Talysson Paulo da Silva

Critérios de divisibilidade: usuais, incomuns e curiosos

João Pessoa

2019

Talysson Paulo da Silva

Critérios de divisibilidade: usuais, incomuns e curiosos

Trabalho de Conclusão de Curso (TCC) apresentado à coordenação do curso de Mestrado em Matemática da Universidade Federal da Paraíba - UFPB, como parte dos requisitos necessários à obtenção do título de mestre em Matemática.

Universidade Federal da Paraíba- (UFPB)

Campus João Pessoa

Mestrado Profissional - PROFMAT

Orientador: Dr. Bruno Henrique Carvalho Ribeiro

João Pessoa

2019

Talysson Paulo da Silva

Critérios de divisibilidade: usuais, incomuns e curiosos

Trabalho de Conclusão de Curso (TCC) apresentado à coordenação do curso de Mestrado em Matemática da Universidade Federal da Paraíba - UFPB, como parte dos requisitos necessários à obtenção do título de mestre em Matemática.

Dr. Bruno Henrique Carvalho Ribeiro
Orientador

Professor
Dr. Ricardo Burity Croccia Macedo - UFPB

Professor
Dra. Yane Lísley Ramos Araújo - UFRPE

João Pessoa

2019

Talysson Paulo da Silva

Critérios de divisibilidade: usuais, incomuns e curiosos

Trabalho de Conclusão de Curso (TCC) apresentado à coordenação do curso de Mestrado em Matemática da Universidade Federal da Paraíba - UFPB, como parte dos requisitos necessários à obtenção do título de mestre em Matemática.

Dr. Bruno Henrique Carvalho Ribeiro
Orientador

Professor
Dr. Ricardo Burity Croccia Macedo - UFPB

Professor
Dra. Yane Lísley Ramos Araújo - UFRPE

João Pessoa

2019

Dedico ao meu bom Deus que guiou todos os meu passos, dedico a minha bisavó: Nadir Luiza e a minha avó: Maria Sônia que partiram para vida eterna. Dedico também a todos da minha família.

Agradecimentos

A presente dissertação de mestrado não poderia chegar ao seu final sem o precioso apoio de várias pessoas.

Agradeço primeiramente ao meu Deus que me deu discernimento para realização desse trabalho, pois sem ele não teria forças para chegar a lugar nenhum.

Agradeço ao meu orientador e Professor Doutor Bruno Henrique Carvalho Ribeiro, por quem tenho grande admiração e respeito não só pelo excelente profissional que é, compromissado e atencioso, mas também pela pessoa simples que mostra ser, onde sem sua atenção, paciência e estímulo este trabalho não seria possível.

Agradeço a minha família por estarem sempre me incentivando, em especial a senhora Ângela, minha mãe, e ao senhor Paulo, meu pai, motivo de exemplo, a minha esposa Kauany Kylvia e a minha filha, Celina Ilene, a quem devo toda motivação, a meu irmão, Huanderson, enfim a todos os parentes por acreditarem sempre na minha capacidade, me motivando e compreendendo a minha ausência devido a rotina acadêmica.

Agradeço também, a todo o corpo docente do departamento de matemática da UFPB, em especial aos docentes do PROFMAT, por me ensinarem ao longo desses dois anos e meio de caminhada, por fim agradeço aos meus amigos do curso do mestrado, que me acompanharam nessa jornada me ajudando de forma direta ou indiretamente para a realização desse trabalho, em especial ao meu amigo Jucélio pelas várias vezes que me acolheu em seu apartamento.

Resumo

Os critérios de divisibilidades são tido por alunos e até mesmo por alguns professores como simples "macetes", pois eles facilitam na resolução de exercícios e evitam o uso de tantos cálculos, no entanto esse assunto remete na sua essência uma aritmética rica e profunda. Tratamos neste trabalho sobre os critérios de divisibilidades comuns, aqueles que se aprende no ensino básico e outros inéditos. Para tanto, estudamos inicialmente alguns preliminares algébricos e aritméticos, como: Princípio da Boa Ordem (PBO), Princípio da Indução Matemática (PIM), divisão euclidiana, divisibilidade, números primos, algoritmo de Euclides, equações Diofantinas, sistema decimal bem como a aritmética modular. Em seguida apresentamos, demonstramos e exemplificamos os critérios de divisibilidade mais usuais, buscando estimular o interesse do leitor por esse conhecimento. Finalizamos com a criação, demonstração e exemplificação dos critérios de divisibilidade mais sofisticados.

Palavras-chave: Princípio da Indução Matemática (PIM); Critérios de divisibilidade; Sistema decimal; Algoritmo de Euclides; Equações Diofantinas; Aritmética modular.

Abstract

The criterion of divisibility is known by students and some teachers as simples "tricks" . They facilitate the resolution of exercises and avoid the use of multiple accounts, however this subject in essence brings a rich and deep arithmetic. We deal with this work on the criterion of common divisibility, those that one learns in basic education and other unpublished ones. Algebra and Arithmetic , such as: Well - Ordering Principle (PGO) , Principle of Mathematical Induction (PMI) , Euclidean division, divisibility, primary numbers , Euclides algorithm , diophantine equations, decimal system and modular arithmetic. After , we present, demonstrate and exemplify the most common divisibility criterion, seeking the reader's interest in knowledge. We finished with the creation, demosntration and exemplification of the most sophisticated criterion of divisibility.

Key-words: Principle of Mathematical Induction (PMI); Criterion of Divisibility ; Decimal System; Euclides Algorithm; Diophantine Equations; Modular Arithmetic.

Lista de ilustrações

Sumário

Introdução

Os números foram considerados durante muito tempo como entes intuitivos e até algumas das suas propriedades, como por exemplo a comutatividade e a associatividade da adição e multiplicação, eram consideradas inerentes a sua própria natureza, sendo assim, não havia necessidade de serem demonstradas.

Segundo [10, p. 05], a aritmética é apresentada sob a ótica de duas vertentes, a primeira como sendo o ramo da matemática que lida com os números e com as operações possíveis entre eles..., sendo assim o ramo mais elementar e antigo da matemática. A segunda vertente é voltada para teoria dos números, a autora afirma que é o ramo da matemática pura que estuda mais profundamente as propriedades dos números em geral.

Já [4] afirma que o estudo das propriedades dos números em especial os inteiros remota das civilizações mais antigas. Entretanto é na Grécia que primeiro identificamos a teoria de números tal como a entendemos hoje em dia. No que se refere aos inteiros, os gregos diferenciavam entre a logística, ou a arte de calcular com os números inteiros, e a aritmética, ou estudo das propriedades fundamentais dos inteiros. A primeira era domínio dos comerciantes; a segunda dos matemáticos e filósofos.

O conjunto dos números inteiros, usualmente denotado por $\mathbb{Z}$, é o exemplo natural da estrutura algébrica chamada *domínio de integridade*. Isto significa que sobre $\mathbb{Z}$ estão definidas duas operações, *soma* e *produto*, que satisfazem as propriedades operatórias usuais: *associatividade, existência do elemento neutro, inverso aditivo, comutatividade e distributividade do produto em relação a soma.* Para mais detalhes veja [7] .

Do ponto de vista algébrico, a principal dificuldade está no fato de que em $\mathbb{Z}$ não é possível realizar divisões em geral, ou seja, nem sempre um número inteiro é divisível por outro. De fato, não podemos calcular inversos multiplicativos, o que impossibilita a resolução de equações lineares simples como $ax = b$ com $a \notin \{-1, 0, 1\}$, por exemplo. A única solução para esta equação seria $x = a^{-1}b$, mas $a^{-1} = \dfrac{1}{a} \notin \mathbb{Z}$ nestas condições.

O principal objetivo desse trabalho é despertar o interesse e a curiosidade tanto dos alunos dos cursos de matemática ou áreas afins, quanto os da educação básica para aritmética, em especial à aritmética modular, bem como expor e desenvolver alguns fatos curiosos a respeito desse assunto. Além disso, queremos que esse trabalho sirva de apoio para a formação continuada do professor e que sirva também de material didático para ser usado

por alunos dos cursos de licenciatura em matemática ou os da educação básica.

Para isso, usamos nesse trabalho os critérios de divisibilidade como fio condutor. A ideia central é identificar os ingredientes básicos da aritmética que já são usadas nos critérios mais usuais e os implementarmos de forma sistemática na criação de critérios de divisibilidade incomuns.

No primeiro capítulo, intitulado Preliminares Algébricos e Aritméticos dos Inteiros, revisitaremos o conjunto dos inteiros $\mathbb{Z}$, nesse estudo daremos um tratamento axiomático, tendo como objetivos analisar suas propriedades elementares do ponto de vista algébrico e aritmético, bem como introduzir os conceitos necessários ao entendimento dos próximos capítulos. Trataremos também de fatos curiosos relacionado ao tema.

No capítulo 2, intitulado Critérios de Divisibilidade Usuais, apresentaremos a definição, demonstração e exemplificação dos critérios de divisibilidade comuns.

O último capítulo, Construção dos Critérios de Divisibilidade Incomuns e Curiosos, é reservado para a construção, desenvolvimento, demonstração e exemplificação dos novos critérios de divisibilidade, tomaremos como base os critérios de divisibilidade usuais.

1 Preliminares Algébricos e Aritméticos dos Inteiros

Neste capítulo revisitaremos algumas propriedades e alguns resultados dos números inteiros do ponto de vista algébrico e aritmético que são de fundamental importância para o entendimento e acompanhamento dos capítulos subsequentes. As principais referências utilizadas na elaboração desse capítulo são [1, 2, 3, 4, 5, 7, 9, 10] .

1.1 O domínio bem ordenado $\mathbb{Z}$

Como dissemos, o conjunto dos números inteiros $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ é o exemplo mais simples da estrutura algébrica denominada de *anel comutativo com unidade*. De acordo com [6] isto significa que sobre $\mathbb{Z}$ estão definidas duas operações, denominadas *soma* $(+)$ e *produto* $(\cdot)$ satisfazendo, para todo $x, y, z \in \mathbb{Z}$, as propriedades operatórias usuais:

(i) *associatividade*: $x + (y + z) = (x + y) + z$ e $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

(ii) *comutatividade*: $x + y = y + x$ e $x \cdot y = y \cdot x$;

(iii) *distributividade*: $x(y + z) = x \cdot y + x \cdot z$

(iv) *existência de elementos neutros*: existem $0, 1 \in \mathbb{Z}$ tal que $0 + x = x$ e $1 \cdot x = x$;

(v) *existência de inverso aditivo*: dado $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$ tal que $x + (-x) = 0$.

Além disso, $\mathbb{Z}$ não possui divisores de zero; isto é, dados $x, y \in \mathbb{Z}, x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$. Um anel com esta propriedade é chamado de *domínio de integridade* ou simplesmente um *domínio*.

Também está definida uma relação de ordem: dados $x, y \in \mathbb{Z}$ dizemos que x *é menor que* y, escrevendo $x < y$, se existe $0 \neq n \in \mathbb{N}$ tal que $x + n = y$. Esta é uma relação de *ordem total* significando que dados $x, y \in \mathbb{Z}$ uma e somente uma das seguintes condições é verificada:

$$x < y \text{ ou } y < x \text{ ou } x = y.$$

Além disso, esta relação é compatível com as operações de soma e produto em $\mathbb{Z}$ no seguinte sentido: dados $x, y \in \mathbb{Z}$ com $x < y$, então $x + z < y + z$, $\forall\ z \in \mathbb{Z}$; e se $0 < z$, então $xz < yz$.

Uma vez que $\mathbb{Z}$ é um conjunto ordenado podemos definir o que se chama *cota inferior* para um subconjunto S de $\mathbb{Z}$. Dizemos que $n_0 \in \mathbb{Z}$ é uma cota inferior para $\varnothing \neq S \subset \mathbb{Z}$ se $n_0 \leq s$ para todo $s \in S$ (onde temos que $a \leq b$ significa $a < b$ ou $a = b$). Um conjunto que possui uma cota inferior é dito ser *limitado inferiormente*. Quando uma cota inferior n_0 pertence a S dizemos que este conjunto possui um elemento mínimo n_0, ou que n_0 é o *menor elemento* de S.

