**UNIVERSIDADE FEDERAL DO PARÁ**
**INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS**
**PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL**

**FRANCISCO ANDRÉ LIMA ARAÚJO**

# DIVISIBILIDADE E CONGRUÊNCIA DE NÚMEROS INTEIROS NO ENSINO BÁSICO

**BELÉM – PA**
**2020**

**FRANCISCO ANDRÉ LIMA ARAÚJO**

# DIVISIBILIDADE E CONGRUÊNCIA DE NÚMEROS INTEIROS NO ENSINO BÁSICO

Dissertação apresentada ao Programa de Pós-graduação PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) na Universidade Federal do Pará oferecido em associação com a Sociedade Brasileira de Matemática, como requisito para obtenção do Título de Mestre em Matemática.

**BELÉM – PARÁ**

**2020**

**Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD**
**Sistema de Bibliotecas da Universidade Federal do Pará**
**Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)**

---

A658d Araújo, Francisco André Lima.
Divisibilidade e congruência de números inteiros no ensino básico / Francisco André Lima Araújo. — 2020.
76 f. : il.

Orientador(a): Prof. Dr. Augusto César dos Reis Costa
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática em Rede Nacional, Belém, 2020.

1. Aritmética modular. 2. Divisibilidade do ensino básico. 3. Congruência no ensino básico. I. Título.

CDD 513.6

---

**FRANCISCO ANDRÉ LIMA ARAÚJO**

# DIVISIBILIDADE E CONGRUÊNCIA DE NÚMEROS INTEIROS NO ENSINO BÁSICO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT) do Departamento de Matemática da Universidade Federal do Pará, como parte dos requisitos para obtenção do título de Mestre em Matemática.

## COMISSÃO EXAMINADORA

Data da defesa: 16/11/2020.

Conceito:...Aprovado.....

---

**Prof. Dr. Augusto César dos Reis Costa - UFPA (Orientador)**

---

**Prof. Dr. Geraldo Mendes de Araújo - UFPA (Membro interno)**

---

**Prof. Dr. Joao Claudio Brandemberg Quaresma – UFPA (Membro externo)**

# Dedicatória

Dedico esta dissertação a minha esposa Jéssica Araújo, que foi meu alicerce em toda essa caminhada, me dando, todo o suporte necessário para que eu pudesse me dedicar ao curso. Dedico também aos meus filhos Paulo André Araújo e Ana Clara Araújo, que com certeza são minhas maiores motivações para concluir esse mestrado e assim buscar novos horizontes.

**Francisco André Lima Araújo**

# Resumo

O presente trabalho é voltado para alunos e professores que atuam no ensino básico. Tem como objetivo mostrar que é possível falar de congruência de números inteiros já nesse nível de ensino, buscando facilitar a resolução de diversas situações-problema. A motivação para escolher esse tema é o fato de diversos resultados relacionados ao tema poderem ser associados a vários conteúdos estudados no ensino básico, podendo assim auxiliar os alunos em diversos exercícios, que inclusive, comumente, são propostos em provas de admissão e em olimpíadas de Matemática.

Inicialmente, no capítulo 1 é feita uma abordagem simples sobre o algoritmo da divisão euclidiana, destacando o significado de dividir um número por outro, além disso, começamos a introduzir a notação da congruência módulo m, para resolver alguns problemas envolvendo divisibilidade e também para justificar os critérios de divisibilidade. No capítulo 2, são apresentados alguns resultados que podem servir como arcabouço teórico na resolução de diversos problemas envolvendo divisibilidade, também abordamos as equações diofantinas lineares com duas incógnitas, cujo objetivo é associa-la aos sistemas lineares que são estudados pelos alunos do ensino básico a partir do 8º ano. No capítulo 3 apresentamos diversos problemas, que são do cotidiano dos alunos, e que podem ser resolvidos de forma mais eficiente usando os conceitos apresentados no capítulo 2.

Por fim, no capítulo 4, apresentamos algumas aplicações cotidianas da congruência dos números inteiros, por exemplo, nos sistemas de identificação como o CPF.

**Palavras-chave:** congruência, divisibilidade, Ensino básico, Resolução de problemas.

# Abstract

The present work is aimed at students and teachers working in basic education. It aims to show that, at this level of education, we may present modular integer congruence, and its use to facilitate resolution of various problems. The motivation for choosing this theme is the fact that many such results can be associated with contents studied in basic education, and thus assist students in various exercises, which are commonly proposed in admission tests and in Math Olympics contests as well.

Initially, in chapter 1 a simple presentation is made concerning the Euclidean division algorithm, highlighting the meaning of dividing one number by another. In addition, we start to introduce the congruence notation module *m*, when solving certain problems involving divisibility, and also to justify divisibility criteria. In chapter 2, results are presented that can serve as a theoretical framework for resolving various problems involving divisibility. We also address linear Diophantine (polynomial) equations with two unknowns, the objective is to create associations with the linear systems studied by elementary school students from the 8th grade onwards. In chapter 3 we present various typical problems from the students' daily lives which can be solved more efficiently using the concepts presented in chapter 2.

Finally, in chapter 4, we present everyday applications of the modular congruence of integers, for example, in identification systems such as the National Registry (CPF).

**Keywords:** congruence, divisibility, basic education, problem solving.

# Sumário

# Introdução

A ideia de escrever sobre o tema “divisibilidade” surgiu ainda na graduação, em Licenciatura em Matemática, cursada na Universidade Federal do Pará (UFPA), quando ficou evidente a grande diferença do estudo dos conteúdos de Aritmética básica e da divisibilidade que nos é ofertado no ensino superior e a forma simplificada e diferente como estes conteúdos nos são apresentados na Educação Básica. Diante de tamanha discrepância fica evidente a necessidade de se introduzir alguns desses conceitos, estudados no ensino superior, já na educação básica.

A Educação Básica, a partir da Lei de Diretrizes e Bases da Educação (LDB - 9.394/96), passou a ser estruturada por etapas e modalidades de ensino, englobando a Educação Infantil, o Ensino Fundamental obrigatório de nove anos (Ensino fundamental 1 e 2) e o Ensino Médio. Em todo esse espaço de aprendizagem, a Matemática ocupa um lugar de destaque, visto que junto com a habilidade inerente à leitura e escrita, constitui como uma das aprendizagens mais fundamentais, de extrema necessidade para o ser humano. Isso porque a matemática proporciona ao homem um preparo para vida, que nenhuma outra disciplina pode oferecer.

A aritmética é o ramo mais elementar da matemática. É a parte da matemática que lida com cálculos como a adição, a subtração, a multiplicação e a divisão. Todos os outros ramos da matemática utilizam os princípios e as regras da aritmética. Com isso, quando os princípios básicos da aritmética não estão suficientemente consolidados, é que surgem os problemas da matemática, visto que, as pessoas usam a aritmética todos os dias. Ela é usada quando compramos ou vendemos algo, quando damos ou recebemos troco, quando desejamos medir velocidades, quantificar ou ainda contar algo.

O termo “aritmética” vem da palavra grega arithmos, que significa “número”. É bastante discutido como o ensino de matemática apresenta tantas rupturas, evidenciado pela insuficiente fundamentação aritmética. O grande exemplo disso pode ser verificado pelo baixo desempenho dos alunos, bem como nas dificuldades que esses vêm enfrentando no cotidiano. A busca por respostas para o problema evidenciado é o que discutiremos nesse trabalho, mostrando a importância de se

introduzir um estudo mais profundo da aritmética modular já no ensino básico. Neste trabalho veremos como a Aritmética Modular, seus conceitos e propriedades podem contribuem para a dinâmica da vida moderna, mostrando suas várias aplicabilidades no dia a dia, por exemplo, nos diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, criptografias, calendários entre outros.

# Capítulo 1

## Uma abordagem da divisibilidade e congruência no ensino básico.

### 1.1 Divisão euclidiana: definição e princípios.

A divisão euclidiana, também conhecida como divisão inteira ou divisão com resto, é um assunto essencial dos conteúdos de matemática nos primeiros anos de aprendizado, mas que nem sempre é dominado logo nas aulas iniciais.

*"Eu tenho cerca de 20 maçãs e três filhos. Quantos frutos cada um receberá?"*

Esta é a famosa operação que usa dois inteiros – dividendo e divisor – e associa dois outros: o quociente e o resto. É definido que todos os números inteiros podem ser divididos por outro inteiro diferente de zero (≠ 0) e ter como resultado um quociente inteiro e um resto, no qual o resto sempre deve ser maior ou igual a zero e menor que o divisor.

**Exemplo1.1**

Vamos efetuar a divisão 478 por 7.

$$\begin{array}{r|l} 478 & 7 \\ \cline{2-2} -\,42\downarrow & 68 \\ \cline{1-1} 58 & \\ -\,56 & \\ \cline{1-1} 2 & \end{array}$$

**Figura1.1**

Assim podemos concluir que $478 = 7.68 + 2$, em que:

$\mathbf{478}$ é o dividendo (número que se quer dividir)

$\mathbf{7}$ é o divisor (número por quem se quer dividir)

$\mathbf{68}$ é o quociente (número que representa, quantas vezes, o $\mathbf{7}$ "cabe" em $\mathbf{478}$)

**2** é o resto (número que representa quanto "falta" para completar $\mathbf{478}$).

**Exemplo1.2**

Vamos efetuar a divisão 134 por 8.

$$\begin{array}{r|l} 134 & 8 \\ \cline{2-2} -\ 8\downarrow & 16 \\ \cline{1-1} 54 & \\ -\ 48 & \\ \cline{1-1} 6 & \end{array}$$

**Figura1.2**

Assim podemos concluir que $134 = 8.16 + 6$, em que:

$\mathbf{134}$ é o dividendo (número que se quer dividir)

$\mathbf{8}$ é o divisor (número por quem se quer dividir)

$\mathbf{16}$ é o quociente (número que representa, quantas vezes, o $\mathbf{8}$ "cabe" em $\mathbf{134}$)

$\mathbf{6}$ é o resto (número que representa quanto "falta" pra completar $\mathbf{134}$).

Desse modo, a partir do exemplo, podemos generalizar para concluir que no algoritmo da divisão Euclidiana, a divisão de $\boldsymbol{a}$ por $\boldsymbol{b}$, resulta num quociente $\boldsymbol{q}$ e um resto **r**, ou seja,

$$\begin{array}{r|l} \boldsymbol{a} & \boldsymbol{b} \\ \cline{2-2} \boldsymbol{r} & \boldsymbol{q} \end{array}$$

**Figura1.3**

tal que $a = b.q + r$, com $0 \leq r < b$.

O algoritmo da divisão Euclidiana é aprendido como uma das quatro operações básicas da matemática, já nas aulas dos anos iniciais do ensino fundamental. Quando abordamos os números naturais, sabemos que o emprego de um algoritmo é uma estratégia para chegar à solução de alguns problemas, mas o que observamos é que não há uma compreensão dos alunos acerca dos conceitos envolvidos; o que também é destacado pelos Parâmetros Curriculares Nacionais (PCN):

> *Embora o estudo dos números e das operações seja um tema importante no currículo do ensino fundamental, constata-se, com frequência, que muitos alunos chegam ao final dessa fase de formação, com um conhecimento insuficiente sobre como eles são utilizados e sem ter desenvolvido uma ampla compreensão dos diferentes significados das operações. (BRASIL, 1998, p. 95)*

Uma grande preocupação por parte dos professores – que nem sempre tem feito sentido – é o de achar que quando um aluno opera com rapidez e facilidade um algoritmo, este apresenta compreensão daquela ideia. Como confirmam Correa e Spinillo,

> *O entendimento dos conceitos de multiplicação e divisão é, muitas vezes, confundido com a competência em operar os algoritmos usados para multiplicar ou dividir. Fazer contas com precisão torna-se, assim, o critério usado pelo professor para avaliar compreensão que seus alunos têm sobre esses conceitos.*
>
> *(CORREA e SPINILLO, 2004, p.105).*

As ideias relacionadas a divisão precisam está bem esclarecidas para os alunos, para que eles possam dar significado ao cálculo que irão executar. É preciso discutir qual o significado de dividir, explicar que quando falamos em divisão, sempre queremos dividir em partes iguais e de modo que sobre o menor resto possível. Um ponto que podemos destacar é o fato de a divisão estar ligada a duas ideias diferentes: repartitivas ou de partilha e a subtrativa ou de medida.

A seguir, exemplificaremos esses modelos, em algumas situações:

**Modelo repartitivo ou de partilha:** Hoje é o dia do aniversário de Raquel! Ela quer dar bolinhas de gude como lembrancinhas a seus convidados. Raquel comprou 42 bolinhas para distribuir entre 5 crianças convidadas. Ajude a menina a montar saquinhos com o mesmo número de bolinhas em cada um.

**Subtrativo ou de medida:** Tenho 45 figurinhas e quero fazer pacotes com 5 figurinhas cada um. Quantos pacotes poderei fazer?

É fácil concluir que ambas as situações serão resolvidas pela operação de divisão, mas elas compreendem ações cognitivas diferentes. Na primeira situação, as bolinhas de gudes que foram divididas entre os amiguinhos, resulta em um total de 8 bolinhas de gude para cada amiguinho, ou seja, iremos descobrir quantos elementos há em cada grupo formado. Na segunda situação, as figurinhas divididas em grupos de 5, resulta em um total de 9 pacotes, ou seja, considerando o exemplo dado, quantos grupos de 5 figurinhas “cabem” ou “estão contidos” em 45 figurinhas. Esses modelos devem ser bem entendidos e é importante que sejam trabalhados em sala de aula, pois refletem na compreensão do algoritmo tradicional da divisão.

De acordo com a BNCC (Base Nacional Comum Curricular), o estudo da divisão deve ser iniciado no 2° ano do ensino fundamental (ensino fundamental 1), com ideias de metade e terça parte, como pode ser observado na habilidade a seguir, retirada do documento oficial da BNCC (*Disponível em http://basenacionalcomum.mec.gov.br/. Acesso em 8 de maio de 2020).*

**(EF02MA08)** Resolver e elaborar problemas envolvendo dobro, metade, triplo e terça parte, com o suporte de imagens ou material manipulável, utilizando estratégias pessoais. [p339].

