a_2 + ...) - (a_1 + a_3 + ...)] \bmod 11$

(Note que: a_0, a_2, ... são algarismos de ordem ímpar e a_1, a_3, ... são algarismos de ordem par).

O que nos diz que N só é divisível por 11 se, e somente se, a soma de suas ordens ímpares, subtraída da soma de suas ordens pares, for um número divisível por 11. ■

Exemplo 4.1.3: Verifique se o número 90827 é divisível por 11.

Solução: Usando o critério de divisibilidade por 11, temos que:

A soma dos algarismos de ordem ímpar é 9 + 8 + 7 = 24.

A soma dos algarismos de ordem par é 0 + 2 = 2.

Subtraindo, 24 – 2 = 22, que é divisível por 11.

Portanto o número 90827 é divisível por 11.

Critérios de divisibilidade por 7.

"Um número é divisível por 7 se, e somente se, quando retirado o algarismo das unidades, em seguida o número que restou subtraído do dobro do número retirado for divisível por 7".

Demonstração: Seja $N = a_r \cdot 10^r + ... + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Podemos escrevê-lo como, $N = 10 \cdot (a_r \cdot 10^{r-1} + ... + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1) + a_0$.

Somando e subtraindo $20 \cdot a_0$, temos que,

$N = 10 \cdot (a_r \cdot 10^{r-1} + ... + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1 - 2 \cdot a_0) + a_0 + 20 \cdot a_0$.

$N = 10 \cdot (a_r \cdot 10^{r-1} + ... + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1 - 2 \cdot a_0) + 21 \cdot a_0$.

$N = 10 \cdot (N_1 - 2 \cdot a_0) + 21 \cdot a_0$, onde $N_1 = a_r \cdot 10^{r-1} + ... + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1$, ou seja, é o número sem o último algarismo de N.

$N \equiv 10 \cdot (N_1 - 2 \cdot a_0) \pmod 7$.

Como 10 não é divisível por 7. Logo para N ser divisível por 7, devemos ter $N_1 - 2 \cdot a_0$ divisível por 7. ■

Exemplo 4.1.4: Verifique se o número 7315 é divisível por 7.

Solução: Aplicando a regra do critério de divisibilidade, temos que:

$731 - 2 \cdot 5 = 721$ que é divisível por 7.

Caso o número obtido ainda for grande, pode-se aplicar a regra novamente, até que possa verificar a divisibilidade por 7.

$72 - 2 \cdot 1 = 70$ que é divisível por 7.

Como já visto em exemplos anteriores, alguns critérios de divisibilidade são combinações entre outros critérios. Por exemplo, para um número ser divisível por 15, ele deve obedecer ao critério de divisibilidade por 3 e por 5, simultaneamente, pois $15 = 5 \cdot 3$.

O objetivo principal desse capítulo é que o aluno após visto as demonstrações apresentadas, tenham um melhor entendimento sobre esses critérios, e possibilitando ao aluno investigar outros métodos.

> A missão dos educadores é preparar as novas gerações para o mundo em que terão de viver. Isto quer dizer proporcionar-lhes o ensino necessário para adquiram as destrezas e habilidades que vão necessitar para seu desempenho, com comodidade e eficiência, no seio da sociedade que enfrentaram ao concluir sua escolaridade. (Santaló 1996, p. 11).

4.2 DÍGITO DE VERIFICAÇÃO

É um mecanismo de controle, também conhecido como número-controle que tem como objetivo verificar a validade e a autenticidade de um valor numérico, evitando fraudes ou erros de transmissão e digitação. Caso uma pessoa cometa um erro de digitação a máquina irá reconhecer o erro e não aceitará os números informados.

Esse tipo de mecanismo se encontra presente em CPF, CNPJ, Título Eleitoral, Cartão de Crédito, Código de Barras e outros.

4.2.1 CPF

O CPF é composto por 11 algarismos, onde o antepenúltimo dígito ou terceiro dígito da direita para a esquerda refere-se ao estado onde foi emitido o documento. No caso de uma pessoa que emitiu o documento no Ceará, terá como o antepenúltimo dígito o algarismo (3). Exemplo: CPF XXX.XXX.XX3 – XX.