De posse destas definições podemos enunciar o Princípio da Boa Ordem:

Princípio da Boa Ordem (PBO): Todo subconjunto S de $\mathbb{Z}$ que é não vazio e limitado inferiormente possui menor elemento.

É importante destacar que embora aparentemente intuitivo, o princípio da boa ordem não é válido no anel ordenado dos números reais $\mathbb{R}$. De fato, se considerarmos o conjunto de números inteiros:

$$S = \{x \in \mathbb{Z} : 1 < x < 6\} = \{2, 3, 4, 5\},$$

temos que S é um conjunto limitado inferiormente (qualquer inteiro menor ou igual a 1 é uma cota inferior para S) e seu menor elemento é 2. Por outro lado, se considerarmos S como um subconjunto de $\mathbb{R}$; isto é

$$S = \{x \in \mathbb{R} : 1 < x < 6\},$$

temos que S é um intervalo aberto de extremos 1 e 6. Como antes, S é limitado inferiormente (qualquer número real menor ou igual a 1 é uma cota inferior para S), mas agora S não possui um menor elemento.

Duas consequências básicas do PBO são o Princípio de Indução Matemática e o Algoritmo de Divisão com Resto, que serão abordados nas próximas seções.

1.2 O Princípio de Indução Matemática

A indução matemática ou indução finita (como às vezes é chamada), é uma ferramenta muito poderosa utilizada em muitas demonstrações de resultados sobre os inteiros.

Explicitamente, se B é um subconjunto de $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ satisfazendo

(i) $1 \in B$;

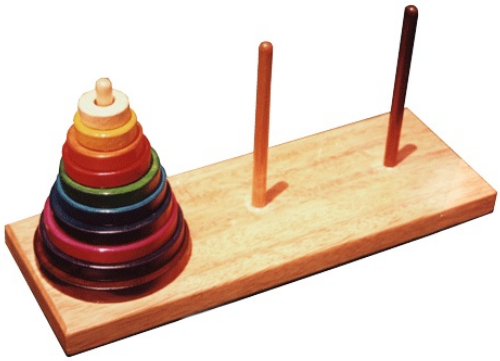
(ii) dado $n \geq 1, n \in B$ implica $n + 1 \in B$,

então $B = \mathbb{N}$.

A justificativa que iremos usar foi inspirada em [5], como mencionamos, tomaremos como base o PBO. A ideia é argumentar por contradição, supondo ser falsa a tese $B = \mathbb{N}$ mesmo sendo válidas as hipóteses i. e ii.. Isto implica que o conjunto $S = \mathbb{N} - B = \{n \in \mathbb{N} : n \notin B\}$ é não vazio. Como $S \subset \mathbb{N}$, segue que S também é limitado inferiormente, o que nos permite aplicar o PBO ao conjunto S. Desta forma existe o menor elemento $s_0 \in S$. Desde que a hipótese i. implica $1 \in B$ concluímos que $s_0 > 1$. Disto $s_0 - 1 \geq 1$ e não pertence a S pois $s_0 - 1 < s_0$ e este é o menor elemento de S. Isso mostra que $s_0 - 1 \in B$ e, pela hipótese ii. (hipótese de indução) $(s_0 - 1) + 1 = s_0 \in B$. Mas isto é uma contradição pois $s_0 \in S = \mathbb{N} - B$. Esta contradição surgiu em consequência de supormos $B \neq \mathbb{N}$, que precisa ser falso, portanto $B = \mathbb{N}$. ■

A indução matemática está presente no nosso cotidiano, como por exemplo, no jogo da torre de Hanói. Este jogo é formado por três hastes em uma das quais está empilhada alguns discos de diâmetro diferentes. Não há um disco de diâmetro menor sob um de diâmetro maior, como mostra a figura Figura 1. O objetivo é mover todos os disco desta haste (um de cada vez) para uma outra, usando a terceira como haste auxiliar, respeitando a regra inicial: não se pode colocar um disco de diâmetro menor sob um de diâmetro maior. A pergunta então é a seguinte: qual o menor número de movimentos necessários para se mover n discos?

Figura 1 – Jogo Torre de Hanói.



Fonte: Produzida pelo autor.

Em [4, p. 87] encontramos uma discussão sobre o princípio de indução matemática como pano de fundo o jogo Torre de Hanói, que resumimos aqui. Como dissemos, o objetivo é determinar o menor número de movimentos necessários para completar o jogo com n discos. Argumentando de forma intuitiva, se tivermos um disco apenas; isto é, se $n = 1$, então será necessário $1 = 2^0$ movimentos. Se $n = 2$ então precisamos mover o disco

menor para a haste auxiliar (haste **B**). O disco maior é movido para a outra haste (haste **C**), e só então o disco menor é movido para lá também. São, portanto, $3 = 2^2 - 1$ movimentos no mínimo. Supondo agora $n = 3$ precisamos mover então o menor disco para haste **C** (movimento 1). O disco médio para haste auxiliar (movimento 2), em seguida movemos também o disco menor para haste auxiliar (movimento 3). Após isso movemos o disco maior para haste **C** (movimento 4), movemos novamente o disco menor para haste **A** (movimento 5). O disco médio para haste **C** (movimento 6) e finalmente o disco menor para haste **C** (movimento 7). Mais uma vez observamos que são necessários no mínimo $7 = 2^3 - 1$ movimentos. Podemos continuar experimentando mais casos, o que empiricamente nos levará a supor que o número mínimo de movimentos necessários para n discos é $N(n) = 2^n - 1$.

O problema com o argumento acima é que indução empírica não é a mesma coisa que indução matemática. Em [8, p. 43] encontramos um exemplo que esclarece perfeitamente a diferença entre as duas. Suponhamos que fizemos a seguinte afirmação sobre os números naturais:

$$\tilde{P}(n) : n = n + (n-1) \cdot (n-2) \cdots (n - 10^6).$$

Certamente esta afirmação e verdadeira para o primeiro milhão de números naturais; isto é, temos um milhão de evidências que nos leva, empiricamente, a acreditar que $\tilde{P}(n)$ é verdadeira para todo $n \geq 1$, mas $\tilde{P}(10^6 + 1)$ é falsa.

Voltando ao nosso exemplo, para mostrarmos que $N(n) = 2^n - 1$ usamos indução matemática. Para tal definimos $P(n) : N(n) = 2^n - 1$ e

$$B = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\}.$$

No passo inicial buscamos saber ser $P(1)$ é verdadeira; ou seja, se o número necessário para mover apenas um disco é $N(1) = 2^1 - 1 = 1$. Como vimos na discussão que fizemos acima; este é o caso e $P(1)$ é verdadeira. Para a etapa indutiva supomos que $P(n)$ é verdadeira para algum $n \geq 1$; isto é, para este n são necessários $N(n) = 2^n - 1$ movimentos (esta é a chamada *hipótese de indução*). Precisamos mostrar, a partir desta hipótese, que $P(n+1)$ é verdadeira; isto é, que $N(n+1) = 2^{n+1} - 1$.

Suponhamos agora que temos no jogo da torre de Hanói $n + 1$ discos. Para movermos o último disco da haste **A** para **C**, devemos primeiro mover todos os n discos anteriores para a haste **B**; isto é, movermos os n discos de **A** para **B**, usando a haste **C** como auxiliar. Isto implica em fazermos no mínimo $N(n)$ movimentos. Depois movemos o último disco para a haste **C**, implicando em mais um movimento. Finalmente, movemos os n discos que estavam na haste **B** para a haste **C**, usando a haste **A** como auxiliar. Isso nos fornece mais $N(n)$ movimentos. Ao todo fizemos no mínimo $N(n) + 1 + N(n) = 2N(n) + 1$

movimentos; isto é

$$N(n+1) = 2N(n) + 1.$$

Usando a hipótese de indução temos $N(n) = 2^n - 1$, logo $N(n+1) = 2(2^n - 1) + 1 = 2^{n+1} - 1$. Disto $P(n+1)$ é verdadeira sempre que $P(n)$ for. Desta forma, segue do princípio de indução matemática que

$$B = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\} = \{n \in \mathbb{N} : n \geq 1\}.$$

■

1.3 Divisão Euclidiana

Como nem sempre é possível expressar uma relação de divisibilidade de um inteiro por outro, segue do Princípio da Boa Ordem que embora em $\mathbb{Z}$ não possamos fazer divisões em geral, existe um processo de divisão muito útil e importante chamado de *divisão com resto*. Mais precisamente:

Definição 1.1 *Dados dois inteiros D e $d \neq 0$ (chamados de* dividendo *e* divisor*, respectivamente), existem inteiros q e r (chamados de* quociente *e* resto*, respectivamente), unicamente determinados por D e d, tais que*

$$D = qd + r, \text{ com } 0 \leq r < |d|.$$

Como dissemos, vamos apresentar uma justificativa para esta afirmação como consequência do PBO. A ideia é considerar o conjunto dos possíveis restos; isto é, o subconjunto $S \subset \mathbb{N}$, cujos elementos são da forma $D - dq$, para algum inteiro $q \in \mathbb{Z}$:

$$S = \{D - qd \in \mathbb{N} : \text{ com } q \in \mathbb{Z}\}$$

Como $S \subset \mathbb{N}$, segue que S é limitado inferiormente. Para usarmos o PBO precisamos mostrar que $S \neq \varnothing$.

Contudo vamos usar um resultado intermediário, chamado por sua vez de **propriedade arquimediana dos inteiros** e que é enunciada da seguinte forma: sejam a e b dois inteiros, com $b \neq 0$. Então existe $q \in \mathbb{Z}$ tal que $q \cdot b \geq a$.

A demonstração dessa propriedade decorre do fato de que, como $b \neq 0$, temos que $\mid b \mid \geq 1$, disto $\mid a \mid\mid b \mid \geq \mid a \mid$.

Se $b < 0$, então $\mid b \mid = -b$, daí $(- \mid a \mid)b \geq \mid a \mid$, isto é $q = - \mid a \mid$. Se $b > 0$, então $\mid b \mid = b$ e $\mid a \mid b \geq \mid a \mid$, logo $q = \mid a \mid$. Em qualquer situação, existe $q \in \mathbb{Z}$ tal que:

$$qb \geq \mid a \mid \geq a.$$

Essa propriedade mostra que existe $q \in \mathbb{Z}$ tal que $q(-d) \geq -D$.(basta fazer $b = -d$ e $a = -D$ e usar o lema para esses valores), logo $n = D - qd \geq 0 \in S$, o que implica em $S \neq \varnothing$, como $\mathbb{Z}$ é bem ordenado, existe um menor elemento s_0 em S, façamos $r = s_0 = D - q_0 d$ para o $q_0 \in \mathbb{Z}$ correspondente. Disto $D = q_0 d + r$ com $r \geq 0$.

Sendo assim, estamos aptos agora para apresentar uma demonstração do teorema da divisão com resto nos inteiros, usualmente encontrada nos livros de álgebra, como em [1, p. 74] então:

Se $r <\mid d \mid$, suponhamos por absurdo, que $r \geq \mid d \mid$. Então existe $s \in \mathbb{N}$ tal que $r = \mid d \mid + s$, como $r = D - q_0 d$ substituindo, obtemos $s + \mid d \mid = D - q_0 d$, disto:

$$s = D - q_0 d - \mid d \mid = D - (q_0 \pm 1)d$$

Onde o sinal (+) ocorre quando $d > 0$ enquanto que o sinal (-) ocorre quando $d < 0$. Em qualquer situação s satisfaz a descrição dos elementos de S; isto é, $s \in S$. Porém $r = s + \mid d \mid$ e $d \neq 0$ mostram que $s < r$ então $s \notin S$, visto que r é o menor elemento de S, esta contradição é o absurdo que procurávamos.