Seu estudo começa a ser aprofundado no 3°e 4° ano, com a alusão explicita a divisão Euclidiana, observado nas habilidades:

**(EF03MA08)** Resolver e elaborar problemas de divisão de um número natural por outro (até 10), com resto zero e com resto diferente de zero, com os significados de repartição equitativa e de medida, por meio de estratégias e registros pessoais. [p243].

**(EF03MA09)** Associar o quociente de uma divisão com resto zero de um número natural por 2, 3, 4, 5 e 10 às ideias de metade, terça, quarta, quinta e décima partes. [p243].

**(EF04MA07)** Resolver e elaborar problemas de divisão cujo divisor tenha no máximo dois algarismos, envolvendo os significados de repartição equitativa e de medida, utilizando estratégias diversas, como cálculo por estimativa, cálculo mental e algoritmos. [p247].

**(EF04MA12)** Reconhecer, por meio de investigações, que há grupos de números naturais para os quais as divisões por um determinado número resultam **em restos iguais**, identificando regularidades. [p247].

**(EF04MA13)** “Reconhecer, por meio de investigações, utilizando a calculadora quando necessário, as relações inversas entre as operações de adição e de subtração e de multiplicação e divisão, para aplicá-las na resolução de problemas”. [p247].

No 5° ano a BNCC sugere que fração é o resultado de uma divisão, como pode ser observado na habilidade a seguir:

**(EF05MA03)** Identificar e representar frações (menores e maiores que a unidade), associando-as ao resultado de uma divisão ou à ideia de parte de um todo, utilizando a reta numérica como recurso. [p251].

No 6° ano é recomendada uma retomada das operações elementares com números naturais, como pode ser observado na habilidade a seguir:

**(EF06MA03)** Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora [p257].

Alertamos para o fato de que a Divisão Euclidiana deveria receber maior atenção no 6° ano, etapa em que o aluno ainda precisa “revisitar” esse conteúdo, objetivando seu aprofundamento e sua plena compreensão, de acordo com a orientação geral, tanto dos PCN [p81]. (*http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf. Acesso em 8 de maio de 2020)*, que recomendam explorar o conceito e a formalização da divisão ainda no 3° ciclo (6° e 7° ano), como também da BNCC [p255] de oportunizar-se, a cada ano escolar, não só uma retomada como também um aprofundamento do conteúdo.

## 1.2 Prática introdutória de congruência em sala de aula para alunos da educação básica.

Uma das ferramentas mais importantes na teoria dos números é o conceito de congruência. Uma congruência é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Por exemplo, o número 9 é congruente ao número 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2\ mod\ 7$. Foi o brilhante Gauss que observou que usávamos com muita frequência frases do tipo

“a dá o mesmo resto que b quando divididos por m” e que essa relação tinha um comportamento semelhante à igualdade. Foi Gauss então que introduziu uma notação específica para este fato e que denominou de “congruência”.

Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O que não é muito comum é o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme veremos adiante.

É um tema bastante atual e que pode ser trabalhado já nas classes do Ensino básico e gerador de excelentes oportunidades de contextualização no processo de ensino / aprendizagem de matemática.

Antes de apresentar as definições e propriedades relacionadas à congruência, vamos desenvolver três exemplos que poderiam ser colocados a alunos da Educação Básica, ainda não familiarizados com o tema, como introdução ao assunto.

**Exemplo 1.3**

Apresentando uma questão retirada do banco de questões do site da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas). Lá sempre se encontram questões interessantes e provocativas para o preparo de nossos alunos da Educação Básica.

**Enunciado:** 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?

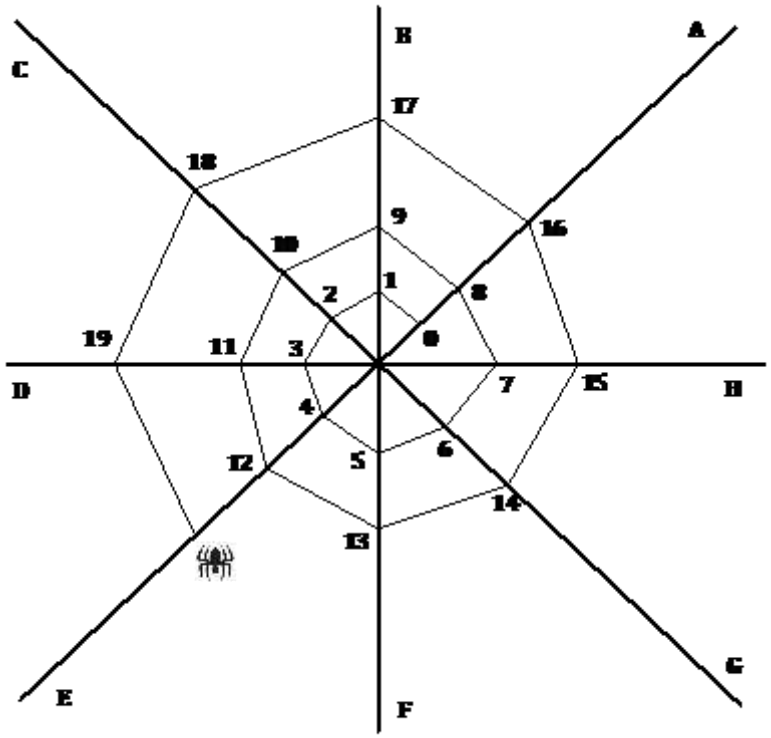


**Figura 1.4**

**Solução**

Podemos construir uma tabela na lousa, para mostrar o que está acontecendo...

| Fios | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| | ... | ... | ... | ... | ... | ... | ... | ... |

**Tabela1.1**

É claro que alguma pessoa bem paciente poderia continuar construindo a tabela até que aparecesse o número118. Assim ela saberia em qual fio a aranha iria estar. Convenhamos que não seria uma solução muito prática e nem rápida. Imagine

se perguntássemos a alunos em sala de aula qual o fio correspondente ao número 890?

Podemos fazê-los observar que os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentem de oito em oito. Mostraríamos também que cada fio pode ser representado a partir dos múltiplos de 8. O fio A corresponde aos números que são múltiplos de 8, ou seja, números que divididos por 8 deixam resto zero $8.n$, com $n \in \mathbb{Z}$). O fio B corresponde aos números que são múltiplos de 8, mais 1, ou seja, números que divididos por 8 deixam resto ($8.n + 1$, com $n \in \mathbb{Z}$.) O fio C corresponde aos números que são múltiplos de 8, mais 2, ou seja, números que divididos por 8 deixam resto 2, ($8.n + 2$, com $n \in \mathbb{Z}$) e essa lógica se mantém até o fio H, definido pelos números que divididos por oito deixam resto 7. É claro que para mostrarmos sobre qual fio estará a aranha quando estiver sobre a posição de número 118, basta verificarmos a qual dessas famílias tal número pertence e isso pode ser facilmente obtido ao dividirmos 118 por 8. Vejamos:

$$\begin{array}{r|l} 118 & 8 \\ \hline 6 & 14 \end{array}$$

**Figura1.5**

Verificamos que o número $118$ é igual a $8.14 + 6$, ou seja, pertence à família dos números que estão no fio G. A aranha estará sobre o fio G.

Todos os números de nosso exemplo, que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8 e são congruentes entre si, no módulo 8.

O número 14, por exemplo, é congruente ao número 22, no módulo 8, e isso significa que esses dois números deixam o mesmo resto quando divididos por 8 (verifique que ambos estão sobre o fio G). Verificando:

$$\begin{array}{r|l} 14 & 8 \\ \hline 6 & 1 \end{array} \qquad \begin{array}{r|l} 22 & 8 \\ \hline 6 & 2 \end{array}$$

**Figura1.6**

A notação usual para representar essa relação é $14 \equiv 22\ mod\ 6$, mas nesse momento não nos preocuparemos com maiores formalidades . Estamos apenas começando a introduzir o conceito de congruência.

**Exemplo1.4**

**Aritmética do relógio**

**Figura1.7**

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.

Assim as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12.

**Exemplo1.5**

Vejamos uma aplicação interessante sobre o tema, relacionada aos calendários:

Pediríamos para que os alunos levassem um calendário para mostrar mais uma aplicação das congruências. Como no exemplo da teia de aranha, seria montada uma tabela com os 7 primeiros dias do ano e seus respectivos dias da semana. Em 2008,

por exemplo, dia 1º de janeiro foi uma terça-feira e assim por diante. Imaginemos que desejássemos saber em qual dia da semana cairia um outro dia qualquer do ano. É só montar uma tabela para esses primeiros dias, que no caso ficaria assim:

| **DIAS DO MÊS DE JANEIRO** | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| **DIAS DA SEMANA** | Terça | Quarta | Quinta | Sexta | Sábado | Domingo | Segunda |

**Tabela1.2**

Verificamos aqui que estamos novamente diante de um caso de congruência, módulo 7 nesse caso. Digamos que pedíssemos para que descobrissem em que dia da semana cairá o dia 15 de outubro, sem que olhassem para o calendário. Primeiro precisamos ver quantos dias existem de 1º de janeiro até 15 de outubro. Vejamos:

| **MESES** | **DIAS** |
|---|---|
| Janeiro | 31 |
| Fevereiro | 29 |
| Março | 31 |
| Abril | 30 |
| Maio | 31 |
| Junho | 30 |
| Julho | 31 |
| Agosto | 31 |
| Setembro | 30 |
| Outubro | 15 |
| **TOTAL** | **289** |

**Tabela1.3**

Devemos lembrá-los que 2008 é um ano bissexto e que os anos bissextos possuem um dia a mais, no mês de fevereiro.

Agora, é como se tivéssemos uma fila de 289 dias e estamos desejando saber, na congruência de módulo 7 (7 dias da semana) qual o correspondente ao 289.

Estaríamos diante de uma situação bem semelhante à que vimos no problema da aranha e também no problema dos relógios analógicos.

Ao dividirem 289 por 7 teriam:

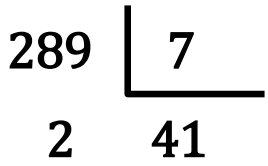


**Figura1.8**

Logo, 289 é congruente a 2, no módulo 7. Isso quer dizer que o 289º dia do ano (dia 15 de outubro) cairá no mesmo dia da semana do dia 2 de janeiro. Como o dia 2 de janeiro de 2008 foi uma quarta-feira, conforme a tabelinha, o 289º dia de 2008 também cairá numa quarta-feira. Portanto, dia 15 de outubro cairá numa quarta-feira.

Assim, com os três exemplos que mostramos, os alunos observariam que em nosso cotidiano existem inúmeras situações onde se faz presente a noção de congruência, módulo k. Calendários, relógios analógicos e problemas em geral envolvendo repetições periódicas.

## 1.3 Ensino de divisibilidade utilizando o conceito de congruência modulo m.

Dando um outro enfoque aos “critérios de divisibilidade”, parece ser possível, valendo-se da linguagem usada na congruência modular, transmitir as ideias por trás da palavra “congruência” para alunos de 6° ou 7° ano e, a partir destas ideias, calcular os **restos** de uma divisão por 2, 3, 4, 5, etc. e mostrar o porquê dos critérios de divisibilidade, através de **congruências modulo m**, quando obtemos resto zero.

### 1.3.1 Divisibilidade por 2.

Vamos utilizar a notação de **“congruência modulo m”** que já pode ser compreendida pelos alunos das séries iniciais (6° e 7° anos):

$$a \equiv b \; mod \; 2.$$

Dizemos que "$a$ é congruente a $b$ módulo 2" e escrevemos $a \equiv b \; mod \; 2$, se $a$ e $b$ deixam o mesmo resto quando divididos por 2.

**Observação:** Se $a$ e $b$ não deixam o mesmo resto na divisão por 2, dizemos então que $a \not\equiv b \; mod \; m$ (Lemos "$a$ não é congruente a $b$ módulo 2").

**Exemplo1.6**

$0 \equiv 2 \; mod \; 2$, pois $2 \div 2 = 1$ e resto $0$; $0 \div 2 = 0$ e resto $0$ também.

$2 \equiv 4 \; mod \; 2$, pois $4 \div 2 = 2$ e resto $0$; $2 \div 2 = 1$ e resto $0$ também.

Dessa forma, $0 \equiv 2 \; mod \; 2, \; 2 \equiv 4 \; mod \; 2, \; 4 \equiv 6 \; mod \; 2, \; 6 \equiv 8 \; mod \; 2$,..., ou seja, todos os números pares são "congruentes módulo 2" porque deixam resto $0$ quando divididos por 2. Podemos escrever $0 \equiv 2 \; mod \; 2$, $2 \equiv 4 \; mod \; 2$, $4 \equiv 6 \; mod \; 2$, $6 \equiv 8 \; mod \; 2$ , da seguinte forma resumida: $0 \equiv 2 \equiv 4 \equiv 6 \equiv 8 \; mod \; 2$.

**Exemplo1.7**

$1 \equiv 3 \; mod \; 2$, pois $3 \div 2 = 1$ e resto $1$,e $1 \div 2 = 0$ e resto $1$, também.

$3 \equiv 5 \; mod \; 2$, pois $5 \div 2 = 2$ e resto $1$ e $3 \div 2 = 1$ e resto $1$ também.

Dessa forma, $1 \equiv 3 \; mod \; 2, \; 3 \equiv 5 \; mod \; 2, \; 5 \equiv 7 \; mod \; 2, \; 7 \equiv 9 \; mod \; 2$,..., ou seja, todos os números ímpares são "congruentes módulo 2" porque deixam resto 1 quando divididos por 2. Podemos escrever $1 \equiv 3 \; mod \; 2$, $3 \equiv 5 \; mod \; 2, \; 5 \equiv 7 \; mod \; 2$, $7 \equiv 9 \; mod \; 2$, da seguinte forma resumida: $1 \equiv 3 \equiv 5 \equiv 7 \equiv 9 \; mod \; 2$.