Para descobrir os dois dígitos de verificação do CPF, iremos aplicar noções de congruência modular.

Primeiramente multiplicamos os nove primeiros algarismos da esquerda para a direita, pelo seu número de ordem e somar os produtos obtidos. O número encontrado, que chamaremos de S_1, deve ser congruente modulo 11. Por exemplo, se o CPF de uma pessoa tem os seguintes nove primeiros algarismos: 243.105.073-XX, o primeiro dígito de controle será obtido da seguinte maneira:

1) $S_1 = 2x1 + 4x2 + 3x3 + 1x4 + 0x5 + 5x6 + 0x7 + 7x8 + 3x9 = 136$.

Aplicando a congruência modulo 11, temos:

2) $136 \equiv 4 \pmod{11}$

Dessa forma o primeiro dígito de controle será o algarismo **4**.

Para determinar o segundo dígito de controle, multiplicamos agora os dez primeiros algarismos da esquerda para a direita, pelo seu número de ordem começando do zero e somar os produtos obtidos. O número encontrado, que chamaremos de S_2, deve ser congruente modulo 11. Continuando com o mesmo exemplo, temos os seguintes dez primeiros algarismos: 243.105.073-4X, assim o segundo dígito de controle será obtido da seguinte maneira:

3) $S_2 = 2x0 + 4x1 + 3x2 + 1x3 + 0x4 + 5x5 + 0x6 + 7x7 + 3x8 + 4x9 = 147$

4) $147 \equiv 4 \pmod{11}$

Dessa forma o segundo dígito de controle será o algarismo **4**. Concluímos então que, no nosso exemplo, o CPF completo seria: 243.105.073-44.

Observação: Caso a congruência modulo 11 seja 10, utilizamos o dígito 0 (zero).

O interessante de trabalhar congruência utilizando o CPF é que podemos inserir de maneira bem simples o conteúdo, de tal modo que provoque o interesse dos alunos, pois estaremos inseridos dentro do cotidiano. Podendo até começar com uma brincadeira, onde eles divulgaria apenas os 8 primeiros algarismos, daí o nono algarismo seria referente ao estado de emissão do CPF e os outros dois algarismos seria descoberta pela congruência.

4.2.2 CÓDIGO DE BARRAS

Atualmente, muitos produtos são identificados através de uma representação por barras e chamado código de barras. Com o avanço das tecnologias, tornou-se relativamente barato e acessível aparelho de leitura óptica e computador, o que tornou este tipo de código de barras bastante frequente. Na figura 4 abaixo, aparece um código de barras, note que abaixo da barra aparece números, de forma que o leitor humano também possa ler.

Primeiramente uma definição técnica. O código de barras é uma representação gráfica de dados, que permite uma rápida captação de dados, proporcionando velocidade nas transações, precisão nas informações, diminuição de erros e um custo baixo. É fácil perceber que seu uso se torna cada vez mais popular devido a suas inúmeras vantagens. Hoje em dia é usado pelo mundo todo em vários campos como, indústria, comércio, bancos, bibliotecas e muitas outras áreas de atuação.

Um dos códigos de barras de maior utilização hoje é o EAN-13, composto por 13 algarismos e tem a seguinte interpretação: os primeiros dois ou três algarismos são usados para a identificação do país de origem. No caso do Brasil são utilizados os algarismos, 789. Os próximos quatro ou cinco algarismos servem para identificação da empresa e os cinco algarismos seguintes são de identificação do produto e o último seria o dígito de verificador ou dígito de controle

Figura 4 – Código de barras EAN-13

Fonte: Portal Registro legal (2015)

No caso de ocorrer algum problema que impeça a leitura do código, o operador deverá digitar o código manualmente.

Como já vimos no CPF, o dígito verificador serve para impedir que erros de digitação possam acontecer. No caso do código de barras usamos a congruência modulo 10 e os fatores da base de multiplicação são apenas 1 e 3, que vão se repetindo.