Dela segue que $r \geq \mid d \mid$ é falsa , isto é, $r <\mid d \mid$. Mostramos até aqui que existem $q.r \in \mathbb{Z}$ tais que $D = qd + r$, com $0 \leq r <\mid d \mid$.

Resta - nos mostrar a unicidade desses números, para tal, suponhamos que existam dois outros números q_1, r_1 com as mesmas propriedades, então temos:

$$D = qd + r = q_1 d + r, \quad \text{com} \quad 0 \leq r, r_1 <\mid d \mid$$

Desta forma temos $(q - q_1)d = r_1 - r$ o que implica $\mid q - q_1 \mid \cdot \mid d \mid = \mid r_1 - r \mid$. Da condição sobre r e r_1 segue $0 \leq \mid r_1 - r \mid <\mid d \mid$, o que implica $\mid q - q_1 \mid \cdot \mid d \mid = \mid r_1 - r \mid <\mid d \mid$. Isto só é possível se $\mid q - q_1 \mid = 0$, consequentemente $\mid r_1 - r \mid = 0,$ logo $q = q_1$ e $r_1 = r$. ■

1.4 Relação de Divisibilidade nos Inteiros

Como em $\mathbb{Z}$ nem sempre é possível dividir exatamente um inteiro por outro, a noção de divisibilidade assume um papel importante.

Definição 1.2 *Sejam a e b dois inteiros, com $a \neq 0$. dizemos que a divide b se e somente se existe um inteiro q tal que $b = a \cdot q$. Se a divide b dizemos também que a é um divisor de b, que b é um múltiplo de a, que a é fator de b ou que b é divisível por a*

.

A afirmação a divide b, será simbolizada pela notação $a \mid b$ e sua negação por $a \nmid b$.

Teorema 1 *Quaisquer que sejam os inteiros a, b e c. Tem -se*

(i) $a \mid 0$, $1 \mid a$ e $a \mid a$;

(ii) Se $a \mid 1$, então $a = \pm 1$;

(iii) Se $a \mid b$ e se $c \mid d$, então $ac \mid bd$;

(iv) Se $a \mid b$ e se $b \mid c$, então $a \mid c$;

(v) Se $a \mid b$ e se $b \mid a$, então $a = \pm b$;

(vi) Se $a \mid b$, com $b \neq 0$, então $|a| \leq |b|$;

(vii) Se $a \mid b$ e se $a \mid c$, então $a|(b\mathrm{x} + c\mathrm{y})$, $\forall x, y \in \mathbb{Z}$

A demonstração de i) e ii) saem direto da definição de divisibilidade, faremos a prova de iii) e iv). A demonstração das outras propriedades podem ser encontradas em [1, p. 69]

iii) Com efeito

$$a \mid b \Longrightarrow b = a \cdot q, \text{com } q \in \mathbb{Z}$$

$$c \mid d \Longrightarrow d = c \cdot s, \text{com } s \in \mathbb{Z}$$

Portanto:

$$b \cdot d = ac \cdot qs \Longrightarrow ac \mid bd.$$

iv) Com efeito

$$a \mid b \Longrightarrow b = a \cdot q, \text{com } q \in \mathbb{Z}^* = \mathbb{Z} - \{0\}$$

$$b \mid c \Longrightarrow c = b \cdot s, \text{com } s \in \mathbb{Z}$$

Portanto:

$$c = a \cdot (qs) \Longrightarrow a \mid c.$$

Na próxima seção apresentaremos o Algoritmo de Euclides, um método que permite calcular efetivamente o máximo divisor comum entre dois inteiros.

1.5 Algoritmo de Euclides

Antes de falarmos sobre esse algoritmo, iniciaremos com a definição de *máximo divisor comum (mdc)*. O máximo divisor comum entre a e b, que denotaremos por (a, b), é o **maior** inteiro positivo **d** que é divisor comum de a e b. Se $(a, b) = 1$, dizemos que a e b são *primos entre si* ou *coprimos*. Podemos generalizar essa ideia para calcular o mdc de uma quantidade finita de números inteiros, vejamos a definição a seguir:

Definição 1.3 *Sejam $a_1, \cdots, a_s$ elementos do anel $\mathbb{Z}$. Diremos que $d \in \mathbb{Z}$ é um máximo divisor comum (mdc) de $a_1, \cdots, a_s$, se as seguintes condições são verificadas:*

(i) $d \mid a_i, \forall i = 1, \cdots, s$;

(ii) $\forall c \in \mathbb{Z}$, *se* $c \mid a_i, \forall i = 1, \cdots, s$, *então* $c \mid d$.

Segundo [9, p. 29], o algoritmo de Euclides já era conhecido na Grécia Antiga, cuja descrição está feita nos elementos de Euclides, escrito em 300 a.C. O método é um primor do ponto de vista computacional e pouco conseguiu - se aperfeiçoá - lo. A origem da palavra algoritmo é curiosa, inicialmente a palavra era escrita *algorismo*. Algorismo ganhou um "t" por conta da palavra "aritmos", que também significa número em grego. O sentido atual da palavra algoritmo é recente, sendo atestada, em inglês, apenas em 1812.

Não faremos aqui a demonstração do Algoritmo de Euclides minuciosamente, pois a mesma se dá de forma construtiva, ou seja, a partir da demonstração desse algoritmo podemos de fato calcular o **mdc** de dois números, mas para quem tiver interesse nos detalhes ela pode ser encontrada em [9]. . Sejam a e b inteiros tais que $a \geq b$. Queremos calcular o máximo divisor entre a e b. O algoritmo de Euclides consiste em dividir a por b, achando o resto r_1. Se $r_1 \neq 0$, dividimos **b** por r_1, obtendo o resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2, obtendo o resto r_3. E assim sucessivamente. O último resto **diferente de zero** desta sequencia é o máximo divisor comum entre a e b. Com ajuda de um quadro resumimos o algoritmo da seguinte forma:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

.

Onde $r_n = (a, b)$ é o último resto não nulo das divisões sucessivas. Vejamos o seguinte exemplo, calculemos o **mdc** de 392 e 260. Aplicando o algoritmo no quadro acima, teremos:

Quociente	1	1	1	32
392	260	132	128	4
132	128	4	0	

Logo o $(392, 260) = 4$.

Notemos que a sequencia de divisões não é infinita, isto é, num certo momento este processo acabará, pois da divisão euclidiana temos $d > r_0 > r_1 > r_2 > \cdots$, e se a sequencia de restos não acabasse, em algum momento teríamos um resto negativo, o que é um absurdo). Sendo assim, o último resto não nulo será o máximo divisor comum.

Teorema 2 *Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros x e y tais que $(a, b) = a \cdot x + b \cdot y$. Em outras palavras, a relação diz que o (a, b) pode ser escrito como combinação linear de x e y.*

A demonstração desse teorema pode ser encontrada em [6, 8]. Na próxima seção discutiremos um pouco sobre as Equações Diofantinas.

1.6 Equações Diofantinas

O estudo das Equações Diofantinas é tarefa básica dos cursos de aritmética e de introdução à álgebra. Diofanto viveu no século III em Alexandria, foi praticamente o único matemático de renome na Grécia Antiga que se dedicou à teoria dos números [8].

Atualmente as Equações Diofantinas são conhecidas como equações polinomiais com coeficientes inteiros, para as quais só se está interessado em soluções inteiras ou racionais. As equações Diofantinas das quais trataremos aqui são do tipo:

$$ax + by = n$$

com a, b e n números inteiros. Dada uma equação é natural fazermos alguns questionamentos tais como, sob quais condições a equação admite solução? Quando existem soluções, como determiná - las? As respostas desses questionamentos serão dadas pelas duas proposições a seguir.

Teorema 3 *A equação $ax + by = n$ admite solução se, e somente se, $(a, b) \mid n$.*

Demonstração: Suponhamos que a equação admita uma solução x_0, y_0, isto é, $a \cdot x_0 + b \cdot y_0 = n$. Como (a, b) divide a e divide b, segue que divide $a \cdot x_0 + b \cdot y_0 = n$. Por outro lado,

suponhamos que $(a,b) \mid n$. Então existe um inteiro t tal que $n = t \cdot (a,b)$. Como existem inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a,b)$, segue que $n = t \cdot (a,b) = t \cdot (a,b) = (t \cdot m_0) \cdot a + (t \cdot n_0) \cdot b$. Logo os inteiros $x_0 = t \cdot m_0$ e $y_0 = t \cdot n_0$ são uma solução da equação.

O resultado seguinte mostra como determinar as soluções das equações Diofantinas.

Teorema 4 *Seja x_0, y_0 uma solução particular da equação $ax + by = n$. Tem - se que x, y é uma solução se, e somente se,*

$$x = x_0 + t \cdot \frac{b}{(a,b)} \quad e \quad y = y_0 - t \cdot \frac{a}{(a,b)}$$

para algum $t \in \mathbb{Z}$. Omitiremos a sua demonstração, mas ela pode ser encontrada em [8, p. 102] . Para fixar bem esse assunto faremos os seguinte exemplos:

Exemplo 1: A equação $9x + 12y = 1$ possui solução nos inteiros?

Solução Não, pois $(9, 12) = 3$ e 3 não divide 1.

Exemplo 2: A equação $28x + 90y = 22$ possui solução nos inteiros?

Solução Primeiramente temos que calcular o $(28, 90)$. Usando o Algoritmo de Euclides temos:

Quociente	3	4	1	2
90	28	6	4	2
6	4	2	0	

, daí como $(28, 90) = 2$ e $2 \mid 22$, segue que a equação admite soluções. Usando o algoritmo de trás para frente, temos

$$\begin{aligned} 2 &= 6 - 1 \cdot 4 \\ 4 &= 28 - 4 \cdot 6 \\ 6 &= 90 - 3 \cdot 28 \end{aligned}$$

Segue que:

$$\begin{aligned} 2 = 6 - 1 \cdot (28 - 4 \cdot 6) &= (-1) \cdot 28 + 5 \cdot 6 \\ &= (-1) \cdot 28 + 5 \cdot (90 - 3 \cdot 28) \\ &= (-16) \cdot 28 + 5 \cdot 90 \end{aligned}$$

Portanto, $2 = (-16) \cdot 28 + 5 \cdot 90$, multiplicando ambos os membros desta igualdade por 11, obtemos:

$$22 = (-176) \cdot 28 + 55 \cdot 90$$

Sendo assim, uma solução particular da equação é dada por $(x_0, y_0) = (-176, 55)$. Portanto, pelo teorema (4), a solução geral é:

$$x = -176 + t \cdot 45 \quad e \quad y = 55 - t \cdot 14, \quad t \in \mathbf{Z}$$

O próximo resultado é conhecido como Lema de Gauss.

Lema 1.1 *Dados $d, m, n \in \mathbb{Z}$. Se $d \mid m \cdot n$ e $(d, m) = 1$, então $d \mid n$.*

Demonstração: Da primeira hipótese temos que, se $d \mid m \cdot n$,então existe um número e inteiro tal que: $d \cdot e = m \cdot n$, enquanto que a segunda hipótese afirma que $(d, m) = 1$, então da relação de Bèzout, existem inteiros x e y tais que $d \cdot x + m \cdot y = 1$, multiplicando essa igualdade dos dois lados por n ficamos com $d \cdot x \cdot n + m \cdot y \cdot n = n$, substituindo $m \cdot n$ por $d \cdot e$, temos $d \cdot x \cdot n + d \cdot e \cdot y = n \Rightarrow d \cdot (x \cdot n + e \cdot y) = n$, então $d \mid n$.