Generalizando, todos os números naturais são "congruentes módulo 2" a 0 ou 1.

Agora, podemos usar as operações de adição e multiplicação na "congruência módulo 2", observe:

**Exemplo1.8**

Considere $2 \equiv 4\ mod\ 2$ e $6 \equiv 8\ mod\ 2$. Somando as congruências, temos:

$$2 + 6 \equiv 4 + 8\ mod\ 2, \text{ isto é, } 8 \equiv 12\ mod\ 2.$$

Multiplicando as igualdades, temos:

$$2.6 \equiv 4.8\ mod\ 2, \text{ isto é, } 12 \equiv 32\ mod\ 2.$$

Em geral,

Se $a \equiv b\ mod\ 2$,e $c \equiv d\ mod\ 2$, então $\begin{cases} a + c \equiv b + d\ mod\ 2 \\ e \\ a.c \equiv b.d\ mod\ 2 \end{cases}$

Sabemos que um número é divisível por 2 quando ele é terminado por um número par. Fazendo uso das "igualdades módulo 2", podemos mostrar agora o porquê disso.

**Exemplo 1.9**

Tomemos o número 692. Podemos escrevê-lo da seguinte forma:

$$692 = 600 + 90 + 2$$
$$692 = 6.100 + 9.10 + 2$$
$$692 = 6.10^2 + 9.10 + 2.$$

Porém,

$$10 \equiv 0\ mod\ 2 \text{ e } 10^2 \equiv 0\ mod\ 2.$$

Então,

$$692 \equiv 6.0 + 9.0 + 2\ mod\ 2 \Rightarrow 692 \equiv 2\ mod\ 2.$$

Como, $2 \equiv 0\ mod\ 2$, então $692 \equiv 0\ mod\ 2$.

**Exemplo1.10**

Vejamos o que acontece aplicando-se procedimento análogo ao número 1159:

$$1159 = 100 + 100 + 50 + 9$$
$$1159 = 1.1000 + 1.100 + 5.10 + 9$$
$$1159 = 1.10^3 + 1.10^2 + 5.10 + 9.$$

Da mesma forma que o exemplo anterior,

$$10 \equiv 0\ mod\ 2,\ 10^2 \equiv 0\ mod\ 2 \text{ e } 10^3 \equiv 0\ mod\ 2.$$

Logo,

$$1159 = 1.0 + 1.0 + 5.0 + 9 \Rightarrow 1159 \equiv 9\ mod\ 2.$$

Como,

$$9 \equiv 1\ mod\ 2.$$

Então,

$$1159 \equiv 1\ mod\ 2.$$

Daí, percebemos porque basta observar o algarismo das unidades para saber se um número é divisível por 2 ou não. Se o algarismo das unidades for igual a 0 módulo 2, deixa resto 0 e será divisível por 2 (pares); se for igual a 1 módulo 0, deixará resto 1 ao ser dividido por 2 (ímpares).

### 1.3.2 Divisibilidade por 3.

Dizemos que "$a$ é congruente a $b$ módulo 3" e escrevemos $a \equiv b\ mod\ 3$, se $a$ e $b$ deixam o mesmo resto quando divididos por 3.

A partir desta definição, teremos:

$$0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots mod\ 3$$

$$1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots mod\ 3$$

$$2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots mod\ 3.$$

Assim, a congruência módulo 3 faz com que todos os números naturais sejam "congruentes módulo 3" a 0, 1 ou 2, ou seja, a divisão por 3 deixará resto 0, 1 ou 2.

Assim como na "congruência módulo 2", podemos fazer uso da adição e multiplicação na "congruência módulo 3" da seguinte maneira:

Se $a \equiv b\ mod\ 3$ e $c \equiv d\ mod\ 3$, então $\begin{cases} a + c \equiv b + d\ mod\ 3 \\ e \\ a.c \equiv b.d\ mod\ 3 \end{cases}$ e a partir do conhecimento das "congruências módulo 3", podemos encontrar o resto da divisão de um número natural por 3.

**Exemplo 1.11**

Qual o resto da divisão de 3758 por 3?

$$3758 = 3.10^3 + 7.10^2 + 5.10 + 8.$$

Mas,

$10 \equiv 1\ mod\ 3$ e, portanto, $10.10 \equiv 1.1\ mod\ 3 \implies 10^2 \equiv 1^2\ mod\ 3$ e $10.10^2 \equiv 1.1^2\ mod\ 3 \Longrightarrow 10^3 \equiv 1^3\ mod\ 3$.

Então,

$$3758 \equiv 3.1^3 + 7.1^2 + 5.1 + 8$$
$$3758 \equiv 3.1 + 7.1 + 5.1 + 8$$
$$3758 \equiv 3 + 7 + 5 + 8$$
$$3758 \equiv 23 \ (23 \div 3 = 7, \text{ resto } 2)$$
$$3758 \equiv 2\ mod\ 3.$$

Portanto o resto da divisão de 3758 por 3 é 2.

Generalizando, todo número natural é “congruente módulo 3” à soma de seus algarismos.

Sendo $3758 \equiv 3 + 7 + 5 + 8\ mod\ 3$, o resto da divisão de 3758 por 3 é igual ao resto da divisão da soma de seus algarismos por 3. Assim, justifica-se através da “congruência módulo 3” o “critério de divisibilidade por 3”: um número é divisível por 3 se a soma de seus algarismos for divisível por 3.

**Exemplo 1.12**

Verifique se 853176 é divisível por 3.

$$85317 \equiv 8 + 5 + 3 + 1 + 7 + 6\ mod\ 3$$
$85317 \equiv 30\ mod\ 3$ ($30 \div 3 = 10$, resto 0), então $85317 \equiv 0\ mod\ 3$.

Portanto, 853176 deixa resto 0 na divisão por 3, ou seja, é divisível por 3.

Outros tipos de problemas:

**Problema 1.1**

Qual é o resto da divisão de $16.83$ por 3?

$16 \div 3 = 5$ (resto 1), $83 \div 3 = 27$ (resto 2). Portanto, $16 \equiv 1\ mod\ 3$ e $83 \equiv 2\ mod\ 3$. Daí, $16.83 \equiv 1.2 \equiv 2\ mod\ 3$. Conclui-se que o resto da divisão de $16.83$ por 3 é 2.

**Problema1.2**

Qual é o resto da divisão de $13^{1000}$ por 3?

$13^{1000} = 13.13.13.13. \ldots .13$ (1000 vezes o fator 13).

Mas, $13 \equiv 1\ mod\ 3$ e, portanto,

$$13^{1000} \equiv 1.1.1.1. \ldots .1\ mod\ 3 \Longrightarrow 13^{1000} \equiv 1\ mod\ 3.$$

Ou seja, $13^{1000}$ deixa resto 1 ao ser dividido por 3. (Aquilo que poderia parecer coisa impossível de se calcular, torna-se bastante simples com o auxílio da "congruência módulo 3").

**1.3.3 Divisibilidade por 4.**

Dizemos que "$a$ congruente a $b$ módulo 4" e escrevemos $a \equiv b\ mod\ 4$, se $a$ e $b$ deixam o mesmo resto quando divididos por 4.

Assim, temos que:

$$0 \equiv 4 \equiv 8 \equiv \cdots mod\ 4$$
$$1 \equiv 5 \equiv 9 \equiv \cdots mod\ 4$$
$$2 \equiv 6 \equiv 10 \equiv \cdots mod\ 4$$
$$3 \equiv 7 \equiv 11 \equiv \cdots mod\ 4.$$

Todo número natural é "congruente módulo 4" a 0, 1, 2 ou 3 (a divisão por 4 deixa resto 0, 1, 2 ou 3) e, como nos casos anteriores,

Se $a \equiv b\ mod\ 4$ e $c \equiv d\ mod\ 4$, então $\begin{cases} a + c \equiv b + d\ mod\ 4 \\ e \\ a.c \equiv b.d\ mod\ 4 \end{cases}$.

E como se calcula o resto de uma divisão por 4?

Vejamos alguns exemplos.

**Exemplo 1.12**

Qual o resto da divisão de 1052 por 4?

$$1252 \equiv 1.10^3 + 2.10^2 + 5.10 + 2\ mod\ 4.$$

Porém,

$$10 \equiv 2\ mod\ 4.$$

Logo,

$$10.10 \equiv 2.2\ mod\ 4 \Longrightarrow 10^2 \equiv 4\ mod\ 4 \Longrightarrow 10^2 \equiv 0\ mod\ 4 \Longrightarrow$$

$$10^2.10 \equiv 0.2\ mod\ 4 \Longrightarrow 10^3 \equiv 0\ mod\ 4.$$

Daí em diante,

$$10^4 \equiv 0\ mod\ 4,\ 10^5 \equiv 0\ mod\ 4,\ \text{etc.}$$

Portanto,

$$1252 \equiv 1.0 + 2.0 + 5.10 + 2\ mod\ 4 \Longrightarrow 1252 \equiv$$

$$52\ mod\ 4 \Longrightarrow 1252 \equiv 0\ mod\ 4.$$

Assim, explica-se o “critério de divisibilidade por 4”, através da “igualdade módulo 4”: um número natural é divisível por 4 se o número formado pelos seus dois últimos algarismos for divisível por 4.

Utilizando a “congruência módulo 4”, podemos brincar com os números e encontrar os restos da divisão por 4 de uma maneira mágica!

**Exemplo1.13**

Calcule, sem efetuar o produto, o resto da divisão de $123456789.876543$ por 4.

Usando os conhecimentos mostrados a pouco,

$$123456789 \equiv 89\ mod\ 4 \quad (89 \div 4 = 22, \text{ com resto 1})$$

$$123456789 \equiv 1\ mod\ 4.$$

E,

$$876543 \equiv 43\ mod\ 4 \quad (43 \div 4 = 10, \text{ com resto 3})$$

$$876543 \equiv 3\ mod\ 4.$$

Portanto,

$$123456789.876543 \equiv 1.3\ mod\ 4 \Longrightarrow 123456789.876543 \equiv 3\ mod\ 4.$$

O resto da divisão de $123456789.876543$ por 4 é 3.

### 1.3.4 Divisibilidade por 5.

Dizemos que "$a$ é congruente a $b$ módulo 5" e escrevemos $a \equiv b\ mod\ 5$, se $a$ e $b$ deixam o mesmo resto quando divididos por 5.

Dessa forma, temos:

$$0 \equiv 5 \equiv 10 \equiv \cdots mod\ 5$$

$$1 \equiv 6 \equiv 11 \equiv \cdots mod\ 5$$

$$2 \equiv 7 \equiv 12 \equiv \cdots mod\ 5$$

$$3 \equiv 8 \equiv 13 \equiv \cdots mod\ 5$$

$$4 \equiv 9 \equiv 14 \equiv \cdots mod\ 5.$$

Assim, a "congruência módulo 5" faz com que todos os números naturais sejam "congruentes módulo 5" a 0, 1, 2, 3 ou 4, ou seja, a divisão por 5 deixará resto 0, 1, 2, 3 ou 4.

Continuam válidas as propriedades:

Se $a \equiv b\ mod\ 5$ e $c \equiv d\ mod\ 5$, então $\begin{cases} a + c \equiv b + d\ mod\ 5 \\ e \\ a.c \equiv b.d\ mod\ 5 \end{cases}$.

Passemos ao estudo da divisibilidade.

**Exemplo1.14**

783 é divisível por 5?

Temos,

$$783 = 7.10^2 + 8.10 + 3.$$

Entretanto,

$$10 \equiv 0\ mod\ 5 \Longrightarrow 10.10 \equiv 0.0\ mod\ 5 \Longrightarrow 10^2 \equiv 0\ mod\ 5.$$

Portanto,

$$783 \equiv 7.0 + 8.0 + 3 \Longrightarrow 783 \equiv 3\ mod\ 5.$$

Através da "congruência módulo 5", mostramos que 783 ao ser dividido por 5 deixa 3 como resto. Então, todo número natural é "congruente módulo 5" ao seu último algarismo. Daí, o critério de divisibilidade por 5; um número é divisível por 5 quando seu último algarismo for 0 ou 5.

### 1.3.5 Divisibilidade por 6.

Dizemos que "$a$ é congruente a $b$ módulo 6" e escrevemos $a \equiv b\ mod\ 6$, se $a$ e $b$ deixam o mesmo resto quando divididos por 6.

Dessa forma, temos:

$$0 \equiv 6 \equiv \cdots mod\ 6$$
$$1 \equiv 7 \equiv \cdots mod\ 6$$
$$2 \equiv 8 \equiv \cdots mod\ 6$$
$$3 \equiv 9 \equiv \cdots mod\ 6$$
$$4 \equiv 10 \equiv \cdots mod\ 6$$
$$5 \equiv 11 \equiv \cdots mod\ 6.$$

Nos casos estudados até agora das "congruências módulo m", de divisibilidade por 2, 3, 4 e 5, obtivemos os restos das divisões com facilidade, pois $10 \equiv 0\ mod\ 2$, $10 \equiv 1\ mod\ 3$, $100 \equiv 0\ mod\ 4$ e $10 \equiv 0\ mod\ 5$.

Porém, na "congruência módulo 6", os cálculos a serem efetuados para se conseguir o resto da divisão de um número natural por 6 ficam mais trabalhosos, tornando-se inviável o ensino numa sala de aula de 6° ou 7° anos, pois:

$$10 \equiv 4\ mod\ 6$$
$$10^2 \equiv 4.4\ mod\ 6 \Longrightarrow 10^2 \equiv 16\ mod\ 6\ \Longrightarrow 10^2 \equiv 4\ mod\ 6$$

$10^3 \equiv 4\ mod\ 6$, etc.