O processo é o seguinte: multiplicamos os doze primeiros algarismos da esquerda para a direita, nessa ordem, pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. O número encontrado, que chamaremos de *S*, deve ser somado com o dígito verificador que ainda não conhecemos que chamaremos de a_{13}, e essa soma deve ser congruente a 0 modulo 10 ($S + a_{13} \equiv 0 \pmod{10}$). Por exemplo, de um código de barras que tem os doze primeiros algarismos, 489166832668.

1) $S = 4 + 8x3 + 9 + 1x3 + 6 + 6x3 + 8 + 3x3 + 2 + 6x3 + 6 + 8x3 = 131$
2) $131 + a_{13} \equiv 0 \pmod{10} \Longrightarrow a_{13} = 9$

Portanto o dígito verificador do exemplo citado é o algarismo 9.

Uma aplicação bem simples, como essa do código de barras, que está presente no dia a dia do aluno, permite que o conteúdo da matemática tenha mais significado ao aluno e eles consigam perceber a matemática ao seu redor. No caso do código de barras, temos também que as combinações dos números podem nós dizer algo, como o país de origem, a fábrica e o produto.

4.3 CRIPTOGRAFIAS

A palavra criptografia vem do grego Kryptos (escondido) + grafia (escrita), e significa a arte de escrever em cifra ou código. A criptografia consiste em uso de técnicas permitindo que somente o remetente e o destinatário de uma mensagem possam decifrar ou entender o verdadeiro significado. O benefício é que caso a mensagem fosse interceptada por algum espião, está mensagem seria ilegível, portanto sem valor algum. Daí o desafio de enviar mensagens sem que elas fossem decifradas. Desde período antes de cristo, já se tem relato do uso da criptografia, vejamos a técnica utilizada, para transmitir mensagem de forma secreta, contada pelo grego Heródoto (485 a.C. - 420 a.C.):

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem

> foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos. (SINGH, 2007, p. 20).

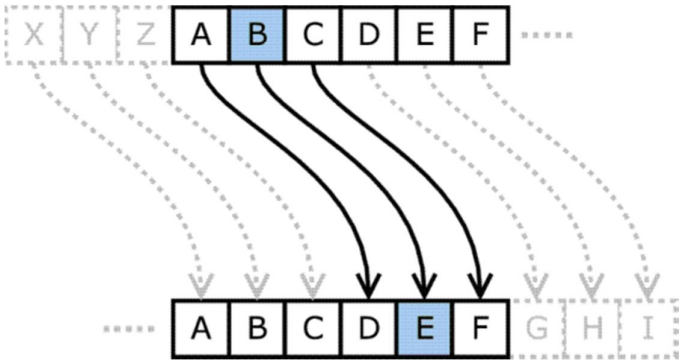
E assim a necessidade de enviar mensagens de forma secreta é tão antiga como a origem da escrita. Com a evolução das tecnologias e os meios de comunicação como os computadores com acesso a internet, tornou cada vez mais difícil de manter sigilo no envio de mensagens. Se há uma necessidade de esconder algo, isto quer dizer que alguém tem interesse em desvendar.

A criptografia consiste em tomar uma mensagem normal e codifica-la, ou seja, escrever de outra forma para caso de terceiros interceptarem não terem acesso ao conteúdo da mensagem. O destinatário que recebe esta mensagem deverá fazer o processo inverso, ou seja, vai decodificar o que seria reescrever a mensagem de forma correta.

> Naturalmente todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo. Portanto para decifrar é preciso ‘quebrar’ o código. (COUTINHO, 2013, p. 1)

Um dos primeiros casos que se ouviu falar em criptografia ocorreu em Roma, com o imperador Júlio César, que enviava mensagens aos seus generais trocando letras do alfabeto a partir de uma simples regra, para fazer a codificação trocava-se cada letra da mensagem original pela terceira letra adiante no alfabeto. Conhecido como “Cifra de César”

Figura 5 – Cifra de César.



Fonte: Wikipédia (2015)

Desta forma, somente quem soubesse da regra conseguiria decodificar a mensagem recebida, ou seja, fazer o processo inverso, troca cada letra da mensagem recebida pela terceira letra atrás no alfabeto.