Teorema 5 *Sejam $a,\ b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b \mid a^n - b^n$.*

Demonstração: Usaremos indução sobre n . É claro que a afirmação é verdadeira pra $n = 1$, pois $a - b \mid a^1 - b^1 = a - b$.
Suponhamos, que $a - b \mid a^n - b^n$. Escrevamos:

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n).$$

Como $a-b \mid a-b$ e, por hipótese, $a-b \mid a^n-b^n$, segue da igualdade acima e do teorema (1), que $a - b \mid a^{n+1} - b^{n+1}$, logo por indução matemática a proposição é verdadeira para todo $n \in \mathbb{N}$.
Uma importante aplicação dessa proposição é o fato de que todo número na forma $10^n - 1$, onde n é natural, seja divisível por 9. Com efeito, basta tomar $a = 10$ e $b = 1$, daí $a-b = 9$ divide $a^n - b^n = 10^n - 1$

Teorema 6 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$*

Teorema 7 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$*

As demonstrações dessas proposições também são feitas por indução sobre n, elas podem encontradas em [9, p. 48] . Daremos ênfase na próxima seção aos números primos, cuja sua importância ocupa lugar de destaque na matemática e desempenham um papel fundamental no desenvolvimento da teoria dos números.

1.6.1 Números Primos

Um dos assuntos mais importantes da matemática sem dúvida nenhuma são os números primos, pois eles desempenham um papel importante na teoria dos números, sem falar que eles são os principais responsáveis por existirem muitos problemas famosos que até hoje depois de algumas gerações de matemáticos permanecem em aberto.

É de conhecimento da grande maioria que a matéria é formada por pequenas partículas: os átomos. Segundo [3], os gregos antigos foram os primeiros a saber que a matéria é formada por tais partículas e o filósofo grego Demócrito (que viveu entre 546 e 460 a.C.) foi quem denominou essas partículas de átomos (do grego – a: não; tomo: divisão), pois acreditava que, de fato, elas eram indivisíveis. Hoje se sabe que os átomos podem ser divididos em partículas menores, mas a ideia de que a matéria existe em "unidades mínimas" segue vigente...

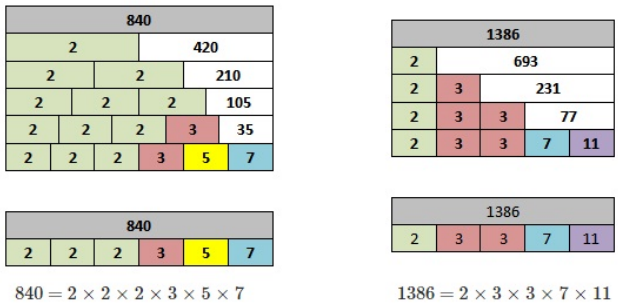
Na aritmética, essa ideia de "unidades mínimas" também existe e também remete da Grécia Antiga. Só que o papel dos átomos, neste caso, é exercido pelos chamados números primos. Os pitagóricos (de 500 a 300 a.C., mais ou menos) foram os primeiros a se interessarem pelas propriedades "místicas" desses números. Mas, diferentemente dos átomos de verdade, os números primos continuam, e vão continuar, funcionando como blocos numéricos fundamentais, responsáveis por gerar todos os números naturais diferentes de 0 e de 1, ou seja, sempre será possível escrever um número natural que não é primo e que seja diferente de 0 e de 1 como produto de números primos, conforme ilustra a figura a seguir.

Esta propriedade é conhecida como Teorema Fundamental da Aritmética – TFA, que será apresentada na subseção seguinte.

Definição 1.4 *Um número inteiro p é primo se $p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$ Um inteiro que não é primo é chamado de composto, ou seja, possui mais de dois divisores.*

Exemplos: Os números 2, 3, 5, 7, 11, 13 são primos, já os números 4, 6, 9, 12 são compostos Um importante teorema dessa seção é o seguinte:

Figura 2 – Bloco dos Primos.



Fonte: Clube de Matemática, adaptada pelo autor.

Teorema 8 (Teorema Fundamental da Aritmética) *Dados um inteiro positivo* $n \geq 2$ *podemos sempre escrevê - lo, de modo único, na forma*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < \cdots < p_k$ *são números primos e* $e_1, e_2, \cdots e_k$ *são inteiros positivos*

Este teorema nos diz duas coisas, a primeira é que todo inteiro pode ser escrito como produto de potências de primos, e a segunda é que só há uma escolha possível de primos e expoentes para a fatoração de um inteiro dado. A demonstração pode ser encontrada em [5, 6].

Um resultado muito importante para o nosso estudos é o chamado lema de Euclides.

Lema 1.2 *Dados* $a, b, p \in \mathbb{Z}$*, com* p *primo. se* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração: Basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Com efeito, suponhamos então que $p \mid ab$ e $p \nmid a$. Segue que $(p, a) = 1$, daí segue do teorema (2) que existem r e s inteiros tais que $ra + sp = 1$. Multiplicando esta ultima igualdade por b tem -se que $rab + spb = b$. Mas $p \mid ab$ e $p \mid p$, portanto $p \mid b$ como desejávamos.

A fatoração de números inteiros em primos revela toda a estrutura multiplicativa desses números, permitindo entre outras coisas, determinar facilmente o máximo divisor comum (mdc) e o mínimo múltiplo comum (mmc) de um conjunto de números naturais, como mostra o teorema seguinte. Usamos a notação: $[a, b] = mmc(a, b)$ para representar o mínimo múltiplo comum entre dois números.

Teorema 9 *Sejam* $a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n}$ *pondo* $\gamma_i = min\{\alpha_i, \beta_i\}$; $\delta_i = max\{\alpha_i, \beta_i\}$, *com* $i = 1, \cdots n$, *tem -se que*

$$(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \text{ e } [a, b] = p_1^{\delta_1} \cdots p_n^{\delta_n}.$$

Demonstração: De fato, como $p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ é um divisor comum de a e b. Seja c um divisor de a e b, logo, $c = \pm p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}$, onde $\varepsilon_i \leq min\{\alpha_i, \beta_i\}$ e, portanto, $c \mid p_1^{\gamma_1} \cdots p_n^{\gamma_n}$. Do mesmo modo, prova - se a outra afirmação do mmc.

Daremos um passo importante no nosso trabalho a partir da próxima seção, visto que ela é o elo que unirá todos os conceitos abordados anteriormente com os conceitos posteriores.

1.7 Sistema de numeração

O sistema universal de numeração utilizado pelas pessoas para representar os números inteiros é **o sistema decimal posicional**, desenvolvido pelos chineses e indianos. No entanto, esse não foi o primeiro sistema de numeração, antes desse usavam - se o sistema de numeração egípcio, romano e babilônicos, mas devida a pouca praticidade operatória o sistema decimal posicional começou a ser amplamente difundido.

Segundo [8, p. 60] foi no Oriente Médio que a introdução do sistema posicional foi bem aceita e as caravanas ajudou a difundi - lá, porém por causa do preconceito, a difusão na Europa foi tardia somente partir de 1202, quando Fibonacci fez a publicação no seu livro *Liber Abacci*, mas somente após vários séculos, esse sistema foi adotado sem restrições pelos europeus.

Atualmente existem outros sistemas de numeração em uso, como por exemplo o sistema binário, que é bastante usado na computação. É importante enfatizar que tanto o sistema decimal, quanto o binário e outros são sistemas posicionais com base constante. Focaremos na representação dos números naturais, pois 0 tem seu próprio símbolo e os inteiros negativos é precedido pelo sinal -, faremos também algumas conversões da base de um sistema para outra.

1.7.1 Alguns sistemas de numeração posicional

Iniciaremos explorando o sistema decimal, todo número inteiro é representado por uma sequência formada pelos algarismos $1, 2, 3, 4, 5, 6, 7, 8, 9$ acrescido do símbolo 0. Esse sistema recebe esse nome por ser constituído de 10 algarismos.

De acordo com a posição, cada algarismo assumirá um peso além do seu valor próprio, esse peso, sempre é uma potência de dez, começando da direita do número, ou seja, o algarismo da extrema direita tem peso um; o seguinte peso 10; o seguinte peso 100, sempre da direita para esquerda; o seguinte peso 1000 e assim por diante.

Por exemplo, o número 13079, na base 10, é representado por:

$$1 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10 + 9$$

Cada algarismo possui uma ordem contada da direita para esquerda e a cada terna de ordens, também contada da direita para esquerda, forma - se uma classe. isto é,

Classe das unidades.

$$(\overbrace{\text{centenas}}^{3^{\text{a}}ordem}, \overbrace{\text{dezenas}}^{2^{\text{a}}ordem}, \overbrace{\text{unidades}}^{1^{\text{a}}ordem}),$$

Classe do milhar

$$(\overbrace{\text{centenas de milhar}}^{6^{\text{a}}ordem}, \overbrace{\text{dezenas de milhar}}^{5^{\text{a}}ordem}, \overbrace{\text{unidades de milhar}}^{4^{\text{a}}ordem})$$

Classe do milhão

$$(\overbrace{\text{centenas de milhão}}^{9^{\text{a}}ordem}, \overbrace{\text{dezenas de milhão}}^{8^{\text{a}}ordem}, \overbrace{\text{unidades de milhão}}^{7^{\text{a}}ordem})$$

Utilizando o número acima como exemplo temos:

Classe das unidades. $(\overbrace{0}^{3^{\text{a}}ordem}, \overbrace{7}^{2^{\text{a}}ordem}, \overbrace{9}^{1^{\text{a}}ordem})$, **Classe do milhar** $(\overbrace{0}^{6^{\text{a}}ordem}, \overbrace{1}^{5^{\text{a}}ordem}, \overbrace{3}^{4^{\text{a}}ordem})$

A próxima proposição é uma aplicação muito importante da divisão euclidiana e uma forma muito eficaz de representar um número a numa base b qualquer.

Teorema 10 *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, \ldots, r_n < b$, com $r_n \neq 0$, univocadamente determinados, tais que $a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n$.*

Demonstração: Essa demonstração é feita por [9, p. 68], usando indução completa sobre a. Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. A unicidade da escrita é clara nesse

caso. Suponhamos o resultado válido para todo natural menor do que a, onde $a \geq b$. Provaremos para a, pela divisão euclidiana, existem q e r, únicos, tais que:

$$a = bq + r, \text{ com } 0 \neq r < b.$$

Como $0 < q < a$, pela hipótese de indução, segue - se que existem números inteiros $n' \geq 0$ e $0 \leq r_1, \cdots r_{n'+1} < b$, com $r_{n'+1} \neq 0$, univocamente determinados, tais que:

$$q = r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}.$$

De acordo com essa última igualdade, temos que

$$a = bq + r = b(r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}) + r,$$

donde o resultado segue -se pondo $r_0 = r$ e $n = n' + 1$.

Essa representação acima é chamada de expansão relativa à base b, quando $b = 10$, essa expansão é dita *expansão decimal*, e quando $b = 2$ recebe o nome de *expansão binária*.

Para obtermos a expansão de um número numa base b qualquer, basta aplicar sucessivamente a divisão euclidiana, como segue.

$$a = bq_0 + r_0, \quad r_0 < b,$$

$$q_0 = bq_1 + r_1, \quad r_1 < b,$$

$$q_1 = bq_2 + r_2, \quad r_2 < b,$$

e assim por diante. Como $a > q_0 > q_1 > \cdots$, deveremos, em um certo momento, ter

$$q_{n-1} = bq_n + r_n.$$

Decorre que $q_n = 0$, o que implica $0 = q_n = q_{n+1} = q_{n+2} = \cdots$, e portanto, $0 = r_{n+1} = r_{n+2} = \cdots$. Assim, temos:

$$a = r_0 + r_1 b + \cdots + r_n b^n.$$

A próxima proposição aborda como devemos comparar dois números inteiros escritos em bases diferentes.