Assim, para provar que 7458 é divisível por 6, poderíamos escrever (como foi feito nos exemplos anteriores):

$$7458 = 7.10^3 + 4.10^2 + 5.10 + 8.$$

Então,

$$7458 \equiv 7.4 + 4.4 + 5.4 + 8\ mod\ 6.$$

Segue que,

$$7458 \equiv 4.(7 + 4 + 5) + 8\ mod\ 6$$

$$7458 \equiv 64 + 8\ mod\ 6$$

$$7458 \equiv 72\ mod\ 6 \Longrightarrow 7458 \equiv 0\ mod\ 6.$$

Ou seja, esse cálculo acaba por não se tornar tão prático nas séries iniciais, como introdução ao conceito de congruência. Fica mais fácil lembrar que um número é divisível por 6 quando for divisível por 2 e 3. Como $7458 \equiv 0\ mod\ 2$ e $7458 \equiv 0\ mod\ 3$, 7458 é divisível por 2 e por 3 e, consequentemente, por 6.

### 1.3.6 Divisibilidade por 7.

Como no caso da divisibilidade por 6, ao repetirmos os procedimentos realizados chegaríamos a um critério de divisibilidade por 7 nada prático, visto que:

$$10 \equiv 3\ mod\ 7$$

$$10^2 \equiv 3.3\ mod\ 7 \Longrightarrow 10^2 \equiv 9\ mod\ 7 \Longrightarrow 10^2 \equiv 2\ mod\ 7$$

$$10^2 \equiv 2.3\ mod\ 7 \Longrightarrow 10^3 \equiv 6\ mod 7$$

$$10^4 \equiv 2.2\ mod\ 7 \Longrightarrow 10^4 \equiv 4\ mod\ 7$$

$$10^5 \equiv 2.6\ mod 7 \Longrightarrow 10^5 \equiv 12\ mod 7 \Longrightarrow 10^5 \equiv 5\ mod 7$$

$$10^6 \equiv 6.6\ mod\ 7 \Longrightarrow 10^6 \equiv 36\ mod\ 7 \Longrightarrow 10^6 \equiv 1\ mod\ 7.$$

Para as demais potências de 10, os resultados se repetem:

3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3,...

Para se calcular o resto da divisão de 9376 por 7, através de “congruência módulo 7”, podemos escrever:

$$9376 = 9.10^3 + 3.10^2 + 7.10 + 6.$$

Então,

$$9376 \equiv 9.6 + 3.2 + 7.3 + 6\ mod\ 7$$

$$9376 \equiv 54 + 6 + 21 + 6 \; mod \; 7$$

$$9376 \equiv 87 \; mod \; 7 \Longrightarrow 9376 \equiv 3 \; mod \; 7.$$

Portanto, 9376 deixa resto 3 ao ser dividido por 7. Certamente, não seria muito conveniente ensinar a encontrar o resto de uma divisão por 7 dessa forma. Como estamos introduzindo a ideia de congruência nas séries iniciais, esses cálculos podem ser feitos apenas a título de curiosidade.

## 1.4 Critérios de divisibilidade e o sistema de numeração

Em alguns casos, não precisaremos tentar dividir para saber se um número é ou não múltiplo de outro. Para isso usaremos as características de nosso sistema de numeração e algumas propriedades do resto de uma divisão. Vamos lembrar alguns fatos.

**1.** No nosso sistema, usamos 10 algarismos (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) cujo valor aumenta ou diminui conforme a posição.

**Exemplo1.15**

$$12948 = 1.10000 + 2.1000 + 9.100 + 4.10 + 8.$$

**2.** Se um número é fator de outros dois números, ele é divisor da sua soma (e da sua diferença).

**Exemplo1.16**

6 é fator de 30

6 é fator de 48.

Então, 6 é fator de $30 + 48$.

E 6 também é fator de $48 - 30$ (pois, $18 = 6 \times 3$).

**3.** Dividimos dois números por um mesmo divisor; se a soma (diferença) dos restos for menor que o divisor, ela será igual ao resto da soma (diferença) dos dois números.

**Exemplo1.17**

Soma:

$22 \div 7 = 3$ e o resto é 1

$33 \div 7 = 4$ e o resto é 5.

A soma dos restos é 6 (que é menor que 7).

$22 + 33 = 55$

$55 \div 7 = 7$ e o resto é 6.

Diferença:

$5 - 1 = 4$

$33 - 22 = 11$

$11 \div 7 = 1$ e o resto é 4.

**Observação:** se a diferença for um número negativo, somamos o divisor.

**Exemplo1.18**

$44 \div 7 = 4$ e o resto é 2

$26 \div 7 = 3$ e o resto é 5

$2 - 5 = -3$ . Nesse caso somamos o divisor, ou seja, $-3 + \mathbf{7} = 4$.

$44 - 26 = 18$

$18 \div 7 = 2$ e o resto é 4.

**4.** Dividimos dois números por um mesmo divisor; se a soma dos restos for maior que o divisor, subtraímos o valor do divisor e o resultado será o resto da soma dos dois números.

**Exemplo1.19**

$26 \div 7 = 3$ e o resto é 5

$32 \div 7 = 4$ e o resto é 4.

A soma dos restos é 9 (que é maior que 7). Nesse caso subtraímos o divisor $9 - \mathbf{7} = 2$.

$26 + 32 = 58$

$58 \div 7 = 8$ e o resto é 2.

### 1.4.1 Divisibilidade por 2: números pares e ímpares.

O critério de divisibilidade mais conhecido é a divisão por 2. Para determinar se um número é divisível por 2 (isto é, par) ou não (ímpar) só precisamos verificar se o último algarismo é par ou ímpar. Observe que:

$10 = 2.5$

$100 = 2.50$

$1000 = 2.500$ e assim por diante.

Então, por exemplo:

$456 = 4.100 + 5.10 + 6$

$400 = 200.2$ é par (divisível por 2)

$50 = 25.2$ é par (divisível por 2)

$6 = 3.2$ é par (divisível por 2).

E 456 é par.

456789123 é ímpar (não é divisível por 2)

456789124 é par (é divisível por 2).

Um fato importante é que todos os fatores de um número ímpar são ímpares. Basta um fator par para que o número seja par.

### 1.4.2 Divisibilidade por 4 e 8.

Observe que:

$100 = 4.25$

$1000 = 4.250.$

E assim por diante...

$$1000000 = 4.250000.$$

Isto é, as potências de 10, a partir de 100, são todas divisíveis por 4. Mas, 10 não é divisível por 4.

Então, para saber se um número é divisível por 4, não precisamos nos preocupar com as centenas, milhares e assim por diante. Essas classes já tem o 4 como fator.

Pra saber se um número é divisível por 4, basta saber se os dois últimos algarismos formam um número divisível por 4.

Para saber o resto da divisão de um número por 4, basta saber o resto da divisão dos seus dois últimos algarismos por 4.

**Exemplo 1.20**

88952432 é divisível por 4?

Basta verificar se 32 é divisível por 4.

$$32 \div 4 = 8 \text{ com resto } 0$$

**Exemplo 1.21**

Qual o resto da divisão de 38955647 por 4?

Basta verificar o resto da divisão de 47 por 4.

$$47 \div 4 = 11 \text{ com resto } 3.$$

Portanto 38955647 não é divisível por 4.

A divisibilidade por 8 segue o mesmo padrão. Veja:

$$1000 = 8.125$$

$$10000 = 8.1250.$$

E assim por diante...

$$1000000 = 8.125000$$

Isto é, as potências de 10, a partir de 1000, são todas divisíveis por 8. Mas, 10 não é divisível por 8 e 100 também não é divisível por 8.

Então, para saber se um número é divisível por 8, não precisamos nos preocupar com os milhares, dezenas de milhares, etc. Essas classes já têm o 8 como fator.

Para saber se um número é divisível por 8, basta saber se os três últimos algarismos formam um número divisível por 8.

Para saber o resto da divisão de um número por 8, basta saber o resto da divisão dos seus três últimos algarismos por 8.

**Exemplo1.22**

35627344 é divisível por 8?

Basta verificar para 344.

$344 \div 8 = 43$, com resto 0. Portanto, 35627344 é divisível por 8.

**Exemplo1.23**

Qual o resto de 457789763?

Basta verificar o resto da divisão de 763 por 8.

$763 \div 8 = 95$ com resto 3.

Portanto, 457789763 não é divisível por 8.

### 1.4.3 Divisibilidade por 5 e 10.

As mesmas ideias da divisibilidade por 2 podem ser usadas na divisibilidade por 5 e 10. Basta observar que:

$$10 = 5.2$$

$$100 = 5.10.2$$

$$1000 = 5.100.2.$$

E assim por diante. Isso mostra que:

**1.** Um número é divisível por 5 se (e só se) o último algarismo for 5 ou 0.

**2.** Um número é divisível por 10 se (e só se) o último algarismo for 0.

Para saber o resto da divisão de um número por 5, basta saber o resto da divisão de seu último algarismo por 5.

Para saber o resto da divisão de um número por 10, basta saber o resto da divisão de seu último algarismo por 10, isto é, basta saber qual é seu último algarismo.

**Exemplo1.24**

Determine o resto das divisões sem executar a soma:

a) $(457 + 378 + 19) \div 10$

Os últimos algarismos somam 24 $(7 + 8 + 9)$. Logo, o resto da divisão é 4.

b) $(358 + 57917 + 123) \div 5$

Os últimos algarismos somam 18 $(8 + 7 + 3)$.. Logo, o resto da divisão é 3.

**Exemplo1.25**

Se somarmos todos os números de 1 a 587, qual será o resto da divisão por 5?

A soma dos algarismos de 0 a 9 $(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9)$. é 45, que é múltiplo de 5. Observe que até 580 a soma dos números será um múltiplo de 45 $(58.45)$, portanto, um múltiplo de 5. Só precisamos então nos preocupar com a soma dos últimos algarismos dos sete últimos números: $1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$. Observe que último algarismo da soma é 8, portanto o resto da divisão da soma desses números por 5 é 3. Logo o resto da divisão da soma de todos os números de 1 a 587 por 5 é 3.

**Exemplo1.26**

Se somarmos todos os números de 1 a 536, qual será o resto da divisão por 10?

A soma dos algarismos de 0 a 9 $(1+2+3+4+5+6+7+8+9)$ é 45. Logo, até 530 a soma dos últimos algarismos dos números será $(53.45)$, um número com último algarismo igual a 5. Só precisamos então nos preocupar com este 5 e com a soma dos últimos algarismos dos seis últimos números: $(5+1+2+3+4+5=26)$. O último algarismo é 6 e o resto da soma é 6.

### 1.4.4 Divisibilidade por 3 e por 9.

**Exemplo1.27**

Qual o resto de $(200+40+7)\div 3$?

$200\div 3=66$ com resto 2 (o mesmo resto de $2\div 3$)

$40\div 3=13$ com resto 1 (o mesmo resto de $4\div 3$)

$7\div 3=2$ com resto 1 (o mesmo resto de $7\div 3$).

O resto de $247\div 3$ é o mesmo resto de $(2+4+7)\div 3$, isto é, o mesmo resto de $13\div 3=4$. E com resto 1.

Investigando um pouco mais...

$1\div 3=0$ com resto 1

$10\div 3=3$ com resto 1

$100\div 3=33$ com resto 1.

E assim por diante...

$100000\div 3=333333$ com resto 1

O resto das potências de 10 quando divididas por 3 é sempre 1. Cada classe contribui com uma unidade para o resto da divisão por 3. Por exemplo, 4000 contribui com 4 unidades para o resto da divisão $4573\div 3$.

Resumindo: o resto da divisão de um número por 3 é o mesmo resto da divisão da soma de seus algarismos por 3.

**Exemplo1.28**

Qual o resto de $4573 \div 3$?

O resto de $4573 \div 3$ é o mesmo resto de $(4.1000 + 5.100 + 7.10 + 3)$ dividido por 3, ou seja, o mesmo resto de $(4.1 + 5.1 + 7.1 + 3)$ dividido por 3, ou ainda, igual ao resto de $(4 + 5 + 7 + 3)$ dividido por 3.Portanto temos o resto igual a 1.

Mais exemplos:

**Exemplo1.29**

O resto da divisão de 4567 por 3 é o resto da divisão de $(4 + 5 + 6 + 7 = 22)$ por 3, isto é, o resto da divisão de $2 + 2 = 4$ por 3 e, finalmente, o resto é 1. De fato, $4567 = 1522.4 + 1$.

**Exemplo1.30**

Se somarmos todos os números de 1 a 536, qual será o resto da divisão por 3?

O resto de $(1 + 2 + 3) \div 3$ é 0; o resto de $(4 + 5 + 6) \div 3$ é 0; e assim por diante, sempre indo de três em três até o próximo múltiplo de 3.

Temos que nos preocupar apenas com os números após o último múltiplo de 3, no caso, 534 (pois $5 + 3 + 4 = 12$). Basta verificar a soma $(535 + 536)$ é divisível por 3. A soma dos algarismos dessa soma é 27, que é múltiplo de 3. Logo, o resto será 0.

Para a divisibilidade por 9, podemos usar a mesma idéia. Vejamos um exemplo:

**Exemplo1.31**

Qual o resto da divisão $(400 + 80 + 7) \div 9$?

$400 \div 9 = 44$ com resto 4 (o mesmo resto de $4 \div 9$)

$80 \div 9 = 8$ com resto 8 (o mesmo resto de $8 \div 9$)

$7 \div 9 = 0$ com resto 7 (o mesmo resto de $7 \div 9$).

O resto de $487 \div 9$ é o mesmo resto de $(4 + 8 + 7) \div 9$, ou seja, o mesmo resto de $19 \div 9$.

$19 \div 9 = 2$ com resto 1.

Investigando um pouco mais...

$1 \div 9 = 0$ com resto 1

$10 \div 9$ =1com resto 1

$100 \div 9 = 11$ com resto 1.

E assim por diante...

$100000 \div 9 = 111111$ com resto 1

O resto das potências de 10, quando divididas por 9, é sempre 1. Cada classe contribui com uma unidade para o resto da divisão por 9. Por exemplo, 4000 contribui com 4 unidades para o resto da divisão $4585 \div 9$.

Resumindo: o resto da divisão de um número por 9 é o mesmo resto da divisão da soma de seus algarismos por 9.

**Exemplo1.32**

Qual o resto de $4585 \div 9$?