Por exemplo, alguém que recebesse a mensagem "*dwfdu dr hvfxuhfhu*", deveria decodificar e só assim conseguiria identificar a mensagem original que seria "atacar ao escurecer".

Com o passar do tempo se tornava cada vez mais utilizado o uso de criptografias, e um dos problemas eram as distribuição dessas chaves de forma segura. Essas chaves tem o mesmo significado de senha, que é utilizado como elemento secreto pelos métodos criptográficos. O método mais seguro para essa distribuição de chaves naquela época era a contratação de pessoas de confiança! Essas chaves seriam o algoritmo de mecanismo da criptografia, ou seja, transforma um texto puro em um texto codificado, ou vice-versa, durante a decodificação, seria um processo similar a "Cifra de César", só que cada chave seria um processo diferente já definido.

Figura 6 – Processo de criptografia simétrica.

Fonte: Revista easy net – magazine 27

A criptografia simétrica se baseava na seguinte maneira; a mesma chave que era usada para criptografar um texto era usada para descriptografar só que de maneira inversa.

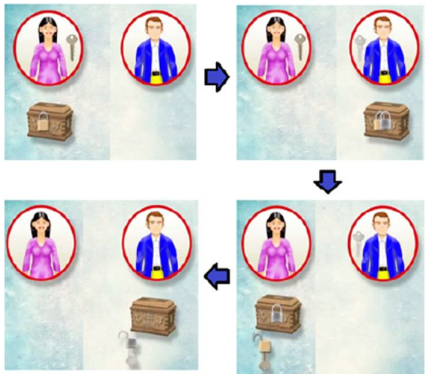
A história de Bob e Alice (Criptografia e chaves públicas) – Mencionada por CRATO.

Imaginemos um casal, Alice e Bob, que vivem isolados e apenas podem comunicar através do correio. Eles sabem que o carteiro é um tremendo "fofoqueiro" e que lê todas as suas cartas. Alice tem uma mensagem para Bob e não quer que ela seja lida. Que é que pode fazer? Ela pensou em enviar um cofre com uma mensagem, fechado a cadeado. Mas como lhe fará chegar à chave? Não pode enviar, pois assim Bob não poderá abrir. Se enviar a chave em separado, o carteiro pode fazer uma cópia.

Depois de muito pensar, ela tem uma ideia. Envia-lhe um cofre fechado com um cadeado. Sabe que Bob é esperto e acabará por perceber sua ideia. Com mais uma ida e volta do correio, e sem nunca terem trocado chaves, a mensagem chega até Bob, que abre o cofre e a lê. Como é que você acha que resolveram o problema? Pense bem no assunto, tente responder a questão. É simples... depois que você descobrir, é claro.

O "truque" usado foi o seguinte: Bob colocou outro cadeado no cofre e ele tinha a chave desse segundo cadeado. Devolve o cofre a Alice por correio, desta vez fechado com os dois cadeados. Alice remove o seu cadeado, com a chave que possui e reenvia o cofre pelo correio só com o cadeado colocado por Bob. É claro que Bob tem apenas que abrir o cofre, com a sua própria chave e ler a mensagem enviada pela sua amada. O carteiro não tem como saber o conteúdo do cofre.

Figura 7 – Esquema da troca de cadeados.



Fonte: http://www.youtube.com/watch?v=pEfEgCEKcJ0

A historia de Bob e Alice mencionada acima se trata de um truque simples, mais retrata a necessidade que se tinha de se esconder algo para que terceiros não descobrissem a mensagem. Assim a criptografia foi ganhando cada vez mais força e sendo aperfeiçoada, de tal modo que se tornava cada vez mais complicada descobrir o segredo para conseguir descriptografar mensagens interceptadas.