Teorema 11 *Sejam dados os números inteiros* $b > 1, n, n' \geq 0, 0 \leq r_0, \cdots r_n < b$ *e* $0 \leq r'_0, \cdots, r'_{n'} < b$, *tem -se:*

(i) $r_0 + r_1 b + \cdots + r_n b^n < b^{n+1}$;

(ii) $n > n'$ *e* $r_n \neq 0 \Longrightarrow r_0 + r_1 b + \cdots r_n b^n > r'_0 + r'_1 b + \cdots + r'_{n'} b^{n'}$;

(iii) $n = n'$ e $r_n > r'_n \Longrightarrow r_0 + r_1 b + \cdots r_n b^n > r'_0 + r'_1 b + \cdots + r'_n b^n$

A demostração dessa proposição pode ser encontrada no livro do [9]. Para expandir um certo número numa certa base, necessitamos de um conjunto S de b símbolos.

$$S = \{s_0, s_1, \cdots, s_{b-1}\},$$

Assim um número natural a na base b escreve - se na forma:

$$x_n x_{n-1} \cdots x_1 x_0.$$

Com $x_n, x_{n-1}, \cdots x_1, x_0 \in S$ e n variando, dependendo de a, representando o número

$$x_0 + x_1 b + \cdots + x_n b^n.$$

Na base $b = 10$, usa - se

$$S = \{0, 1, 2, \cdots, 9\}$$

Se $b \leq 10$ usaremos os símbolos $\{0, 1, 2, \cdots, b-1\}$. Se $b > 10$, usaremos os símbolos anteriores acrescido de outros.
Na base 2, temos que

$$S = \{0, 1\}.$$

Na base 12, temos que

$$S = \{0, 1, \cdots, 9, A, B\},$$

onde os dois últimos símbolos foram inventados para representar a quantidade 10 e 11.

Resumindo, temos:

$$\text{base } 2 = \{0, 1\};$$

$$\text{base } 3 = \{0, 1, 2\};$$

$$\vdots$$

$$\text{base } b = \{0, 1, \cdots, b-1\}.$$

A ideia de poder escrever um mesmo número em qualquer base numérica é bastante evidente. Logicamente, dependendo da base numérica utilizada, o número é representado de uma forma diferente, por exemplo o número 3 na base 10 é representado por 11 na base 2.

Para evitar confusão, usaremos a notação $[x_n \cdots x_1 x_0]_b$ para significar que o número é representado por $x_n \cdots x_1 x_0$ na base b. Se a base numérica não for especificada, considere a base numérica usual, ou seja, a decimal. Assim, temos que:

$$[x_n \cdots x_1 x_0]_b = x_0 + x_1 b + \cdots + x_n b^n$$

Logo $[100]_2 = 0+0\cdot 2+1\cdot 2^2 = 4$, $[111]_2 = 1+1\cdot 2+1\cdot 2^2 = 7, [1210]_3 = 0+1\cdot 3+2\cdot 3^2+1\cdot 3^3 = 48, [11]_5 = 1+1\cdot 5 = 6, [123]_5 = 3+2\cdot 5+1\cdot 5^2 = 38$.
Faremos a conversão do número 37 na base 10 para base 3. Faremos isso por divisões euclidiana sucessivas,

$$\begin{aligned} 37 &= 12\cdot 3+1 \\ 12 &= 4\cdot 3+0 \\ 4 &= 1\cdot 3+1 \\ 1 &= 0\cdot 3+1 \end{aligned}$$

Daí, temos que $37 = [1101]_3$.
No próximo exemplo faremos o contrário, isto é converteremos o número $[257]_8$ para base dez. Começamos notando que para escrever um número na base 8 só são utilizado algarismo de 0 a 7, assim:

$$[257]_8 = 7+5\cdot 8+2\cdot 8^2 = 175.$$

Perceba que os exemplos anteriores ou queríamos passar da base 10 para outra base b qualquer ou queríamos o contrário, mas se quiséssemos ir de uma base b para uma outra base b' qualquer sem ser a base 10, como faríamos?

Bom para responder a essa questão, faremos essa conversão em duas etapas, primeiro passaremos da base b para base 10 e em seguida da base 10 para base b', para ficar claro, mostraremos como converter o número $[1124]_5$ para base 11. Assim a primeira etapa é converter para base 10:

$$[1124]_5 = 4+2\cdot 5+1\cdot 5^2+1\cdot 5^3 = 164$$

a segunda etapa é realizar as divisões sucessivas para converter para base 11:

$$\begin{aligned} 164 &= 14\cdot 11+10 \\ 14 &= 1\cdot 11+3 \\ 1 &= 0\cdot 11+1 \end{aligned}$$

encontrando $[13A]_{11}$. Portanto $[1124]_5 = [13A]_{11}$.

A próxima seção é de grande importância, não apenas por ser um dos temas centrais desse trabalho, mas também para uma boa compreensão dos capítulos seguintes, pois a partir dela ganharemos uma bagagem algébrica e aritmética que será intensamente usada nas demonstrações das proposições seguintes.

1.8 Aritmética modular

O conhecimento da aritmética modular tem grandes utilidades não só teóricas, mas também práticas no nosso cotidiano, começaremos esta seção com um exemplo dessa segunda utilidade. Como se identifica as pessoas aqui no Brasil? Muitos diriam que se identifica uma pessoa pelo seu nome, porém existem várias pessoas que possuem o mesmo nome, logo apenas o nome não é suficiente para a identificação de uma pessoa.

Em sua dissertação, [2, p. 86], afirma que é através do Cadastro de Pessoas Físicas - CPF, junto a Receita Federal que ocorre a identificação de uma pessoa, pois o mesmo além de ser único, é intransferível, o CPF é composto por 11 dígitos, no qual os dois últimos dígitos são de controle, a congruência modular aparece quando se quer determinar os dois dígitos de controle.

Figura 3 – Cadastro de Pessoa Física - CPF

Fonte: Produzida pelo autor.

Para isso basta usar congruência módulo 11 de um número e seguir o algoritmo. Primeiro atribuímos pesos a cada um dos 9 dígitos, isto é $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ devem ser multiplicados pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ nessa ordem, o segundo passo é somar todos os produtos obtido, essa soma será denotada por S e o décimo dígito a_{10}, será o resto da divisão da soma S por 11, isto quer dizer que $S - a_{10}$ é múltiplo de 11, ou que S menos a_{10} é congruente a zero módulo 11.

Se tomarmos o CPF, cujo os 9 primeiros dígitos são 046 876 654, poderemos calcular os dígitos de controle seguindo o que foi dito:

$$0 \cdot 1 + 4 \cdot 2 + 6 \cdot 3 + 8 \cdot 4 + 7 \cdot 5 + 6 \cdot 6 + 6 \cdot 7 + 5 \cdot 8 + 4 \cdot 9 = 247$$

Fazendo a divisão euclidiana de 247 por 11, temos $247 = 22 \cdot 11 + 5$, logo $a_{10} = 5$, para achar o décimo primeiro dígito (segundo dígito de controle), basta seguir o mesmo algoritmo, porém agora devemos acrescentar o a_{10} aos noves primeiro dígitos e multiplicamos agora pela base $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, Novamente o resto da divisão da soma S por 11 resulta no décimo primeiro dígito. Assim:

$0 \cdot 0 + 4 \cdot 1 + 6 \cdot 2 + 8 \cdot 3 + 7 \cdot 4 + 6 \cdot 5 + 6 \cdot 6 + 5 \cdot 7 + 4 \cdot 8 + 5 \cdot 9 = 246$

Da divisão euclidiana de 246 por 11, temos $246 = 22 \cdot 11 + 4$, logo $a_{11} = 4$, se o resto da divisão em algum dos dois caso fosse 10 usaríamos o dígito zero. Portanto o CPF completo é 046 876 654 54.

Uma outro exemplo, mas agora teórico seria determinar o resto da divisão de 7^{10} por 51, deixaremos para mostrar a solução desse exemplo depois que explorarmos algumas definições e resultados.

Definição 1.5 *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, dizemos que a e b são congruentes módulo m se o resto da divisão euclidiana por m são iguais, escrevemos: $a \equiv b \ mod \ m$*

$$a \equiv b \ mod \ m$$

Um exemplo é $35 \equiv 5 \ mod \ 10$, pois ambos deixam restos iguais na divisão por 10. Se a congruência acima for falsa dizemos que a e b são *incongruentes módulo m* e escreveremos

$$a \not\equiv b \ mod \ m$$

Como o resto da divisão de um número qualquer por 1 é sempre nulo. Então $a \equiv b \ mod \ 1$, quaisquer que sejam a e $b \in \mathbb{Z}$. Logo torna - se pouco interessante a aritmética dos restos módulo 1, logo $m > 1$.

Não é necessário dividir dois números por m para saber se eles são congruentes módulo m, basta aplicar a seguinte proposição:

Teorema 12 *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem - se que $a \equiv b \ mod \ m$ se, e somente se, $m \mid b - a$.*

Demonstração: Faremos a divisão euclidiana de a e b por m obtendo então que: $a = m \cdot q + r$ e $b = mq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$ e $0 \leq r, r' < m$. Então, temos que:

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

$$b - a = m \cdot (q' - q) + (r' - r),$$

Portanto, segue que $a \equiv b \ mod \ m$ se, e somente se, $r = r'$, o que da igualdade acima é equivalente a $m \mid b - a$, já que $\mid r' - r \mid < m$.

Os próximos três itens da proposição abaixo nos fornecem que a congruência módulo m é na verdade uma relação de equivalência, os demais resultados são de compatibilidade da relação de adição e multiplicação e nos auxiliaram nas demonstrações dos critérios de divisibilidade. As demonstrações são semelhantes às encontradas em [1, p. 152].

Teorema 13 *Sejam $a, b, c, d, m, n \in \mathbb{Z}$, com $m > 1$ e $n \geq 1$. Temos que:*

(i) $a \equiv a \ mod \ m$;

(ii) *Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$;*

(iii) *Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$;*

(iv) *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$ então $a + c \equiv b + d \ mod \ m$;*

(v) *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a \cdot c \equiv b \cdot d \ mod \ m$*

(vi) *Se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$*

Demonstração: Começaremos com a primeira propriedade (i), conhecida como reflexiva. De fato a diferença $a - a$ é múltiplo de m, pois o zero é múltiplo de qualquer inteiro. A segunda propriedade (ii) é a simétrica, se $a \equiv b \ mod \ m$, então $a - b$ é múltiplo de m, mas $b - a = -(a - b)$, logo $b - a$ também é múltiplo de m, portanto $b \equiv a \ mod \ m$. A terceira propriedade (iii) é a transitividade, suponhamos que $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, assim temos que $a - b$ é múltiplo de m e $b - c$ é múltiplo de m somando múltiplos de m resulta em múltiplos de m. Logo $(a - b) + (b - c) = (a - c)$ é um múltiplo de m, daí concluímos que $a \equiv c \ mod \ m$. Sendo assim, a congruência módulo m é de fato uma relação de equivalência. As próximas propriedades não tem um nome específico, (iv) temos que $m \mid b - a$ e $m \mid d - c$, logo temos que $m \mid (b - a) + (d - c)$, ou seja, $m \mid (b + d) - (a + c)$, consequentemente $a + c \equiv b + d \ mod \ m$, (v), temos que $m \mid b - a$ e $m \mid d - c$, assim $m \mid (b - a) \cdot d$ e $m \mid (d - c) \cdot a$, então $m \mid (b - a) \cdot d + (d - c) \cdot a$ e como, $(b - a) \cdot d + (d - c) \cdot a = b \cdot d - a \cdot d + a \cdot d - a \cdot c = b \cdot d - a \cdot c$, então $m \mid b \cdot d - a \cdot c$. Portanto $a \cdot c \equiv b \cdot d \ mod \ m$. A sexta propriedade (vi) segue imediatamente da (v)

Agora estamos aptos a mostrar a solução do segundo exemplo que mencionamos no início dessa seção, no qual queríamos descobrir saber qual o resto da divisão euclidiana de 7^{10} por 51. Sabemos que $7^2 = 49$ e que $49 + 2 \equiv 0 \ mod \ 51$, então $7^2 + 2 \equiv 0 \ mod \ 51 \Rightarrow 7^2 \equiv -2 \ mod \ 51$, pelo teorema (12) e pelo item (**vi**) do teorema (13), temos que $(7^2)^5 \equiv (-2)^5 \ mod \ 51 \Rightarrow 7^{10} \equiv -32 \ mod \ 51$ e pela divisão euclidiana segue que - 32 por 51 é $-32 = 51 \cdot (-1) + 19$, isto é, $-32 \equiv 19 \ mod \ 51$. Portanto $7^{10} \equiv 19 \ mod \ 51$.