O resto de $4585 \div 9$ é o mesmo resto de $(4.1000 + 5.100 + 8.10 + 5) \div 9$, isto é, o mesmo resto de $(4.1 + 5.1 + 8.1 + 5) \div 9$, ou ainda, $(4 + 5 + 8 + 5 = 22) \div 9$. O resto é 4.

Outros exemplos:

**Exemplo1.33**

O resto da divisão de 4567 por 9 é o resto da divisão de $(4 + 5 + 6 + 7 = 22)$ por 9, isto é, o resto da divisão de $(2 + 2)$ por 9, e finalmente, o resto será 4. De fato, $4567 = 507 \times 9 + 4$.

**Exemplo1.34**

Se somarmos todos os números de 1 a 536, qual será o resto da divisão desta soma por 9?

O resto de $(1+2+3+4+5+6+7+8+9) \div 9$ é o mesmo de $45 \div 9$, que é 0; o resto de $(10+11+12+13+14+15+16+17+18) \div 9$ é o mesmo de $126 \div 9$ que é zero; e assim por diante...

Temos que nos preocupar apenas com os números após o último múltiplo de 9, no caso 531 (pois $5+3+1=9$). Basta verificar a soma $(532+533+534+534+536)$. A soma dos algarismos é 60. O resto de $60 \div 9$ é 6. Logo, o resto da soma de todos os números de 1 a 536 por 9 será 6.

# Capítulo 2

## Uma abordagem mais sofisticada da divisibilidade e congruência no ensino básico.

### 2.1 Aritmética dos restos.

Neste capítulo, inicialmente, apresentaremos algumas das noções mais importantes da aritmética que serão utilizados no decorrer do mesmo. Todas as definições e resultados que serão apresentados podem ser encontrados em Hefez, Abramo (2016).

**Definição2.1:** Seja *m* um número natural. Diremos que dois números inteiros *a* e *b* são congruentes módulo *m* se os restos de sua divisão euclidiana por *m* são iguais. Quando os inteiros *a* e *b* são congruente módulo *m*, escreve-se:

$$a \equiv b \; mod \; m \leftrightarrow a = mq + b$$

**Exemplo2.1**

$17 \equiv 9 \; mod \; 2$, já que os restos da divisão de 17 e 9 por 8 são iguais a 1.

**Proposição2.1:** Suponha que *a, b,* $m \in \mathbb{Z}$, com *m > 0.* Tem-se que $a \equiv b \; mod \; m$ se, e somente se, *m*|*b – a.*

***Demonstração.***

(⟹) Se $a \equiv b \; mod \; m$, então $m|a - b.$

De fato, se $a \equiv b \, mod \, m$, então $a$ e $b$ deixam o mesmo resto quando divididos por $m$ **(Definição)**. Assim podemos escrever:

$$a = mq + r \text{ e } b = mq' + r, \text{ com } q, q' \in \mathbb{Z} \text{ e } 0 \leq r < m.$$

Daí, segue que

$$a - b = m(q - q') + (r - r) \Leftrightarrow a - b = m(q - q').$$

Portanto $m|a - b$.

($\Leftarrow$) Se $m|a - b$, então $a \equiv b \, mod \, m$.

De fato, se $m|a - b$, então $a - b = mq \Leftrightarrow a = b + mq$, com $q \in \mathbb{Z}$. O que é o mesmo que dizer que $a \equiv b \, mod \, m$.

**Proposição2.2:** Seja $m \in \mathrm{N}^*$. Para todos $a, b \, e \, c \in \mathbb{Z}$, tem-se que

(i) $a \equiv a \, mod \, m \, (reflexiva)$,

(ii) $a \equiv b \, mod \, m, então \, b \equiv a \, mod \, m \, (simétrica)$,

(iii) $a \equiv b \, mod \, m, e \, b \equiv c \, mod \, m \, então \, a \equiv c \, mod \, m \, (transitiva)$

***Demonstração.***

$(i)$ $a \equiv a \, mod \, m \Leftrightarrow m \setminus a - a \Leftrightarrow a - a = m.0$. O que prova a reflexividade da congruência, pois zero é múltiplo de qualquer número.

$(ii)$ $a \equiv b \, mod \, m \Leftrightarrow a - b = mq, com \, q \in \mathbb{Z}$, multiplicando $a - b = mq \, por - 1$, obtemos $b - a = m(-q)$ e assim $b \equiv a \, mod \, m$. O que equivale dizer que se um dado número é divisível por *m* seu simétrico também o é.

$(iii)$ $a \equiv b \, mod \, m \, e \, b \equiv c \, mod \, m$. Escrevendo na forma de igualdades, temos: $a - b = mq_1 \, e \, b - c = mq_2$, com $q_1 \, e \, q_2 \in \mathbb{Z}$. Somando as equações

$$a - b + b - c = mq_1 + mq_2)$$

obtemos

$$a - c = m(q_1 + q_2)$$

daí

$$a = c \ mod \ m.$$

**Proposição2.3:** Sejam *a, b, c* e $m \in \mathbb{Z}$, com $m > 1$, tais que $a \equiv b \ mod \ m$, então:

$(i)$ $a + c \equiv b + c \ mod \ m$

$(ii)$ $a - c \equiv b - c \ mod \ m$

$(iii)$ $ac \equiv bc \ mod \ m$

***Demonstração.***

$(i)$ $De \ a \equiv b \ mod \ m \ temos \ a - b = mq \ e \ como \ a - b = a + c - (b + c)$ resulta que:

$$a + c \equiv b + c \ \ mod \ m.$$

$(ii)$ Como $a - c - (b - c) \ e \ a - b = mq$ , temos que $a - c = b - c \ \ mod \ m$.

$(iii)$ De $a \equiv b \ mod \ m,$ temos $a - b = mq$ então $ac - bc = mcq,$ com $c \in \mathbb{Z},$ o que implica que $m \setminus ac - bc$, logo $ac \equiv bc \ mod \ m$.

**Proposição2.4:** Se *a, b, c, d e m* são inteiros tais que $a \equiv b \ mod \ m \ e \ c \equiv d \ mod \ m$, então:

$(i)$ $a + c \equiv b + d \ mod \ m$

*(ii)* $a - c \equiv b - d \ mod \ m$

$(iii)$ $ac \equiv bd \ mod \ m$

***Demonstração.***

$(i)$ De fato, como $a \equiv b \ mod \ m \ e \ c \equiv d \ mod \ m,$ temos que $m \setminus b - a \ e \ m \setminus c - d,$ daí basta observar que $m \setminus (b - a) + (c - d)$ e, portanto, $m \setminus (b + d) - (a + c),$ assim $a + c \equiv b + d \ mod \ m.$

$(ii)$ Como $a \equiv b\ mod\ m\ e\ c \equiv d\ mod\ m$ temos: $a - b = mq_1\ e\ c - d = mq_2$ com $q_1\ e\ q_2 \in \mathbb{Z}$. Subtraindo as equações

$$a - b - c + d = mq_1 - mq_2$$
$$a - c - b + d = mq_1 - mq_2$$
$$a - c - (b - d) = m(q_1 - q_2)$$

logo

$$a - c \equiv b - d\ mod\ m.$$

$(iii)$ Basta notar que $bd - ac = d(b - a) + a(d - c)$, como de (i) temos que $m \setminus b - a\ e\ m \setminus c - d$ e fácil concluir que $m \setminus bd - ac$, logo $ac \equiv bd\ mod\ m$.

Este resultado é de grande valia, pois considerando quaisquer dois inteiros $a = mq_1 + r_1\ e\ b = mq_2 + r_2$, onde $r_1\ e\ r_2$ são os restos da divisão, pela proposição temos que $a \pm b \equiv r_1 \pm r_2\ mod\ m$ o que verifica que o resto de $a \pm b$ depende apenas dos restos da divisão de $a$ e $b$ por *m.*

**Exemplo2.2**

Vamos calcular o resto da divisão de $98 + 34 + 78 + 45$ por 5.

**Solução:**

Observe que:

$$98 \equiv 3\ mod\ 5$$
$$34 \equiv 4\ mod\ 5$$
$$78 \equiv 3\ mod\ 5$$
$$45 \equiv 0\ mod\ 5.$$

Segue que pela **proposição 2.4**, temos $98 + 34 + 78 + 45 \equiv 3 + 4 + 3 + 0 \equiv 10 \equiv 0\ mod\ 5$.

Portando o resto da divisão de $98 + 34 + 78 + 45$ por 5 é 0.

**Proposição2.5:** Se a, b, c e m são inteiros e $ac \equiv bc\, mod\, m$, então $a \equiv b\, mod\, \left(\frac{m}{d}\right)$, onde $d = mdc(c; m)$.

***Demonstração.***

Como $\frac{m}{d}$ e $\frac{mc}{d}$ são coprimos, temos que:

$$ac \equiv bc\, mod\, m \Leftrightarrow m \setminus (b-a)c \Leftrightarrow \frac{m}{d} \setminus (b-a)\frac{c}{d}$$
$$\Leftrightarrow \frac{m}{d} \setminus (b-a) \Leftrightarrow a \equiv b\, mod\, \left(\frac{m}{d}\right).$$

Outro resultado muito útil e importante dessa teoria é dado pela seguinte proposição.

**Proposição2.6:** Sejam *a m, b* $\epsilon\, \mathbb{Z}$, com $m > 0$ . Se $a \equiv b\, mod\, m$, então tem se que $a^n \equiv b^n\, mod\, m$.

***Demonstração.***

A prova segue diretamente da identidade:

$$a^n - b^n = (a-b).(a^{n-1} + a^{n-2}b^1 + a^{n-3}b^2 + \cdots + a^1 b^{k-2} + b^{k-1}).$$

Vejamos alguns exemplos:

**Exemplo2.3**

Calcule o resto das divisões de $15^6 + 9^{10}$, $9^{10} - 15^6$ e $15^6 . 9^{10}$ por 7.

Facilmente obtemos as soluções usando as proposições apresentadas, observe:

***Solução.***

$(i)$ Vamos calcular o resto da divisão de $15^6 + 9^{10}$ por 7.

Da definição de congruência sabemos que $15 \equiv 1\ mod\ 7$ e $9 \equiv 2\ mod\ 7$. Daí temos:

$$15^6 \equiv 1^6\ mod\ 7 \text{ e } 9^{10} \equiv 2^{10} \equiv 1024 \equiv 2\ mod\ 7$$ **(proposição2.6).**

Somando membro a membro as congruências acima, temos:

$$15^6 + 9^{10} \equiv 1 + 2 \equiv 3\ mod\ 7$$ **(proposição2.4).**

Logo, o resto da divisão da soma $15^6 + 9^{10}$ por 7 é 3.

$(ii)$ Vamos calcular o resto da divisão de $9^{10} - 15^6$ por 7.

Da mesma forma, podemos subtrair as congruências obtidas:

$$9^{10} - 15^6 \equiv 2 - 1 \equiv 1 \bmod 7$$ **(proposição2.4).**

Logo, o resto da divisão de $9^{10} - 15^6$ por 7 é 1.

$(iii)$ Vamos calcular o resto da divisão de $15^6 . 9^{10}$ por 7.

Ainda usando a **proposição2.4** podemos multiplicar membro a membro as congruências:

$$15^6 . 9^{10} \equiv 1.2 \equiv 2\ mod\ 7.$$

Logo, o resto da divisão de $15^6 . 9^{10}$ por 7 é 2.

**Exemplo2.4**

Sejam *a* e *b* dois números inteiros cujos restos da divisão por 13 são, respectivamente, 7 e 5. Determine os restos da divisão de *a* + *b*, $a - b$ e *a.b* por 13.

***Solução.***

Escrevendo os dados do problema em forma de congruência, temos:

$$a \equiv 7 \; mod \; 13 \text{ e } b \equiv 5 \; mod \; 13.$$

Assim,

$$(i) \;\; a + b \equiv 7 + 5 \equiv 12 \; mod \; 13.$$

$$(ii) \;\; a - b \equiv 7 - 5 \equiv 2 \; mod \; 13.$$

$$(iii) \; a.b \equiv 7.5 \equiv 35 \equiv 9 \; mod \; 13.$$

Logo os restos da divisão de $a + b$, $a - b$, e $a.b$, por 13 são, respectivamente, 12, 2 e 9.

## 2.2 Pequeno Teorema de Fermat

Pierre de Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Estudou direito em Toulouse, onde serviu no parlamento local, primeiro como advogado, mais tarde como conselheiro. Dedicava à Matemática apenas as suas horas de lazer e, mesmo assim, foi considerado um dos maiores matemáticos de seu tempo (BOYER. 2003).

Vamos utilizar nessa sessão um de seus teoremas que nos auxiliará no estudo das congruências modulares, esse teorema é intitulado "**Pequeno Teorema de Fermat"**, que além de facilitar muito a resolução de algumas situações-problema, é considerado a base para a criação dos Testes de Primalidade modernos, sendo que a maioria destes testes foi uma modificação ou uma generalização do Teste de Fermat, que tem como base o **Pequeno Teorema de Fermat (P.T.F)**.

Embora este tema não faça parte da grade curricular obrigatória das escolas brasileira, muitas provas nacionais de olimpíadas e concursos trazem problemas que sugerem o uso de congruência modular em suas resoluções.

**Teorema2.1 (P.T.F):** Se $p$ é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \, mod \, p$.

***Demonstração.***

Primeiro observe que se $a^p \equiv a \, mod \, p \Leftrightarrow p \setminus a^p - a$. De fato:

- Se $p = 2$, o resultado é imediato, visto que $a^2 - a = a.(a-1)$ é par.

- Suponhamos agora $p$ ímpar. Neste caso basta mostrar o resultado para $a \geq 0$. Vamos provar por indução sobre $a$.

Observe que o resultado vale para $a = 0$, pois $p \setminus 0$.

Supondo o resultado válido para $a$, mostraremos que também vale para $a + 1$. Pelo Binômio de Newton, temos:

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a.$$

Por hipótese de indução, temos $a^p - a$ divisível por $p$ e $\binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$ também é divisível por $p$.

Portanto o resultado é válido para todo $p$ primo e $a \, \epsilon \, \mathbb{N}$.