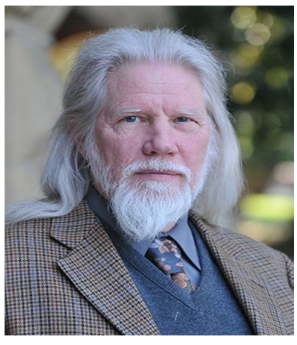
O filme *O jogo da imitação* (2014) retrata como foi importante o papel da criptografia durante a segunda guerra mundial. O matemático britânico Alan Turing o protagonista do filme teve um papel decisivo no fim do combate, pois junto com um grupo de superdotados o qual ele comandou conseguiu decifrar o código do Enigma, sistema criptográfico usado pelas forças alemãs para transmitir mensagens a seus homens em campo de batalha, tal feito só foi possível graças a uma construção de uma máquina. Historiadores estimam que esse feito de Alan Turing, encurtou a guerra em aproximadamente dois anos, poupando milhões de vidas, tal fato que só foi reconhecido mais de 50 anos depois, quando foi perdoado pela Rainha Elizabeth II, pela prática homossexual, que era considerada crime naquela época.

4.3.1 CRIPTOGRAFIA DE DIFFIE-HELLMAN

Com o passar do tempo tornava-se necessário inventar novos códigos, que fossem difíceis de decifrar e pudesse transmitir mensagens com mais seguranças, e uma dessas formas foi à utilização da troca de chaves, método específico desenvolvido por Whitfield Diffie e Martin Hellman.

Whitfield Diffie nasceu em 1944, Nova York, Estados Unidos e ficou muito conhecido pela descoberta do conceito de chave pública com Martin Hellman. Desde novo apresentou encanto pela matemática; formou-se em matemática no Massachusetts Instituteof Technology – MIT. Diffie percebeu que a criptografia se tornaria uma ferramenta essencial e que o problema da distribuição da troca de chaves, deveria ser solucionado. Ele ficou a procura da solução do problema da troca de chaves.

Figura 8 – Whitfield Diffie.



Fonte: http://cisac.fsi.stanford.edu/people/whitfield_diffie

Martin Hellman nasceu 1945, Nova York, Estados Unidos. Por ser judeu sofreu diversas formas de perseguições e discriminações ao longo da vida. Ele lembra que queria ser como os outros meninos, mas percebeu que não poderia ser, daí adotou uma postura defensiva. Ele conta que este foi um dos motivos pelos quais começou a se interessar pela criptografia.

Os colegas o chamavam de louco por fazer pesquisa de criptografia, concorrer com a National Security Agency (NSA), uma agência bilionária, e julgar que pudesse descobrir algo sem que eles soubessem? Sem falar que a NSA se apoderaria da descoberta e a classificaria como secreta.

Figura 9 – Martin Hellman.

Fonte: Wikipédia (2015)

Em 1974 Diffie procurou Hellman para conversar sobre o assunto que era comum a ambos, a partir de então se tornaram grandes amigos e companheiros. E juntos, começaram a estudar o problema da distribuição de chaves.

Por volta de 1976 o algoritmo inventado por Whitfield Diffie e Martin Hellman colocou a aritmética modular a serviço da criptografia, que ficou conhecido como a criptografia de Diffie-Hellman. A função utilizada é a seguinte $\boldsymbol{n^x}$ **(mod** $\boldsymbol{m}$**)**, com n e $m \in \mathbb{N}$ e $n < m$, permitindo a troca de chaves com segurança, sem haver a necessidade da contratação de pessoas de confiança.

A troca dessas chaves é feita da seguinte maneira: (Utilizando como personagens dessa história, João e Maria) primeiramente João e Maria escolhem dois valores para n e m sem se importar com a segurança na divulgação desses dois valores, ou seja, seriam valores públicos. Por exemplo: João e Maria combinam entre si $n = 7$ e $m = 11$, criando assim uma

função 7^x (mod 11). Depois cada um escolhe um número que será secreto para si; João escolhe o número 3 e Maria escolhe o número 4. Depois seguem os seguintes passos:

1º - João substitui o *x* por 3 na função, obtendo $7^3 \equiv 2$ (mod 11);

2º - Maria substitui o *x* por 4 da função, obtendo $7^4 \equiv 3$ (mod 11);

3º - João e Maria trocam os números obtidos entre si;

4º - João troca o *n* da função pelo número enviado por Maria que no caso foi o número 3 e substitui novamente *x* por 3, daí temos:

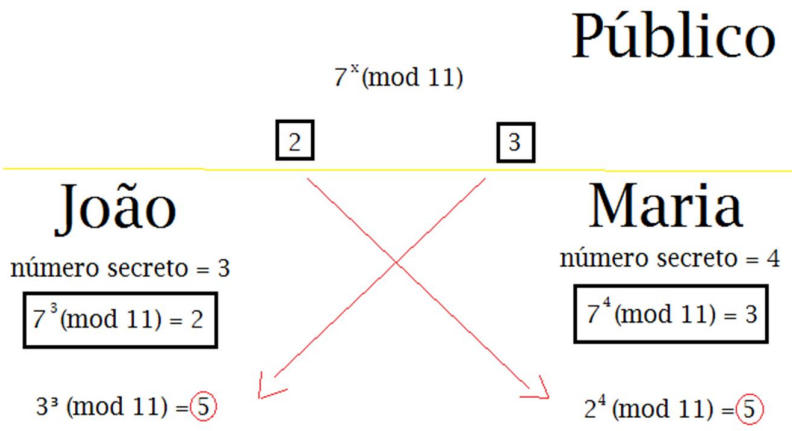
$3^3 \equiv 5$ (mod 11);

5º - Maria troca o *n* da função pelo número enviado por João que no caso foi o número 2 e substitui novamente *x* por 5, daí temos:

$2^4 \equiv 5$ (mod 11);

A chave secreta encontrada é o número 5, que será usado para trocar mensagens criptografadas entre si. O interessante que os números são trocados sem qualquer segurança e se obtém uma chave secreta!

Figura 10 – Ilustração da troca de chaves.



Fonte: Autor (2015)

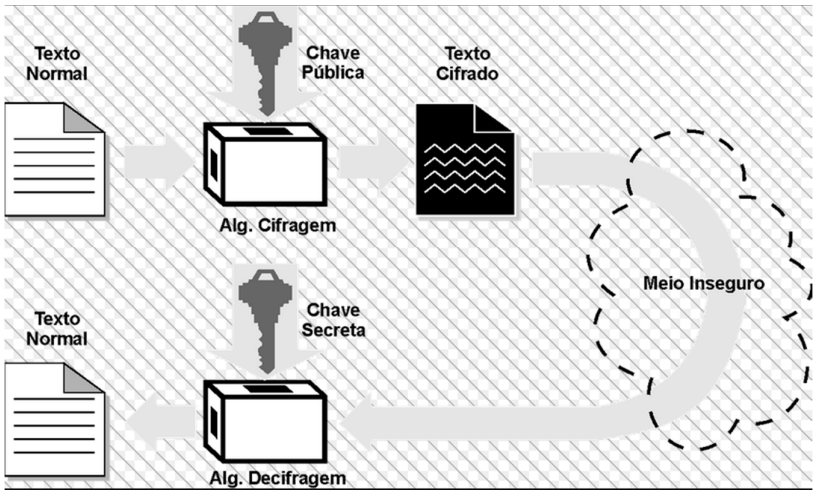
O segredo para João e Maria obterem as mesmas chaves de segurança está no 4º e 5º passos, quando eles trocam os números da base é como eles tivessem pegue a operação realizada pelo o outro. Por exemplo, no 4º passo João pega o 3 fornecido por Maria, mais esse 3 veio da operação $7^4 \equiv 3$ (mod 11), ou seja, é como João fizesse no final a seguinte conta: $(7^4)^3 = 7^{12}$; Maria seguindo os mesmos passos chega no final a seguinte conta: $(7^3)^4 = 7^{12}$.

Portanto a explicação para que Maria e João cheguem ao mesmo número, pois $(7^4)^3 \equiv (7^3)^4 \pmod{m}$.

Alguém que tenha escutado toda a conversa entre João e Maria só terá as informações sobre a função $7^x \pmod{11}$ e os números trocados entre si, 2 e 3; no entanto não sabendo os números escolhidos por João e Maria que foram secretos; o que impede a descoberta da chave que foi obtida por eles, devido a função não ser injetiva. Aqui no exemplo escolhemos números pequenos, para uma melhor compreensão do leitor. Para obtermos uma chave mais segura utilizamos números muito grandes para dificultar a tentativa e erro de alguém que deseja obter a chave para a criptografia.