Teorema 14 *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. tem - se que $a + c \equiv b + c \ mod \ m \Leftrightarrow a \equiv b \ mod \ m$.*

Demonstração: Como $a \equiv b \ mod \ m$ e pelo item (**i**) do teorema (12), temos $c \equiv c \ mod \ m$, daí, pelo teorema (13) item (**iv**), temos $a + c \equiv b + c \ mod \ m$. Reciprocamente se $a + c \equiv b + c \ mod \ m$, temos então pelo teorema (12):

$$m \mid (b + c) - (a + c) \text{ mas } (b + c) - (a + c) = b - a, \text{ então } m \mid b - a.$$

consequentemente $a \equiv b \ mod \ m$.

Teorema 15 *Sejam $a, b, c, m, n \in \mathbb{Z}$ com $m > 1$. tem - se que.*

(i) *Se $a \cdot c \equiv b \cdot c \ mod \ m \Leftrightarrow a \equiv b \ mod \ \frac{m}{(c,m)}$;*

(ii) *Se $a \cdot c \equiv b \cdot c \ mod \ m$, com $(c, m) = 1$, então $a \equiv b \ mod \ m$.;*

(iii) *Se $a \equiv b \ mod \ m$ e se $n \mid m$, então $a \equiv b \ mod \ n$;*

(iv) *$a \equiv b \ mod \ m$ e $a \equiv b \ mod \ n$ se, e somente se, $a \equiv b \ mod \ [n, m]$, onde $[n, m]$ é o mínimo múltiplo comum entre n e m.*

A demonstração desse teorema pode ser encontrada em [1, p. 154] .

Apresentaremos no próximo capítulo, alguns critérios de divisibilidade usuais, bem como as suas respectivas demonstrações.

2 Critérios de Divisibilidade Usuais

As demonstrações dos critérios de divisibilidade que vamos apresentar foram inspiradas em [3] e [11]. Chega a ser intrigante quando nos deparamos pela primeira vez com "macetes", regras ou os chamados critérios de divisibilidade, pois nos vem logo a mente os seguintes questionamentos: Como surgiram? Sempre funcionam para qualquer número inteiro? Já foram testadas? Neste capítulo iremos responder a esses e outros questionamentos.

2.1 Definição

Os critérios de divisibilidade surgem da necessidade de saber se um número n é divisível por um número m sem precisar de fato realizar o algoritmo da divisão euclidiana. Eles tem, portanto, o papel no que diz respeito a praticidade. Os critérios são consequências da maneira como representamos usualmente os números naturais: utilizando o sistema decimal, tema esse abordado no capítulo anterior.

Definição 2.1 *Fixado um número natural não nulo d, um critério de divisibilidade é uma condição P necessária e suficiente para que um número natural seja divisível por d,ou seja um número natural n é divisível por d se, e somente se, a condição P é satisfeita.*

Isso não só significa que “se P for satisfeita, então n é divisível por d”, mas também significa que “se a condição P não for satisfeita, então n não é divisível por d”.

Na seção 1.7 do capítulo anterior apresentamos que representamos os números naturais por uma sequência finita de um ou mais dentre os dez algarismos que caracterizam o sistema { 0 1 2 3 4 5 6 7 8 9 }. Em cada sequência, os algarismos (também chamados de dígitos) representam múltiplos de potências de dez, o que caracteriza o sistema que utilizamos como um sistema posicional. A soma dos múltiplos das potências de dez relativas a uma dada sequência determina, de modo único, o número que ela representa. Um exemplo:

$$675 = 6 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0.$$

Iremos abordar nas próximas seções os critérios de divisibilidade mais usados tais como os critérios de divisibilidade por: 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11.

2.2 Critério de divisibilidade por 2

Um número natural $n = a_r a_{r-1} \cdots a_2 a_1 a_0$ é divisível por 2 se, e somente se seu último algarismo for terminado em 0, ou 2, ou 4, ou 6, ou 8.

Demonstração: Para demonstrar esse primeiro critério, basta observar que se n é um número natural na base 10 da forma

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

, então podemos reescrevê-lo na forma $n = 10 \cdot k + a_0$, com $k \in \mathbb{N}$. Como 10 é divisível por 2, então n será divisível por 2 se, e somente se, a_0(algarismo) for divisível por 2, ou seja, a_0 será divisível por 2 se, e somente se, $a_0 = 0$, ou $a_0 = 2$, ou $a_0 = 4$, ou $a_0 = 6$ ou $a_0 = 8$, apresentaremos outra justificativa desse critério usando a linguagem da congruência.

Consideremos $n \in \mathbb{N}$ na base dez tal que $n = a_r \cdot 10^r + \cdots a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$. Observemos que $10 \equiv 0 \; mod \; 2$ e pelo teorema (13) no item **vi**, temos que $10^r \equiv 0 \mod 2$, com $r \in \mathbb{N}$, assim temos que $10^1 \equiv 0 \; mod \; 2, 10^2 \equiv 0 \; mod \; 2$, e assim por diante até $10^r \equiv 0 \mod 2$. Do item **v** do mesmo teorema, segue que $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv a_0 \; mod \; 2$, ou seja, $2 \mid n$ se, e somente se, a_0 é divisível por 2. ■

Exemplos: O número $n = 6749029876539871375986$ é divisível por 2?

Usando o critério temos que n termina em 6, logo é divisível por 2. Já o número 7629817 não é divisível por 2, pois termina em 7.

2.3 Critério de divisibilidade por 3 e 9

Seja $n = a_r a_{r-1} \cdots a_2 a_1 a_0$ um número natural escrito na base 10, então n será divisível por 3, respectivamente por 9 se, e somente se, $a_r + \cdots + a_2 + a_1 + a_0$ seja divisível por 3, respectivamente por 9.

Demonstração: Temos que, $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ subtraindo $a_r + \cdots + a_2 + a_1 + a_0$ dos dois lados da igualdade ficamos, $n - (a_r + \cdots + a_2 + a_1 + a_0) = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 - (a_r + \cdots + a_2 + a_1 + a_0) = a_r \cdot (10^r - 1) + \cdots + a_1 \cdot (10 - 1)$. Sabemos do teorema (5) que $9 \mid 10^r - 1$, ou seja:

$$n = (a_r + \cdots + a_1 + a_0) + 9k.$$

Onde $9k = a_r \cdot (10^r - 1) + \cdots + a_1 \cdot (10 - 1)$, daí n é divisível por 3, respectivamente por 9 se, e somente se, $a_r + \cdots + a_2 + a_1 + a_0$ for divisível por 3, respectivamente por 9.

Apresentaremos outra justificativa por meio da linguagem de congruência, primeiro analisaremos os restos das potências de 10 por 3 e 9, isto é: $10^0 \equiv 1 \ mod\ 3$ ou $mod\ 9$, $10^1 \equiv 1 \ mod\ 3$ ou $mod\ 9$, $10^2 \equiv 1 \ mod\ 3$ ou $mod\ 9$, ou seja, para todo $i \in \mathbb{N}$, segue que $10^i \equiv 1 \ mod\ 3$ ou $mod\ 9$. Assim, temos: $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv a_r + \cdots + a_2 + a_1 + a_0 \ mod\ 3$ ou $mod\ 9$, ou seja 3 ou $9 \mid n$ se, e somente se $a_r + \cdots + a_1 + a_0 \equiv 0 \ mod\ 3$ ou $mod\ 9$. ■

Exemplos: Verifique se $n = 754371$ é divisível por 3 e 9.

Aplicando o critério temos, $7 + 5 + 4 + 3 + 7 + 1 = 27$, assim como $3 \mid 27$ e $9 \mid 27$, concluímos que de fato, 754371 é divisível por 3 e por 9. Já o número 7865 não é divisível por 3 nem por 9, pois $7 + 8 + 6 + 5 = 26$.

2.4 Critério de divisibilidade por 4

Um número natural $n = a_r a_{r-1} \cdots a_2 a_1 a_0$, com mais de dois dígitos é divisível por 4 se, e somente se, o número formado por seus dois últimos algarismos for divisível por 4 ou 00.

Demonstração:

Seja $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$, logo podemos reescrever n da seguinte forma: $n = 100 \cdot k + (a_1 \cdot 10 + a_0)$, com $k \in \mathbb{N}$. Assim como 100 é divisível por 4, então n será divisível por 4 se, e somente se $a_1 \cdot 10 + a_0$ for divisível por 4, ou seja $4 \mid n$ se, e somente se $a_1 a_0$ também for divisível por 4.

Apresentaremos outra demonstração desse critério usando congruência, notemos que $a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 = (a_r \cdot 10^{r-2} + \cdots + a_2)100$, como $100 \equiv 0 \ mod\ 4$ e $10 \equiv 2 \ mod\ 4$, temos pelo teorema (13), item (**v**) que $(a_r \cdot 10^{r-2} + \cdots + a_2)100 + a_1 10 + a_0 \equiv 2a_1 + a_0 \ mod\ 4$, sendo assim concluímos que um número é divisível por 4 se o dobro do algarismo da dezena somado com o algarismo da unidade também for. ■

Exemplo: Verifique se o número $n = 472856$ é divisível por 4.

De fato, pelo critério temos que n tem o 56 como os dois últimos algarismos e como 56 é divisível por 4, concluímos então que 472856 também é divisível por 4.

2.5 Critério de divisibilidade por 5 e 10

Seja $n = a - ra_{r-1}\cdots a_2a_1a_0$, um número natural na base 10, uma condição necessária e suficiente para que n seja divisível por 5 é que a_0 seja 0 ou 5 e para se divisível por 10 é que a_0 seja 0.

Demonstração: Como $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$, então pondo o 10 em evidência obtemos: $n = 10 \cdot (a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10^1 + a_1) + a_0$, como 10 é divisível por 5, temos que n é divisível por 5 se, e somente se, a_0 é divisível por por 5, isto é $a_0 = 0$ ou $a_0 = 5$, por outro lado n é divisível por 10 se, e somente se, a_0 é divisível por 10, ou seja $a_0 = 0$.

Por congruência sabemos que $10 \equiv 0$ *mod* 5 ou *mod* 10, portanto temos que $a_i \cdot 10^i \equiv 0$ *mod* 5 ou *mod* 10, para todo $i \in \mathbb{N}$, logo seja $n = a_r \cdots a_1 \cdot a_0$, na base 10, temos pelo teorema (13), item (**v**) que $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv a_0$ *mod* 5 ou *mod* 10. O que nos diz que n é divisível por 5 ou 10 se, e somente se, a_0 é divisível por 5 ou 10. ■

Exemplos: Verifique se o número $n = 76890$ é divisível por 5 e por 10.

De acordo com o critério o número 76890 é divisível por 5 e por 10, pois n termina em 0. Já o número 34895 só é divisível por 5, pois seu último algarismo é divisível por 5, mas não por 10.

2.6 Critério de divisibilidade por 6

Um número natural $n = a_ra_{r-1}\cdots a_2a_1a_0$ é divisível por 6 se, e somente se, n for divisível simultaneamente por 2 e 3. Uma justificativa desse critério vem do Teorema Fundamental da Aritmética - TFA, de fato notemos, que a decomposição em fatores primos do 6 é $6 = 2 \cdot 3$.