**Corolário2.1:** Se $p$ é um número primo e se $a$ é um número natural não divisível por $p$,então $a^{p-1} \equiv 1 \, mod \, p$.

***Demonstração.***

Se $a^p \equiv a \, mod \, p \Leftrightarrow p \setminus a(a^{p-1} - 1) \Longrightarrow p \setminus a$ ou $p \setminus (a^{p-1} - 1)$. Mas como $p$ não divide $a$ tem-se que $p \setminus (a^{p-1} - 1)$, logo $a^{p-1} \equiv 1 \, mod \, p$.

Vejamos a seguir um exemplo em que obtemos o resultado mais facilmente pela aplicação do Teorema de Fermat.

**Exemplo2.5**

Calcule o resto da divisão de $2^{100}$ por 7.

**Solução:**

Como 7 e 2 são primos, pelo **P.T.F**, observe que $2^6 \equiv 1 \, mod \, 7$. Desta forma podemos escrever:

$$2^{100} = (2^6)^{16}.2^4 \equiv 1^{16}.2^4 \equiv 16 \equiv 2 \, mod \, 7.$$

Portanto concluímos que o resto da divisão de $2^{100}$ por 7 é 2.

**Exemplo2.6**

Mostre que $2^{50} + 3^{50}$ é divisível por 13

**Solução:**

Como 13 e 2 são primos, pelo **P.T.F**, observe que $2^{12} \equiv 1 \, mod \, 13$. Desta forma podemos escrever:

$$2^{50} = (2^{12})^4.2^2 \equiv 1^4.2^2 \equiv 4 \, mod \, 13 \, (\boldsymbol{i}).$$

Como 13 e 3 são primos, temos também que $3^{12} \equiv 1\ mod\ 13$. Assim podemos escrever:

$$3^{50} = (3^{12})^4 . 3^2 \equiv 1^4 . 3^2 \equiv 9\ mod\ 13\ (\boldsymbol{ii}).$$

De $(\boldsymbol{i})$ e $(\boldsymbol{ii})$ temos que:

$$2^{50} + 3^{50} \equiv 4 + 9 \equiv 13 \equiv 0\ mod\ 13.$$

O que mostra a proposição.

## 2.3 Equações Diofantinas Lineares em duas variáveis

As equações diofantinas lineares de duas variáveis são equações do tipo:

$$ax + by = c$$

com $a, b, c \in \mathbb{Z}$ e com $a$ e $b$ não simultaneamente nulos.

Tais equações são chamadas assim em homenagem a Diofanto de Alexandria e suas soluções são da forma $(x_0, y_0)$ tal que $a.x_0 + b.y_0 = c$. Essas equações são de fundamental importância na solução de diversos problemas que são apresentados aos alunos desde o ensino fundamental, além disso, pode ser vinculado a diversos assuntos estudados na educação básica.

As definições que serão apresentadas a seguir são baseadas em Hefez, Abramo (2016).

**Definição2.2:** Chamaremos de $x_0$ e $y_0$ uma solução particular da equação $ax + by = c$ esta solução particular é um par de números inteiros que torna a sentença $a.x_0 + b.y_0 = c$ verdadeira.

**Proposição2.7:** Sejam $a, b, c \in \mathbb{Z}$, com $a\ e\ b$ não ambos nulos e seja $d = mdc(a, b)$. Então a equação $ax + by = c$ tem solução em $\mathbb{Z}$ se e somente se $d \setminus c$.

**Demonstração.**

(⇒) Suponhamos que ∃ $x, y \in \mathbb{Z}$ tal que $ax + by$ = c. Como $d \setminus a$ e $d \setminus b$, temos que $d$ divide qualquer combinação linear e, portanto, $d \setminus ax + by$, ou seja, $d \setminus c$.

(⇐) Suponhamos que $d \setminus c$. Então ∃ $e \in \mathbb{Z}$ tal que $d.e = c$. Mas $d = mdc(a, b)$. Logo, ∃ $\alpha, \beta \in \mathbb{Z}$ tal que $a.\alpha + b.\beta = d$. Multiplicando por $e$, obtemos:

$$a.\alpha.e + b.\beta.e = d.e.$$

Sejam $x = \alpha.e$ e $y = \beta.e$, então $ax + by$ = c, ou seja, a equação diofantina tem solução em $\mathbb{Z}$.

É possível perceber que para uma equação do tipo $ax + by = c$, em que $d = mdc(a, b)$ divide c, pode ser escrita de forma equivalente através da equação $a_i x + b_i y = c_i$, com $a_i = \frac{a}{d}, b_i = \frac{b}{d}, c_i = \frac{c}{d}$, em que $mdc(a_i, b_i) = 1$. Desta forma, encontrar solução para a equação $ax + by = c$ é equivalente a encontrar solução para $a_i x + b_i y = c_i$.

**Teorema2.2:** Se a Equação Diofantina Linear $ax + by = c$ possui uma solução do tipo $(x_0, y_0)$, então possui infinitas soluções do tipo $\left(x = x_0 + \frac{b}{t}t,\ y = y_0 - \frac{a}{t}t\right)$, com $t \in \mathbb{Z}$.

**Demonstração.**

Sejam $(x_0, y_0)$, uma solução particular e $(x_k, y_k)$, uma solução qualquer da equação $ax + by = c$. Segue que $a.x_0 + b.y_0 = c = a.x_k + b.y_k = c$. Assim, $ax_0 + by_0 = ax_k + by_k = c$. Subtraindo $ax_0$ de ambos os lados temos, $by_0 = ax_k + by_k - ax_0$. Subtraindo $by_k$ de ambos os lados da igualdade temos que:

$$a(x_k - x_0) = b(y_0 - y_k).$$

Como $d \setminus a$ e $d \setminus b$, existem $p$ e $q \in \mathbb{Z}$, tais que $a = pd$ e $b = qd$, com $mdc(p,q) = 1$. Isto nos diz que, $p(x_k - x_0) = q(y_0 - y_k)$. Percebemos então que $p \setminus q(y_0 - y_k)$, como $mdc(p,q) =$ 1 segue que $p \setminus (y_0 - y_k)$, pois p e q são primos entre si, logo existe $t \in \mathbb{Z}$, tal que $(y_0 - y_k) = pt$. Notemos que $(y_0 - y_k) = pt \Rightarrow y_k = y_0 - pt$, mas $p = \frac{a}{d}$, logo,

$$y_k = y_0 - \frac{b}{d}t.$$

Agora observemos que $(y_0 - y_k) = pt$ implica em, $q(y_0 - y_k) = qpt = p(x_k - x_0)$, cancelando o fator p nos dois últimos membros da igualdade temos, $qt = (x_k - x_0) \Longrightarrow x_k = x_0 + qt$, mas $q = \frac{b}{d}$, logo,

$$x_k = x_0 + \frac{b}{d}t.$$

Vejamos agora alguns exemplos

**Exemplo2.7**

Determine as soluções inteiras, caso existam, da equação diofantina $2x + 4y = 7$.

**Solução**

Observe que $mdc(2,4) = 2$. Com 2 não divide 7, podemos concluir que a equação $2x + 4y = 7$ não possui solução inteira.

**Exemplo2.8**

Determine as soluções inteiras, caso existam, da equação diofantina $12x + 5y = 7$.

**Solução**

Observe que $mdc(12,5) = 1$. Como 1 divide 7, então a equação $12x + 5y = 7$ possui solução inteira. Assim, inicialmente, vamos determinar uma solução para a equação $12x + 5y = 1$, para isso, observe que usando o algoritmo de Euclides temos:

$$1 = 5 - 2.2$$

$$1 = 5 - 2.(12 - 2.5)$$

$$1 = 5 - 2.12 + 4.5$$

$$1 = -2.12 + 5.5$$

Segue que se multiplicarmos a última igualdade por 7, obtemos uma solução particular para a equação $12x + 5y = 7$. Assim temos:

$$7 = -14.12 + 35.5$$

Ou seja, $x_0 = -14$ e $y_0 = 35$. Concluímos então que a solução geral da equação é dada por:

$$x = -14 + 5t \text{ e } y = 35 - 12t, \text{ com } t \in \mathbb{Z}$$

## 2.4 Resolvendo equações diofantinas lineares usando congruência

Para resolvermos uma Equação Diofantina Linear do tipo $ax + by = c$ podemos escrevê-la como uma congruência do tipo $ax \equiv c\ mod\ b$ ou $by \equiv c\ mod\ a$. Assim, resolver a equação $ax + by = c$ equivale a resolver a congruência $ax \equiv c\ mod$ ou $by \equiv c\ mod\ a$, ou seja, precisamos encontrar a classe de equivalência $\bar{x}$ tal que $ax \equiv c\ mod\ b$ ou $by \equiv c\ mod\ a$.

Vejamos agora alguns exemplos:

**Exemplo2.9**

Determine as soluções inteiras, caso existam, da equação diofantina $12x + 5y = 7$.

**Solução**

Observe que $mdc(12,5) = 1$. Como 1 divide 7, então a equação $12x + 5y = 7$ possui solução inteira. Inicialmente vamos reescrever a equação usando módulo 5.

Assim temos:

$$2x \equiv 2 \; mod \; 5.$$

Agora basta determinar a classe $\bar{x}$ que multiplicada pela classe 2 obtemos um valor que quando dividido por 5 deixa resto 2. Nesse caso temos que a classe $\bar{x} = 1$, Assim temos:

$$x \equiv 1 \; mod \; 5.$$

Desta forma podemos escrever que $x = 5t + 1$, com $t \in \mathbb{Z}$. Substituindo o valor de $x$ na equação $12x + 5y = 7$, obtemos:

$$12(5t + 1) + 5y = 7$$

$$60t + 12 + 5y = 7$$

$$5y = -5 - 60t$$

$$y = -1 - 12t.$$

Portanto a solução geral da equação é dada por $x = 5t + 1$ e $y = -1 - 12t$.

**Exemplo 2.10**

Determine a solução geral caso exista, da equação diofantina $4x + 10y = 12$.

**Solução**

Observe que $mdc(4,10) = 2$. Como 2 divide 12, então a equação $4x + 10y = 12$ possui solução inteira. Inicialmente simplificar a equação por 2 obtendo assim a equação equivalente $2x + 5y = 6$ . Agora vamos reescrever a equação $2x + 5y = 6$ usando módulo 2. Assim temos:

$$y \equiv 0 \; mod \; 2.$$

Desta forma podemos escrever que $y = 2t$, com $t \in \mathbb{Z}$. Substituindo o valor de $y$ na equação $2x + 5y = 6$, obtemos:

$$2x + 5.2t = 6$$
$$2x = 6 - 10t$$
$$x = 3 - 5t.$$

Portanto a solução geral da equação é dada por $x = 3 - 5t$ e $y = 2t$.

# Capítulo 3

## Algumas problemas que podem ser resolvidos usando congruência modular.

Uma vez já estabelecidas, no capítulo anterior, as definições e conceitos de aritmética modular, vamos apresentar agora algumas situações problema em que podemos fazer uso desses conceitos nas suas resoluções. Essas aplicações serão constituídas de situações problema elementares e também de problemas mais substanciais. Esperamos assim destacar a aplicabilidade desses conceitos na resolução de problemas a partir do ensino básico.

**Problema 3.1: (Apostila Aritmética dos restos: problemas com congruência – Questão 20 - Portal do saber)** Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer natural n.

**Solução**

Usando a ideia de congruência, perceba que a expressão deve ser congruente a zero módulo 133. Assim observe que:

$(i)$ $11^{n+2} \equiv 121.11^n \equiv -12.11^n \; mod\; 133$

$(ii)$ $12^{2n+1} \equiv 144^n.12 \equiv 11^n.12 \; mod\; 133.$

Somando $(i)$ e $(ii)$, temos

$$11^{n+2} + 12^{2n+1} \equiv -12.11^n + 11^n.12 \equiv 0 \; mod\; 133.$$

Portanto a expressão $11^{n+2} + 12^{2n+1}$ é divisível por 133.

**Problema 3.2: (Banco de Questões OBMEP - 2017, pg. 102)** Determine todos os inteiros não negativos $x$ e $y$ que satisfazem a equação $7x + 11y = 154$.

**Solução**

Observe que $mdc(7,11) = 1$. Como 1 divide 154, então a equação $7x + 11y = 154$ possui solução inteira. Inicialmente vamos reescrever a equação usando módulo 7. Assim temos:

$$11y \equiv 4y \equiv 0 \, mod \, 7.$$

Ou seja

$$y \equiv 0 \, mod \, 7.$$

Desta forma podemos escrever que $y = 7t$, com $t \in \mathbb{Z}$. Substituindo o valor de $y$ na equação $12x + 5y = 7$, obtemos:

$$7x + 11.7t = 154$$
$$7x = 154 - 77t$$
$$x = 22 - 11t.$$

Portanto a solução geral da equação é dada por $x = 22 - 11t$ e $y = 7t$.

Como $x$ e $y$ devem ser inteiros não negativos temos:

- $x \geq 0 \Longrightarrow 22 - 11t \geq 0 \Longrightarrow t \leq 2$
- $y \geq 0 \Longrightarrow 7t \geq 0 \Longrightarrow t \geq 0.$

Ou seja, os valores possíveis para t são:

$$t = 0 \Longrightarrow x = 22; y = 0$$
$$t = 1 \Longrightarrow x = 11; y = 7$$
$$t = 2 \Longrightarrow x = 0; y = 14.$$

Concluímos então que as soluções inteiras não negativas que satisfazem a equação são $(22,0); (11,7); (0,14)$.

**Problema 3.3: (Programa Olímpico de Treinamento Intensivo – POTI)** Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau; quando

sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200?