Agora como funciona a criptografia de Diffie-Hellman: após a obtenção da chave secreta, já vista no algoritmo acima, é divulgada de forma pública uma chave para cifrar a mensagem original, possibilitando o uso de qualquer pessoa, agora essa mensagem cifrada, só é decifrado com o uso de uma chave secreta, esse tipo de processo é chamada de criptografia assimétrica onde existe uma chave pública para codificar e outra secreta para decodificar. A ilustração a seguir revela como funciona esse processo.

Figura 11 – Criptografia por chave pública.



Fonte: http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm

É claro que o tema da criptografia é muito mais amplo do que foi abordado, existindo vários outros modelos de criptografias, como já mencionado, é um assunto que está sempre se renovando, devido à procura de cada vez mais, manter conversas de maneira sigilosa. Por exemplo, as transações envolvendo dinheiro são feitas de maneira eletrônica, via

internet e essas informações correm o risco de serem interceptados pelos conhecidos “hackers”.

A criptografia RSA é hoje a mais utilizada devido a sua grande complexidade de codificar e decodificar e é claro de decifrar, ou seja, ‘quebra’ de código, se tornando uma das mais confiáveis e seguras. A criptografia RSA tomou como base a criptografia de Diffie-Hellman, porém usando outro método matemático para a criação das chaves públicas. Eles utilizam o fato de que é fácil obter o resultado de uma multiplicação de dois números primos extensos, porém muito difícil de fazer o processo inverso, ou seja, obter os fatores primos de um número muito extenso. Que pode ser lida de uma maneira mais esclarecedora no livro de COUTINHO.

Observamos que no mundo atual é imprescindível que determinadas informações trafeguem de forma em aberto por esses meios de comunicações como a internet, para isso é necessário o uso da criptografia, para que as mesmas sejam codificadas de tal maneira que somente o destinatário consiga ler a mensagem de forma correta, após decodifica-la.

O que mostramos através de criptografia de Diffie-Hellman, foi à relação existente entre o cotidiano e o conteúdo de congruência modular. Como o assunto é bem atual e interessante, principalmente para os mais novos que vivem no meio de comunição cada vez mais evoluído. O que facilitaria o processo de ensino de matemática na educação básica, pois relaciona conceitos importantes como, divisibilidade, funções e operações inversas.

5 DISCUSSÃO

Durante o período da realização desse trabalho, ocorreu uma preocupação em usar uma linguagem de fácil interpretação nas partes de fundamentação teórica. Foram apresentados, conceitos, definições, propriedades, sempre com a utilização de exemplos, possibilitando ao leitor maneiras diferentes de compreender o tema abordado. Portanto a preocupação de abordar assuntos sempre apoiado em problemas que serviram de exemplos, para assim entender a sua aplicabilidade de uma maneira clara, tanto de forma teórica como de forma pratica.

O processo de pesquisa bibliográfica foi bastante proveitoso, com acréscimos de assuntos novos de muita utilidade. Foram também encontrados vários trabalhados relacionados à minha área de pesquisa, gerando um trabalho de filtro, onde foi preciso fazer uma seleção dos assuntos de maior relevância, aqueles que iriam trazer uma maior curiosidade e interesse ao leitor.

6 CONSIDERAÇÕES FINAIS

Foi visto por meio de congruência modular, que podemos resolver determinados problemas de matemática de uma maneira ágil e eficaz.

Sabemos das diversas dificuldades presentes no ensino da matemática, com isso procurou-se desenvolver nesse trabalho técnicas de aulas mais atrativas, através de assuntos que provoquem curiosidade ou que esteja diretamente ligado ao seu dia-a-dia, que é o caso do dígito de verificação presente no CPF, código de barras e em várias outras sequências numéricas. Também apresentamos outras técnicas envolvendo congruência modular de bastante utilidade, como os critérios de divisibilidade, que facilitam o processo da divisão e uma parte da criptografia que se utiliza de ferramentas matemáticas para conseguir fazer o processo de troca de mensagens de maneira secreta e segura.