Demonstração: Seja n um número natural, tomando $n = 6{\cdot}t = 2{\cdot}(3{\cdot}t)$, se fizermos $x = 3{\cdot}t$, então $n = 2 \cdot x$, com $x \in \mathbb{N}$, daí n é divisível por 2. Analogamente $n = 6 \cdot t = 3 \cdot (2 \cdot t)$, se fizermos $z = 2 \cdot t$, então $n = 3 \cdot z$, com $z \in \mathbb{N}$, assim $3 \mid n$, logo se n é divisível por 6, então n é divisível por 2 e 3.

Por outro lado, suponhamos, que n seja divisível por 2 e 3, como $2 \mid n$, então $\exists\ k \in \mathbb{N}$ tal que $n = 2 \cdot k$, notemos que 3 - 2 = 1, multiplicando essa igualdade por k, obtemos $3 \cdot k - 2 \cdot k = k \Rightarrow 3 \cdot k - n = k$ (i), por outro lado, existe também $t \in \mathbb{N}$ tal que $n = 3 \cdot t$, pois $3 \mid n$ (ii), logo, por (i) e (ii) temos que $k = 3 \cdot k - n = 3 \cdot k - 3 \cdot t = 3 \cdot (k - t)$,

finalmente, fazendo $y = k - t$, e como $k - t \geq 0$, então $k = 3 \cdot y$, com $y \in \mathbb{N}$. Logo, $n = 2 \cdot k = 2 \cdot 3 \cdot y = 6 \cdot y$, com $y \in \mathbb{N}$ e isso garante que n é divisível por 6. Concluímos, portanto, que se n for divisível por 3 e 2, então n será divisível por 6. ■

Exemplo: Verifique se o número $n = 489324$ é divisível por 6.

De acordo com o critério temos: $4 + 8 + 9 + 3 + 2 + 4 = 30$, o que implica que $3 \mid 30$ ou seja, o número n é divisível por 3, por outro lado o número n tem o 4 como algarismo da unidade, logo $2 \mid n$. Portanto, como n é divisível por 2 e 3, então n é divisível também por 6.

2.6.1 Outro Critério de Divisibilidade por 6

Um número natural $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, na base 10 é divisível por 6 se, e somente se, a soma do algarismo da unidade com o quádruplo de cada um dos outros algarismos é divisível por 6.

Demonstração: Seja $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, note que:

$$10^1 \equiv 4 \ mod \ 6$$

$$10^2 \equiv 4^2 \ mod \ 6 \equiv 4 \ mod \ 6$$

$$\vdots \qquad \vdots$$

$$10^r \equiv 4^r \ mod \ 6 \equiv 4 \ mod \ 6,$$

Daí temos pelo teorema (13) item (**v**) que:

$n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv 4 \cdot (a_r + \cdots + a_2 + a_1) + a_0 \ mod \ 6$, portanto $6 \mid n$ se, e somente se, $4 \cdot (a_r + \cdots + a_1) + a_0 \equiv 0 \ mod \ 6$. ■

Exemplo: Verifique se o número $n = 489324$ é divisível por 6.

Pelo segundo critério temos: $4 \cdot (4 + 8 + 9 + 3 + 2) + 4 = 16 + 32 + 36 + 12 + 8 + 4 = 108$, repetindo o critério, obtemos $4 \cdot (1 + 0) + 8 = 12$, daí concluímos que 12 é divisível por 6, portanto o número n também é divisível por 6.

2.7 Critério de Divisibilidade por 7

Sejam S_{ci} e S_{cp} a soma dos números das classes ímpares e pares respectivamente. Um número natural $n = a_r \cdots a_2 a_1 a_0$, escrito na base 10 é divisível por 7 se, e somente se:

$S_{ci} - S_{cp} \equiv 0$ mod 7, ou seja, quando a diferença não negativa entre a soma dos números das classes ímpares e a soma dos números das classes pares é divisível por 7.

Demonstração: Analisando os restos da divisão de das potências de 10 por 7, temos:

$$\begin{aligned}
10^0 &\equiv 1 \ mod\ 7 \\
10^1 &\equiv 3 \ mod\ 7 \ \text{ ou } \ 10^1 \equiv -4 \ mod\ 7 \\
10^2 &\equiv 2 \ mod\ 7 \ \text{ ou } \ 10^2 \equiv -5 \ mod\ 7 \\
10^3 &\equiv 6 \ mod\ 7 \ \text{ ou } \ 10^3 \equiv -1 \ mod\ 7 \\
10^4 &\equiv 4 \ mod\ 7 \ \text{ ou } \ 10^4 \equiv -3 \ mod\ 7 \\
10^5 &\equiv 5 \ mod\ 7 \ \text{ ou } \ 10^5 \equiv -2 \ mod\ 7 \\
10^6 &\equiv 1 \ mod\ 7 \ \text{ ou } \ 10^6 \equiv -6 \ mod\ 7 \\
\vdots &\equiv \vdots
\end{aligned}$$

Assim por diante, até 10^r. Seja $k \in \mathbb{N}$, note que se k for par, então $10^k \equiv$ 1 ou 2 ou $-$ 3 *mod* 7, caso k seja ímpar $10^k \equiv -1$ ou -2 ou 3 *mod* 7, logo:
$n = a_r \cdot 10^r + \cdots + a_8 \cdot 10^8 + a_7 \cdot 10^7 + a_6 \cdot 10^6 + a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv (a_0 + 3 \cdot a_1 + 2 \cdot a_2) - (a_3 + 3 \cdot a_4 + 2 \cdot a_5) + (a_6 + 3 \cdot a_7 + 2 \cdot a_8) - (a_9 + 3 \cdot a_{10} + 2 \cdot a_{11}) + \cdots + (a_{r-5} + 3 \cdot a_{r-4} + 2 \cdot a_{r-3}) - (a_{r-2} + 3 \cdot a_{r-1} + 2 \cdot a_r) \equiv (a_2 a_1 a_0 + a_8 a_7 a_6 + a_{r-5} a_{r-4} a_{r-3}) - (a_5 a_4 a_3 + a_{11} a_{10} a_9 + \cdots + a_{r-2} a_{r-1} a_r)$ *mod* 7, então n será divisível por 7 se, e somente se, $(S_{cí} - S_{cp})$ for divisível por 7. ■

Exemplo: Verifique se o número $n = 22389651536$ é divisível por 7.

Aplicando o critério, ficamos: $536 - 651 + 389 - 22 = -115 + 367 = 252$, como 252 é divisível por 7, concluímos que n é divisível por 7. Notemos que esse critério é mais utilizado quando o número tem muitos algarismos na sua composição.

2.8 Critério de divisibilidade por 8

Um número $n = a_r \cdots a_2 a_1 a_0$, com mais de três algarismos, é divisível por 8 se, e somente se, o número formado por seus três últimos algarismos for divisível por 8.

Demonstração: Seja $n = a_r \cdot 10^r + \cdots a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, desta forma colocamos 1000 em evidência ficamos com, $n = 1000 \cdot (a_r \cdot 10^{r-3} + \cdots + a_3) + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 = 1000 \cdot k + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, onde $k = (a_r \cdot 10^{r-3} + \cdots + a_3)$ e $k \in \mathbb{N}$ já que $1000 = 10^3 < 10^4 < \cdots < 10^r$. Daí como $8 \mid 1000$, segue que n será divisível por por 8 se, e somente se $a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ for divisível por 8, ou seja, se os últimos três algarismos for divisível por 8. ■

Outra demonstração pode ser feita por congruência, basta analisarmos os restos da divisão das potências de 10 por 8, isto é:

$$\begin{aligned} 10^0 &\equiv 1 \ mod \ 8 \\ 10^1 &\equiv 2 \ mod \ 8 \\ 10^2 &\equiv 4 \ mod \ 8 \\ 10^3 &\equiv 0 \ mod \ 8 \\ 10^4 &\equiv 0 \ mod \ 8 \\ &\vdots \quad \vdots \\ 10^r &\equiv 0 \ mod \ 8 \end{aligned}$$

.

Então $n = a_r \cdot 10^r + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv 0 + \cdots + 0 + a_2a_1a_0 \ mod \ 8$, portanto $8 \mid n$ se, e somente se, $a_2a_1a_0 \equiv 0 \ mod \ 8$, podemos também pensar da seguinte forma, notemos que $a_r \cdot 10^r + \cdots + a_3 \cdot 10^3 = (a_r \cdot 10^{r-3} + \cdots + a_3)1000$, como $1000 \equiv 0 \ mod \ 8$, $100 \equiv 4 \ mod \ 8$ e $10 \equiv 2 \ mod \ 8$, temos $(a_r \cdot 10^{r-3} + \cdots + a_3)1000 + a_2100 + a_110 + a_0 \equiv 4a_3 + 2a_2 + a_0 \ mod \ 4$, sendo assim concluímos que um número é divisível por 8 se o quadrúplo do algarismo da centena somado com o dobro do algarismo da dezena somado com o algarismo da unidade também o for. ■

Exemplo: Verifique se o número $n = 589120$ é divisível por 8.

De fato pelo critério, temos que os três últimos algarismos é 120 e como ele é divisível por 8, então n também é divisível por 8.

Na próxima seção faremos uma generalização dos critérios de divisibilidade por qualquer potência de 2.

2.9 Critério de divisibilidade por potências de 2

Começaremos esta seção relembrando que, um número é divisível por 2 quando o último algarismo é divisível por 2. O número é divisível por 4, ou 2^2, quando o número formado pelos dois últimos algarismos é divisível por 4. O número é divisível por 8, ou 2^3, quando o número formado pelos três últimos algarismos é divisível por 8, respectivamente. Diante desses casos, podemos generalizar esse critério para qualquer potência de 2, ou seja:

Um número é divisível por 2^n quando o número formado pelos últimos n algarismos é divisível por 2^n.

Demonstração: Sabemos que $10 = 2 \cdot 5$, daí temos que $10^n = 2^n \cdot 5^n$. Dado um número natural N, seja b o número formado pelos seus últimos n algarismos. Então $N = 10^n + b$. Como 10^n é divisível por 2^n. Se b for divisível por 2^n então N também é divisível por 2^n. ■

Por outro lado, se o resto da divisão de b por 2^n for m, então é possível escrever $b = 2^n\, q + m$, com $q \in \mathbb{N}$, logo $N = 10^n a + b = 10^n a + (2^n q + m)$, ou seja, $N = 2^n(5^n a + q) + m$ o que significa que o resto da divisão de N por 2^n é m. Em outras palavras, os critérios exibidos acima não só apontam quando um número é divisível por uma potência de 2, como também determinam o resto da divisão por essa potência de 2.

Por exemplo, o número 349854 não é divisível por 4 pois 54 não é divisível por 4. Além disso, como 54 deixa resto 2 quando dividido por 4, o número 349854 também deixa resto 2 quando dividido por 4. Da mesma forma, 349854 deixa resto 6 quando dividido por 8, pois esse é o resto que 854 deixa quando dividido por 8.

2.10 Critério de divisibilidade por 11

Um número natural $n = a_r a_{r-1} \cdots a_2 a_1 a_0$ é divisível por 11 se, e somente se, a soma alternada dos algarismos de ordem par e dos algarismos de ordem ímpar for divisível por 11.

Demonstração: Como $10 \equiv -1\ mod\ 11$, pelo teorema (13), temos que $10^{2i} \equiv 1\ mod\ 11$ e $10^{2i+1} \equiv -1\ mod\ 11$, daí seja $n = a_r \cdots a_4 a_3 a_2 a_1 a_0$ um número na base 10, segue que:

$$\begin{aligned} a_0 &\equiv a_0\ mod\ 11 \\ a_1 \cdot 10^1 &\equiv -a_1\ mod\ 11 \\ a_2 \cdot 10^2 &\equiv a_2\ mod\ 11 \\ a_3 \cdot 10^3 &\equiv -a_3\ mod\ 11 \\ \vdots &\quad \vdots \\ a_r \cdot 10^r &\equiv (-1)^r a_r\ mod\ 11 \end{aligned}$$

Do teorema (13) item (**iv**) encontramos:

$$\begin{aligned} n = a_r \cdot 10^r + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 &\equiv \\ (-1)^r a_r + \cdots - a_3 + a_2 - a_1 + a_0\ mod\ 11 &\equiv \sum_{k=0}^{r} (-1)^k a_k\ mod\ 11, \end{aligned}$$

ou seja $11 \mid n$, se, e somente se, a soma alternada dos algarismos de ordem par e dos algarismos de ordem ímpar for divisível por 11.