**Solução**

Seja x o número de degraus da escada. Pelos dados do problema podemos montar o seguinte sistema:

$$\begin{array}{ll} x \equiv 1\ mod\ 2 & (i) \\ x \equiv 2\ mod\ 3 & (ii) \\ x \equiv 3\ mod\ 5 & (iii). \end{array}$$

Observe que em $(i)$ podemos escrever que $x = 1 + 2t$, com $t \in \mathbb{Z}$. Substituindo $x$ em $(ii)$ temos:

$$1 + 2t \equiv 2\ mod\ 3$$
$$2t \equiv 1\ mod\ 3.$$

Agora basta determinar a classe $\bar{t}$ que multiplicada pela classe 2 obtemos um valor que quando dividido por 3 deixa resto 1. Nesse caso temos que a classe $\bar{t} = 2$, Assim:

$$t \equiv 2\ mod\ 3.$$

Ou seja,

$$t = 2 + 3q, \text{ com } q \in \mathbb{Z}.$$

Substituindo $t$ em $x = 1 + 2t$, temos:

$$x = 1 + 2.(2 + 3q)$$
$$x = 5 + 6q.$$

Vamos substituir agora $x = 5 + 6q$ em $(iii)$ daí,

$$5 + 6q \equiv 3\ mod\ 5$$

$$6q \equiv 3\ mod\ 5.$$

Agora basta determinar a classe $\bar{q}$ que multiplicada pela classe 6 obtemos um valor que quando dividido por 5 deixa resto 3. Nesse caso temos que a classe $\bar{q} = 3$, Assim:

$$q \equiv 3\ mod\ 5.$$

Ou seja,

$$q = 3 + 5k, \text{ com } k \in \mathbb{Z}.$$

Substituindo $q$ em $x = 5 + 6q$, temos:

$$x = 5 + 6.(3 + 5k)$$

$$x = 23 + 30k.$$

Como x está entre 150 e 200, segue que:

$$150 < 23 + 30k < 200 \Rightarrow 127 < 30k < 177 \Rightarrow 4 < k < 6 \Rightarrow k = 5$$

Portanto, o número de degraus da escada é $x = 23 + 30.5 = 173$.

**Problema 3.4: (Apostila Aritmética dos restos: problemas com congruência – Questão 1 - Portal do saber)** Prove que $n^5 + 4n$ e divisível por 5 para todo inteiro $n$.

**Solução**

Pelo **Pequeno Teorema de Fermat**, temos $n^5 \equiv n\ mod\ 5$, já que $n$ é inteiro e 5 é primo. Assim podemos escrever:

$$n^5 + 4n \equiv n + 4n \equiv 5n \equiv 0\ mod\ 5$$

Portanto a expressão $n^5 + 4n$ e divisível por 5 para todo inteiro $n$.

**Problema 3.5: (Programa Olímpico de Treinamento Intensivo – POTI)** Prove que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um número inteiro para todo $n \in \mathbb{Z}$.

**Solução**

Observe que pelo **Pequeno Teorema de Fermat** temos:

- $n^5 \equiv n \; mod \; 5$, já que $n$ é inteiro e 5 é primo.
- $n^3 \equiv n \; mod \; 3$, já que $n$ é inteiro e 3 é primo.

Assim podemos reescrever a expressão $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ da seguinte forma:

$$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{n}{5} + \frac{n}{3} + \frac{7n}{15} = \frac{3n+5n+7n}{15} = \frac{15n}{15} = n \text{ (inteiro).}$$

Portanto a expressão $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um número inteiro para todo $n \in \mathbb{Z}$.

**Problema 3.6: (Colégio Militar de Fortaleza – 2011)** Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7 o resto será:

a) 1

b) 2

c) 3

d) 4

e) 5

**Solução**

Seja $x$ e $y$ os números procurados. Pelos dados do problema podemos

É possível escrever:

- $x \equiv 6 \; mod \; 7$

- $y \equiv 5 \, mod \, 7$.

Somando $x$ e $y$, temos:

$$x + y \equiv 6 + 5 \, mod \, 7$$

$$x + y \equiv 11 \equiv 4 \, mod \, 7.$$

Portanto o resto da divisão da soma desses números por 7 é igual a 4.

**Problema 3.7: (OBMEP – 2012 – NÍVEL 3)** Para fazer várias blusas iguais, uma costureira gastou R$ 2,99 para comprar botões de 4 centavos e laços de 7 centavos. Ela usou todos os botões e laços que comprou. Quantas blusas ela fez?

a) 2

b) 5

c) 10

d) 13

e) 23

**Solução**

Seja $x$, $y$ e as quantidades de botões e laços respectivamente. Pelos dados do problema podemos escrever a seguinte equação:

$$0{,}04x + 0{,}07y = 2{,}99.$$

Multiplicando a equação por 100 temos:

$$4x + 7y = 299.$$

Como o $mdc(4, 7) = 1$. Como 1 divide 299, então a equação $4x + 7y = 299$ possui solução inteira. Inicialmente vamos reescrever a equação usando módulo 4. Assim obtemos:

$$7y \equiv 3y \equiv 3 \, mod \, 4.$$

Observe que $mdc(3, 4) = 1$, portanto temos:

$$y \equiv 1\ mod\ 4$$

Desta forma podemos escrever que $y = 1 + 4t$, com $t \in \mathbb{Z}$. Substituindo o valor de $y$ na equação $4x + 7y = 299$, obtemos:

$$4x + 7.(1 + 4t) = 299$$
$$4x + 7 + 28t = 299$$
$$x = 73 - 7t$$

Portanto a solução geral da equação é dada por $x = 73 - 7t$ e $y = 1 + 4t$. Como $x$ e $y$ devem ser inteiros positivos temos:

- $x > 0 \Longrightarrow 73 - 7t > 0 \Longrightarrow t < 10{,}4$
- $y > 0 \Longrightarrow 1 + 4t > 0 \Longrightarrow t > -0{,}25$

Ou seja, os valores possíveis para t são:

$$t = 0 \Longrightarrow x = 73; y = 1$$
$$t = 1 \Longrightarrow x = 66; y = 5$$
$$t = 2 \Longrightarrow x = 59; y = 9$$
$$t = 3 \Longrightarrow x = 52; y = 13$$
$$t = 4 \Longrightarrow x = 45; y = 17$$
$$t = 5 \Longrightarrow x = 38; y = 21$$
$$t = 6 \Longrightarrow x = 31; y = 25$$
$$t = 7 \Longrightarrow x = 24; y = 29$$
$$t = 8 \Longrightarrow x = 17; y = 33$$
$$t = 9 \Longrightarrow x = 10; y = 37$$
$$t = 10 \Longrightarrow x = 3; y = 41.$$

Analisando o contexto do problema é possível perceber que a quantidade de laços é igual a quantidade de blusas, ou seja , a quantidade de botões é múltiplo da quantidade de laços, já que cada blusa deve ter a mesma quantidade de botões. Concluímos então que as soluções inteiras que satisfazem o problema são $(73{,}1); (52{,}13)$. Portanto a quantidade de blusas feitas foi igual a 13.

**Problema 3.8: (Programa Olímpico de Treinamento Intensivo – POTI)** O consumo de 5 copos de suco, 10 coxinhas e 6 hambúrgueres para um grupo de estudantes totalizou R$ 48,00. Outro grupo consumiu 8 copos de suco, 6 coxinhas e 3 hambúrgueres ao preço de R$ 37,00. Quanto custa cada um dos produtos consumidos?

**Solução**

Sejam $x$, $y$ e $z$ os preços de cada copo de suco, de cada coxinha e de cada hambúrguer respectivamente. Pelos dados do problema podemos escrever as seguintes equações:

$$5x + 10y + 6z = 48 \quad (i)$$
$$8x + 6y + 3z = 37 \quad (ii).$$

Multiplicando a equação $(i)$ por 8 e a equação $(ii)$ por $-5$ e depois somando $(i)$ e $(ii)$, obtemos:

$$\begin{array}{r} 40x + 80y + 48z = 384 \quad (i).8 \\ -40x - 30y - 15z = -185 \quad (ii).(-5) \\ \hline 50y + 33z = 199. \end{array}$$

Segue que para resolver o problema basta resolver a equação diofantina $50y + 33z = 199$. Observe que $mdc(50,33) = 1$. Como 1 divide 199, então a equação $50y + 33z = 199$ possui solução inteira. Inicialmente vamos reescrever a equação usando módulo 33 . Assim temos:

$$50y \equiv 17y \equiv 1 \; mod \; 33.$$

Agora basta determinar a classe $\bar{y}$ que multiplicada pela classe 17 obtemos um valor que quando dividido por 33 deixa resto 1. Nesse caso temos que a classe $\bar{y} = 2$, Assim:

$$y \equiv 2 \; mod \; 33.$$

Desta forma podemos escrever que $y = 2 + 33t$, com $t \in \mathbb{Z}$. Substituindo o valor de $y$ na equação $50y + 33z = 199.$, obtemos:

$$50.(2 + 33t) + 33z = 299$$
$$100 + 1650t + 33z = 299$$
$$z = 3 - 50t.$$

Portanto a solução geral da equação é dada por $y = 2 + 33t$ e $z = 3 - 50t$.

Como $y$ e $z$ devem ser inteiros positivos então:

- $y > 0 \Longrightarrow 2 + 33t > 0 \Longrightarrow t > -0{,}06$
- $z > 0 \Longrightarrow 3 - 50t > 0 \Longrightarrow t < 0{,}06.$

Ou seja, $t = 0$, Assim

- $y = 2 + 33.0 = 2$
- $z = 3 - 50.0 = 3.$

Substituindo $y = 2$ e $z = 3$ em qualquer uma das equações iniciais, encontramos $x = 2$, logo o preço de cada copo de suco é $R\$\ 2{,}00$, o de cada coxinha é $R\$\ 2{,}00$ e o de cada hambúrguer é de $R\$\ 3{,}00$.

# Capítulo 4

## Algumas aplicações do uso da congruência modular no cotidiano

### 4.1 Aplicações de congruências em sistemas de identificação: Cadastro das Pessoas Físicas na Receita Federal (CPF).

Um exemplo importante do nosso cotidiano: verificação dos dois dígitos de controle do CPF de uma pessoa.

O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são dígitos de controle ou de verificação . A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência.

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

Se $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por $a_{10}$ deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é $S$, o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $(S - a_{10}) \equiv 0\ mod\ 11$. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Seria proposto aos alunos que trouxessem alguns números de CPF's para que verificassem como se obtém os dois dígitos verificadores. Por exemplo, no caso de um aluno que trouxesse um número de CPF com os seguintes 9 primeiros dígitos: 235

343 104, mostraríamos que o primeiro dígito de controle seria obtido da seguinte maneira:

Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

$$\begin{array}{ccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

**Figura 4.1**

Efetuando as multiplicações correspondentes, sempre ajudando no caso de qualquer dificuldade, teríamos:

$$2.1 + 3.2 + 5.3 + 3.4 + 4.5 + 3.6 + 1.7 + 0.8 + 4.9 = 116.$$

Dividindo o número 116 por 11, teremos:

$$\begin{array}{r|l} 116 & 11 \\ \cline{2-2} 6 & 10 \end{array}$$

**Figura 4.2**

Dessa forma, o primeiro dígito de controle encontrado seria o algarismo **6**.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora pediríamos para que acrescentassem o décimo dígito (que é o que acabaram de calcular) e usaríamos uma base de multiplicação de 0 a 9. Vejamos:

$$\begin{array}{cccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

**Figura 4.3**

Efetuando as multiplicações, encontrariam o seguinte resultado:

$$2.0 + 3.1 + 5.2 + 3.3 + 4.4 + 3.5 + 1.6 + 0.7 + 4.8 + 6.9 = 145.$$

Dividindo o número 145 por 11, teríamos:

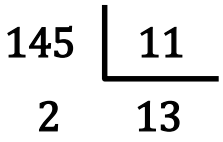


**Figura 4.4**

Logo, o segundo dígito de controle encontrado é o **2**.

Concluiriam então que, para este exemplo, o CPF completo seria: 235 343 104 **62.**

Caso encontrassem como resto da divisão por 11 o número 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito **zero**.

## 4.2 Congruência e Criptografia.

Relatos históricos mostram que a criptografia existe desde a antiguidade e já foi bastante utilizada em ações secretas, disfarçando informações por intermédio de codificações e decodificações. No que concerne ao uso da criptografia nos dias de hoje, uma grande aplicação da mesma está relacionada a sites de compras pela internet utilizando protocolos que funcionam com o auxílio da mesma, permitindo que o cliente consiga realizar compras seguras. Vejamos um exemplo do uso da criptografia.

**Gpukpq Hwpfcogpvcn**

**Figura 4.5**

Com certeza, à primeira vista, a frase acima não possui significado algum. Parece algum idioma desconhecido ou de outro planeta. Experimentemos agora substituir cada letra pela segunda letra que vem antes dela, na sequência do alfabeto completo (26 letras, incluindo k, w e y). Sem grande dificuldade, teríamos escrito ***"Ensino Fundamental"***.

De uma forma simplificada é o que ocorre na criptografia, quando alguém deseja transmitir alguma informação que não deseja partilhar com os outros, a não

ser o destinatário final e combina uma chave qualquer para transmissão e recepção da informação. O receptor, de posse da chave, decodifica a mensagem, transformando-a novamente para que possa entender e ler o que lhe foi enviado. No exemplo que demos, que é bastante simples, o emissor substituiu cada letra do alfabeto por uma outra que ficava duas posições depois dela, no alfabeto. O receptor, sabendo da chave dessa "criptografia", aplicava a operação inversa na frase recebida, ou seja, substituía cada letra recebida pela que ficava duas posições antes dela, no alfabeto.

Se designarmos por x a letra original e por y a letra que a substituirá no código, é como se tivéssemos uma função, definida $y = x + 2$.

Sabe-se que a primeira aplicação de criptografia foi inventada pelo imperador romano Júlio César, que enviava mensagens aos seus generais trocando letras do alfabeto a partir de uma simples regra, similar à que exemplificamos acima, que seria "pule três" (chave 3). Através deste esquema, 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.

Vejamos como funcionava essa chave 3, de Júlio 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 |

**Tabela 4.1**

Ou seja, uma palavra simples como **"atacar"** seria codificada como **"xqxzxo"**. Este sistema e outros similares, obtidos através de permutações em que as letras são "embaralhadas", são muito simples e não são difíceis de serem "decifrados", mas por muito tempo serviram para "esconder" mensagens.