Observando assim à importância da divisão Euclidiana, como sendo ferramenta principal, onde se apoia toda a base do trabalho, tendo como requisito básico para poder compreender o desenvolvimento apresentado.

Espero que após a leitura desse trabalho, professores possam se apoiar nesse material para o melhoramento de suas aulas no ensino básico, de uma maneira mais prazerosa aos alunos, através das aplicações. Sei da dificuldade de se mudar a estrutura curricular do ensino básico, mais a ideia é que este assunto de congruência modular possa ser inserido de uma maneira que sirva como apoio a assuntos relacionados.

Neste trabalho foram vistos algumas aplicações de congruência modular, mas é fato que existem outras aplicações como o interessante Teorema Chinês do Resto, que não vimos mais que pode ser visto no livro do HEFEZ e também a aplicação de congruência modular que está presente no calendário gregoriano, onde se mostrar as relações entre os dias da semana, dos meses e anos que é muito útil e que pode ser lido na dissertação de MELO.

REFERÊNCIAS

BARBOSA JUNIOR, J. H. Congruências modulares: construindo um conceito e as suas aplicações no ensino médio. 2013. 51f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Sergipe, São Cristóvão. 2013.

BIGODE, Antônio José Lopes; GIMENEZ, Joaquim. Metodologia para o ensino da aritmética: competência numérica no cotidiano. São Paulo: FTD, 2009.

CORREA, J. A compreensão intuitiva da criança acerca da divisão partitiva de quantidades contínuas. Estudos de Psicologia, Rio de Janeiro, v. 5, n. 1, p. 11-31, 2000. Disponível em: <http://www.scielo.br/pdf/epsic/v5n1/a02v05n1.pdf>. Acesso em: 20 fev. 2015.

COUTINHO, Severino Collier. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2013.

CRATO, Nuno. Alice e Bob. Expresso / Revista, 22 de setembro, pp. 118-120. (2001).

DOMINGUES, Hygino H. Fundamentos de aritmética. São Paulo: Atual, 1991.

ESQUINCA, J. C. P. Aritmética: códigos de barras e outras aplicações de congruências. 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Mato Grosso do Sul, Campo Grande. 2013.

HEFEZ, Abramo. Elementos Aritméticos. 2.ed. Rio de Janeiro: SBM, 2011.

JOGO da Imitação, O. Direção: Morten Tyldum. Produção: Nora Grossman, Ido Ostrowsky e Teddy Schwarzman, 2014. 114 min.

MARQUES, T. V. Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula. 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal da Paraíba, João Pessoa. 2013.

MELO, C. B. A matemática dos restos e o calendário gregoriano. 2014. 55f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Ceará, Juazeiro do Norte. 2014.

MUNIZ NETO, Antonio Caminha. Tópicos de Matemática Elementar: teoria dos números. 1.ed. Rio de Janeiro: SBM, 2012.

PAENZA, Adrián. Matemática, cadê você?: sobre números, personagens, problemas e curiosidades. Rio de Janeiro: Civilização Brasileira, 2009.

SANT'ANNA, I. K. A aritmética modular como ferramenta para as séries finais do ensino fundamental. 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Instituto de Matemática Pura e Aplicada, Rio de Janeiro. 2013.

SANTALÓ, Luis Antonio. A matemática para não matemáticos. In: PARRA, Cecília. (Org.). Didática da Matemática: Reflexões Psicopedagógicas. Porto Alegre: Artes Médicas, 1996.

SANTOS, P. S. A. Congruência e equações diofantinas lineares: uma proposta para o ensino básico.2013. 111f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Alagoas, Maceió. 2013.

SINGH, Simon. O livro dos códigos. 6.ed. Rio de Janeiro: Record, 2007.

TRINTA, F. A. M; MACÊDO, R. C. Um estudo sobre Criptografia e Assinatura Digital. 1998. Departamento de informática, Universidade Federal de Pernambuco. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em 25 fev. 2015.