Em sala de aula, poderíamos propor uma brincadeira em que a classe ficaria dividida em grupos. Assim, um grupo enviaria mensagens codificadas para que outro grupo as decifrasse. Os códigos a serem usados poderiam ser os seguintes:

| **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

**Tabela 4.2**

**Chave: Somar 4**

Dessa forma, cada letra ficaria representada por um número que representa a sua posição no alfabeto. Com a chave acima, ela ficaria substituída pela letra cujo

número corresponde ao número original, aumentado de 4. Se acontecesse do resultado ser superior ao 26, voltaríamos ao início do alfabeto. Por exemplo, o número 28 corresponderá à letra b, pois $28 = 26 + 2$ e sabemos que $28 \equiv 2\ mod\ 26$.

Através da chave dada como exemplo (somar 4 ou $y = x + 4$.), se a mensagem a ser enviada fosse **CIDADE MARAVILHOSA**, o grupo emissor teria que criptografá-la como: **GMHEHI QEVEZMPLSWE**.

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:

| EMISSOR | CÁLCULO | RECEPTOR |
|---|---|---|
| **G** | $7 - 4 = 3$ | **C** |
| **M** | $13 - 4 = 9$ | **I** |
| **H** | $8 - 4 = 4$ | **D** |
| **E** | $5 - 4 = 1$ | **A** |
| **H** | $8 - 4 = 4$ | **D** |
| **I** | $9 - 4 = 5$ | **E** |

**Tabela 4.3**

| EMISSOR | CÁLCULO | RECEPTOR |
|---|---|---|
| **Q** | $17 - 4 = 13$ | **M** |
| **E** | $5 - 4 = 1$ | **A** |
| **V** | $22 - 4 = 18$ | **R** |
| **E** | $5 - 4 = 1$ | **A** |
| **Z** | $26 - 4 = 21$ | **V** |
| **M** | $13 - 4 = 9$ | **I** |
| **P** | $16 - 4 = 12$ | **L** |
| **L** | $12 - 4 = 8$ | **H** |
| **S** | $19 - 4 = 15$ | **O** |
| **W** | $23 - 4 = 19$ | **S** |
| **E** | $5 - 4 = 1$ | **A** |

**Tabela 4.4**

Atividades como essa, aplicadas nas classes do Ensino Fundamental, levarão os alunos a perceber que, na tradução da mensagem enviada, eles terão que aplicar a operação inversa da que foi usada pelo emissor da mensagem na criação da mensagem criptografada.

## 4.3 Balanceando equações químicas usando equações diofantinas.

Equação química é a representação simbólica de uma reação química. Em uma equação química, as substâncias que reagem são chamadas *reagentes*, as substâncias formadas são denominadas *produtos.* (Souza, Líria Alves de. «Equação Química». *Brasil Escola*).

Por convenção, os reagentes e os produtos são separados por uma seta (→), que por sua vez indica a direção da reação.

$$NaOH_{(g)} + HCl_{(l)} \longrightarrow NaCl_{(aq)} + H_2O_{(l)}.$$

Os reagentes ficam do lado esquerdo da seta, ou seja, *NaOH* e *HCl* e os produtos ficam do lado direito da seta, ou seja, *NaCl* e $H_2O$.

De acordo com **Jennifer Rocha Vargas Fogaça**, do site Manual da química, balancear uma equação química significa acertar os coeficientes estequiométricos (menores números inteiros e positivos que aparecem antes das substâncias nas equações) para que a quantidade de átomos de cada elemento seja igual nos dois lados da equação, isto é, nos reagentes (primeiro membro) e nos produtos (segundo membro).

Isso é importante primeiramente porque, conforme a **Lei de Lavoisier** da conservação das massas diz, **"**numa reação química feita em recipiente fechado, a soma das massas dos reagentes é igual à soma das massas dos produtos"**.** Portanto, o balanceamento das equações que representam as reações químicas é justamente tornar isso verdade. Além disso, é importante saber balancear as equações porque em processos químicos são realizadas análises e cálculos das quantidades de reagentes e/ou produtos (cálculos estequiométricos) em que se depende em grande parte do balanceamento das equações.

Um dos métodos mais utilizados para realizar o balanceamento das equações é método algébrico, que consiste em representar as equações químicas por um conjunto de equações, onde as variáveis são os coeficientes estequiométricos.

Vejamos alguns exemplos:

**Exemplo 4.1**

Faça o balanceamento da seguinte equação $NH_4NO_3 \longrightarrow N2O + H_2O$.

**Solução**

Inicialmente vamos chamar os coeficientes estequiométricos de $x, y$ e $z$, Assim teremos:

$$xNH_4NO_3 \longrightarrow yN2O + z\ H_2O.$$

Usando o método algébrico vamos igualar a quantidade de átomos de cada elemento, Observe que:

- $2x = 2y$ (em *N*).
- $4x = 2z$ (em *H*).
- $3x = y + z$ (em *H*).

Ou seja, balancear esta equação química equivale a encontrar as menores soluções inteiras positivas da equação diofantina $2x - z = 0$. Como $mdc(2, -1) = 1$ e 1 divide zero, então a equação $2x - z = 0$ possui solução inteira. Escrevendo a equação usando módulo 2, temos:

$$-z \equiv z \equiv 0\ mod\ 2.$$

Desta forma podemos escrever que $z = 2t$, com $t \in \mathbb{Z}$. Substituindo o valor de $z$ na equação $2x - z = 0$, obtemos $x = t$.

Como queremos os menores valores inteiros positivos para $x$ e $z$, basta substituir $t = 1$. Assim teremos $x = 1$, $y = 1$ e $z = 2$. Portanto a equação balanceada é:

$$NH_4NO_3 \longrightarrow N_2O + 2\ H_2O.$$

**Exemplo 4.2**

Vamos balancear a equação química que representa a reação de combustão do gás butano, que é um dos componentes do gás de cozinha.

$$C_4H_{10(g)} + O_{2(g)} \longrightarrow CO_{2(g)} + H_2O_{(v)}.$$

**Solução**

Inicialmente vamos chamar os coeficientes estequiométricos de $x, y, z$ e $w$. Assim teremos:

$$xC_4H_{10(g)} + yO_{2(g)} \longrightarrow zCO_{2(g)} + wH_2O_{(v)}.$$

Usando o método algébrico vamos igualar a quantidade de átomos de cada elemento, Observe que:

- $4x = z$ (em *C*).
- $10x = 2w$ (em *H*).
- $2y = 2z + w$ (em *O*).

Ou seja, balancear esta equação química equivale a encontrar as menores soluções inteiras positivas da equação diofantina $2y - 13x = 0$. Como $mdc(2, -13) = 1$ e $1$ divide zero, então a equação $2y - 13x = 0 = 0$ possui solução inteira. Escrevendo a equação usando módulo 2, temos:

$$-x \equiv x \equiv 0 \; mod \; 2.$$

Desta forma podemos escrever que $x = 2t$, com $t \in \mathbb{Z}$. Substituindo o valor de $z$ na equação $2y - 13x = 0$, obtemos $y = 13t$.

Como queremos os menores valores inteiros positivos para $x$ e $z$, basta substituir $t = 1$. Assim teremos $x = 2$, $y = 13$, $z = 8$ e $w = 10$. Portanto a equação balanceada é:

$$2C_4H_{10(g)} + 13O_{2(g)} \longrightarrow 8CO_{2(g)} + 10H_2O_{(v)}.$$

## 4.4 A “prova dos nove” ou “regra dos noves fora.”

A “prova dos nove” ou “regra dos noves fora” é amplamente utilizada para provar a veracidade de resultados de operações com números naturais e trata-se de uma aplicação simples de congruência modular. Na aplicação dessa prova, ao retirar os noves fora, encontra-se o resto da divisão de um número por 9. Por exemplo: como saber se o resultado de $246.624 = 172224$ está correto? Primeiro tiramos os noves fora do multiplicando 246 $(2 + 4 + 6 = 12 \div 9 = 1 + resto\ 3)$, descobrimos que $246 \equiv 3\ mod\ 9$. Em seguida tiramos os noves fora do multiplicador 624 $(6 + 4 + 2 = 12 \div 9 = 1 + resto\ 3)$, donde descobrimos que $624 \equiv 3\ mod\ 9$. Depois retiramos os noves fora da multiplicação entre os restos $(3.3 = 9 \div 9 = 1 + resto\ 0)$, logo $9 \equiv 0\ mod\ 9$. Se ao tirarmos os noves fora do produto 172224 encontrarmos um resultado igual a 0 a multiplicação está correta. Então, $(1 + 7 + 2 + 2 + 2 + 4 = 18 \div 9 = 2 + resto\ 0)$. Note que $172224 \equiv 0\ mod\ 9$, logo a conta está correta.

É aceitável que surja o seguinte questionamento: **A prova dos 9 dá 100% de certeza?**

Não, mas podemos considerar um forte indicativo. Como se pode perceber até aqui, há um arcabouço teórico forte de aritmética modular para fundamentar a Prova dos Noves. O problema é que basta que a operação que se deseja verificar esteja com o resultado errado, mas dê o um mesmo resto na divisão por 9 do que o resultado correto, podendo assim mascara o erro. Vejamos mais um exemplo: Será que a o resultado de $845.62 = 52370$ está correto? Primeiro vamos tirar os noves fora do multiplicando 845 $(8 + 4 + 5 = 17 \div 9 = 1 + resto\ 8)$, assim verificamos que $845 \equiv 8\ mod\ 9$. Agora tiramos os noves fora do multiplicador 62 $(6 + 2 = 8 \div 9 = 0 + resto\ 8)$. Daí temos $62 \equiv 8\ mod\ 9$. Tiramos agora, os 9 foras da multiplicação entre os restos $(8.8 = 64 \div 9 = 7 + resto\ 1)$, logo $845.62 \equiv 64 \equiv 1\ mod\ 9$. Se ao tirarmos os noves fora do produto 52370 encontrarmos um resto igual a 1, a multiplicação está correta. Então, $(5 + 2 + 3 + 7 + 0 = 17 \div 9 = 1 + resto\ 8)$. Note que $52370 \equiv 8\ mod\ 9$, logo a conta está errada.

# Considerações Finais

Mesmo a Congruência de números inteiros não fazer parte do currículo do Ensino Básico, acreditamos que a sua introdução a partir do 6° ano do ensino fundamental seria muito pertinente, pois poderia contribuir e incentivar a aprendizagem dos alunos, esta teoria possui diversos resultados que são de fácil compreensão, por isso, poderia ser empregada, tanto para a aquisição de novos conhecimentos como metodologia de aprimoramento de conceitos já estudados, visto que, o pré-requisito para se estudar as congruências modulares é ter os conhecimentos relacionados a divisibilidade. Além disso o seu estudo poderia auxiliar na aquisição das competências e habilidades necessárias, tanto para o âmbito escolar, como para o desempenho de atividades cotidianas dos alunos, como calcular, refletir e comparar, o que favoreceria a sua tomada de decisão.

A congruência de números inteiros, também pode favorecer a aproximação do aluno com a aplicabilidade da matemática no cotidiano em diversas áreas tecnológicas, como por exemplo nos códigos de identificação, além disso, com a fundamentação apresentada e justificada não é de surpreender que o tema se torne uma ferramenta para futuras conjecturas por parte dos alunos.

Portanto, acreditamos que a congruência de inteiros, mesmo não fazendo parte do currículo do alunado do ensino básico, pode servir de arcabouço teórico a fim de auxiliar no desenvolvimento dos mesmos, oportunizando a aquisição de competência e habilidades que lhes serão de grande relevância para vida acadêmica e cotidiana.

# Referências Bibliográficas


ALENCAR FILHO, Edgar de. *Teoria Elementar dos Números.* São Paulo: Nobel, 1992. 336p.

BALANCEAMENTO DE EQUAÇÕES QUÍMICAS. Disponível em: https://www.manualdaquimica.com/quimica-geral/balanceamento-equacoes.htm. Acesso em: mai. 2020.

BASE NACIONAL COMUM CURRICULAR. Disponível em: http://basenacionalcomum. mec.gov.br/abase/. Acesso em: mar. 2020.

BRASIL. Parâmetros Curriculares Nacionais: terceiro e quarto ciclos do ensino fundamental: matemática. Brasília: MEC/SEF, 1998.

BOYER, C.B. *História da Matemática,* 4.ª ed. (Trad. Elza F. Gomide). São Paulo: EdgardBlücher.2003.

COUTINHO, S. C. Números inteiros e criptografia RSA. Rio de Janeiro: IMPA/SBM, 1997.

COUTINHO, Severino Criptografia Rio de Janeiro, IMPA, 2016.

CORREA e SPINILLO, 2004, p.105.

DANTE, L. R. Restos, congruência e divisibilidade. Revista do Professor de Matemática, Rio de Janeiro, n. 10, p. 33-40.

HEFEZ, Abramo. – Aritmética. Coleção PROFMAT. Rio de Janeiro: SBM, 2016.

HEFEZ, Abramo. – Elementos de Aritmética. Textos Universitários. Rio de Janeiro: SBM, 2016.

DE SÁ, I. P. Tratamento da informação na Educação Básica: aritmética modular e os códigos de identificação do cotidiano. Disponível em: http://sbem.iuri0094.hospedagemdesites.ws/anais/ix_enem/Html/minicursos. Acesso em: mai. 2020.

OBMEP. – Provas e Soluções. Disponível em <http://www.obmep.org.br>. . Acesso em 04 mai. 2020.
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO (POTI). Disponível em: https://poti.impa.br/index.php/modulo/lista?serie=2. Acesso em: mai. 2020.

PORTAL DO SABER. Apostila Aritmética dos restos: problemas com congruência. Disponível em: https://portaldaobmep.impa.br/index.php/modulo/ver?modulo=63. Acesso em: mai. 2020.

SANTOS, José Plínio de O. *Introdução à Teoria dos Números.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPq, 1998. 199p.

SHOKRANIAN, Salahoddin. Criptografia para Iniciantes. Brasília: UNB, 2005.