Exemplo: Verifique se o número $n = 187896346$ é divisível por 11.

De acordo com o critério, primeiro somaremos os algarismos de ordem par em seguida os de ordem ímpar e por fim faremos a diferença entre essas duas somas. Aplicando esse critério temos: $6 + 3 + 9 + 7 + 1 = 26$ e $4 + 6 + 8 + 8 = 26$, daí 26 - 26 = 0, como zero é divisível por qualquer número, concluímos portanto que n é divisível por 11.

No último capítulo faremos a construção, a demonstração e exemplificação dos critérios de divisibilidade mais sofisticados, as demonstrações usarão essencialmente a linguagem das congruências.

3 Construção dos Critérios de Divisibilidade Incomuns e Curiosos

Em decorrência dos assuntos estudados anteriormente seremos capazes de apresentar nesse capítulo um resultado interessante e inédito a respeito dos critérios de divisibilidade para todos os números primos. É importante relembrar que um dos nossos objetivos é despertar o interesse e a curiosidade dos alunos dos cursos de matemática e áreas afins para aritmética, tendo como fio condutor os critérios de divisibilidade, embora os que são tratado aqui não tenha necessariamente utilidade do ponto de vista prático. Ressaltamos que o ineditismo aqui mencionado se refere ao fato de que todos os resultados foram elaborado por conta própria.

3.1 Uma quebra nas unidades

Seja $n = a_r a_{r-1} \cdots a_1 a_0$ um número natural. Nesta seção apresentamos alguns critérios de divisibilidade que consistem em "quebrar" o número n no algarismo das unidades, obtendo, a partir deste, o número $m = a_r a_{r-1} \cdots a_1 + xa_0$ para algum inteiro x a ser determinado. A ideia é mostrar que um determinado primo p divide n se, e somente se, p divide m.

3.1.1 Critério de divisibilidade por 11

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 11 *se, e somente se,* $m = a_r a_{r-1} \cdots a_1 + xa_0$ *é divisível por* 11.

Demonstração: Suponhamos que $11 \mid m$, ou seja:

$$m = a_r a_{r-1} \cdots a_1 + xa_0 \equiv 0 \ mod\ 11 \tag{3.1}$$

Multiplicando (3.1) por 10, tem - se:

$$10m = a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 \ + \ a_1 \cdot 10 \ + \ 10xa_0 \equiv 0 \ mod\ 11.$$

Notemos que $a_r \cdot 10^r \ + \cdots + a_2 \ + \ a_1 \cdot 10 = n - a_0$, logo:

$$\begin{aligned} n - a_0 + 10xa_0 &\equiv 0 \ mod\ 11 \\ n + (10x - 1)a_0 &\equiv 0 \ mod\ 11 \end{aligned}$$

Assim para que 11 divida n, deveremos encontrar a solução da congruência linear $10x \equiv 1 \ mod \ 11$, calculando o inverso multiplicativo de 10 módulo 11, encontramos $x = -1$. Portanto $m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 - a_0$.

De fato, multiplicando m por 10, ficamos com $a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 10 \cdot a_0 \equiv 0 \ mod \ 11$, daí temos: $n - a_0 - 10 \cdot a_0 \equiv 0 \ mod \ 11 \implies n - 11 \cdot a_0 \equiv 0 \ mod \ 11$, como $11 \mid 11$ concluímos que $n \equiv 0 \ mod \ 11$.

Reciprocamente, se $n \equiv 0 \ mod \ 11$ e $m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 + xa_0$, segue que:

$$10m = n - a_0 + 10xa_0 = n + (10x - 1)a_0 = n - 11$$

Assim, como $11 \mid -11$, concluímos que $m \equiv 0 \ mod \ 11$, sendo assim o critério é de fato verdadeiro para $x = -1$. ■

Exemplo: Verifique se o número $n = 22737$ é divisível por 11.

Aplicando o critério temos, 2273 - 7= 2266, repetindo o processo temos: $226 - 6 = 220 \Rightarrow 22 - 0 = 22$ e como $11 \mid 22$ segue $11 \mid n$.

3.1.2 Critério de divisibilidade por 13

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 13 *se, e somente se,* $m = a_r a_{r-1} \cdots a_1 + xa_0$ *é divisível por* 13.

Demonstração: Suponhamos que $13 \mid m$, ou seja:

$$m = a_r a_{r-1} \cdots a_1 + xa_0 \equiv 0 \ mod \ 13 \tag{3.2}$$

Multiplicando (3.2) por 10, tem - se:

$$10m = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 10xa_0 \equiv 0 \ mod \ 13.$$

Notemos que $a_r \cdot 10^r + \cdots + a_2 + a_1 \cdot 10 = n - a_0$, logo:

$$\begin{aligned} n - a_0 + 10xa_0 &\equiv 0 \ mod \ 13 \\ n + (10x - 1)a_0 &\equiv 0 \ mod \ 13 \end{aligned}$$

Assim para que 13 divida n, deveremos encontrar a solução da congruência linear $10x \equiv 1 \ mod \ 13$, usando a tabela da multiplicação das classe de equivalência módulo 13, encontramos $x = 4$. Portanto $m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 + 4a_0$.

De fato, multiplicando m por 10, ficamos com $a_r \cdot 10^r \ + \cdots + \ 10 \cdot 4 \cdot a_0 \equiv 0 \ mod \ 13$, daí temos: $n - \ a_0 \ + 40a_0 \equiv 0 \ mod \ 13 \implies n + \ 39 \cdot a_0 \ \equiv \ 0 \ mod \ 13$, como $13 \mid 39$ concluímos que $n \ \equiv \ 0 \ mod \ 13$.

Reciprocamente, se $n \equiv 0 \ mod \ 13$ e $m = a_r \cdot 10^{r-1} \ + \cdots + \ a_2 \cdot 10 \ + \ a_1 \ + xa_0$, segue que:

$$10m = n - a_0 + 10xa_0 = n + (10x - 1)a_0 = n + 39$$

Assim, como $13 \mid 39$, concluímos que $m \equiv \ 0 \ mod \ 13$, sendo assim o critério é de fato verdadeiro para $x = 4$. ■

Exemplo: Verifique se o número $n = 15678$ é divisível por 13.

Aplicando o critério sucessivas vezes, temos:

$$15678 \longrightarrow 1567 + 4 \cdot 8 = 1599 \longrightarrow 159 + 4 \cdot 9 = 195 \longrightarrow 19 + 4 \cdot 5 = 39$$

portanto como $13 \mid 39$, então 15678 é divisível por 13 também.

3.1.3 Critério de divisibilidade por 17

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 17 *se, e somente se,* $m = a_r a_{r-1} \cdots a_1 + xa_0$ *é divisível por* 17.

Demonstração: Suponhamos que $17 \mid m$, ou seja:

$$m = a_r a_{r-1} \cdots a_1 + xa_0 \equiv 0 \ mod \ 17 \tag{3.3}$$

Multiplicando (3.3) por 10, tem - se:

$$10m = a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 \ + \ a_1 \cdot 10 \ + \ 10xa_0 \equiv 0 \ mod \ 17.$$

Notemos que $a_r \cdot 10^r \ + \cdots + a_2 \ + \ a_1 \cdot 10 = n - a_0$, logo:

$$\begin{aligned} n - a_0 + 10xa_0 \ &\equiv \ 0 \ mod \ 17 \\ n + (10x - 1)a_0 \ &\equiv \ 0 \ mod \ 17 \end{aligned}$$

Assim para que 17 divida n, deveremos encontrar a solução da congruência linear $10x \equiv 1 \ mod \ 17$, usando a tabela da multiplicação das classe de equivalência módulo 17, encontramos $x = -5$. Portanto $m = a_r \cdot 10^{r-1} \ + \cdots + \ a_2 \cdot 10 \ + \ a_1 \ - 5a_0$.

De fato, multiplicando m por 10, ficamos com $a_r \cdot 10^r \ + \cdots - \ 10 \cdot 5a_0 \equiv 0 \ mod \ 17$, daí temos: $n - \ a_0 \ - 50a_0 \equiv 0 \ mod \ 17 \implies n - \ 51 \cdot a_0 \ \equiv \ 0 \ mod \ 17$, como $17 \mid -51$ concluímos que $n \ \equiv \ 0 \ mod \ 17$.

Reciprocamente, se $n \equiv 0\ mod\ 17$ e $m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 + xa_0$, segue que:

$$10m = n - a_0 + 10xa_0 = n + (10x - 1)a_0 = n - 51a_0$$

Assim, como $17 \mid -51$, concluímos que $m \equiv 0\ mod\ 17$, sendo assim o critério é de fato verdadeiro para $x = -5$. ■

Exemplo: Verifique se o número $n = 456722$ é divisível por 17.

Aplicando o critério sucessivas vezes, temos:

$456722 \longrightarrow 45672 - 5 \cdot 2 = 45662 \longrightarrow 4566 - 5 \cdot 2 = 4556 \longrightarrow 455 - 5 \cdot 6 = 425 \longrightarrow 42 - 5 \cdot 5 = 17$

Como 17 é divisível por 17, segue que 456722 também é divisível por 17.

Por outro lado, é importante ressaltar que o resto que m e n deixam na divisão por p não são iguais, entretanto existe uma correlação entre os mesmos, para esclarecer essa última afirmação, apresentaremos a correlação entre os restos que m e n deixam na divisão por 11, quando o $11 \nmid m$, considerando que $x = -1$ e supondo que:

$$m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 - a_0 \equiv k\ mod\ 11,$$

com $k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, fazendo a multiplicação dessa congruência por 10, encontramos:

$$a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 10 \cdot a_0 \equiv 10k\ mod\ 11$$

Como $a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 = n - a_0$, ficamos com:

$$\begin{aligned} n - a_0 - 10a_0 &\equiv 10k\ mod\ 11 \Longrightarrow \\ n - 11a_0 &\equiv 10k\ mod\ 11 \quad como \quad 11 \mid 11 \Longrightarrow \\ n &\equiv 10k\ mod\ 11 \end{aligned}$$

Sendo assim, temos que quando $k = 0$, obtemos $m \equiv 0\ mod\ 11 \Longrightarrow n \equiv 0\ mod\ 11$, porém se $k \neq 0$ temos que $m \equiv k\ mod\ 11 \Longrightarrow n \equiv 10k\ mod\ 11$, ou seja, a segunda congruência é múltipla da primeira.

Em outras palavras se $m \equiv 5\ mod\ 11 \Longrightarrow n \equiv 50\ mod\ 11$, se $m \equiv 7\ mod 11 \Longrightarrow n \equiv 70\ mod\ 11$ e assim sucessivamente. Logo se m deixa resto 5 na divisão por 11, então n deixa resto 6 na divisão por 11, visto que $50 \equiv 6 mod\ 11$. Portanto concluímos que os restos não são necessariamente preservados. Podemos observar de forma resumida tudo que foi dito antes na seguinte tabela:

k	Resto de m na divisão por 11	Resto de n na divisão por 11
0	0	0
1	1	10
2	2	9
3	3	8
4	4	7
5	5	6
6	6	5
7	7	4
8	8	3
9	9	2
10	10	1

Para finalizar, vale a pena notar que a partir dessa discussão surge uma curiosidade interessante que é o fato de não ser mais necessário dividirmos o n por 11 para sabermos quem é seu resto basta para isso dividir o $10k$ por 11. Para facilitar a compreensão tomaremos o exemplo seguinte, seja $n = 3899$ e $m = 389 - 9 = 380$, daí temos $m \equiv k = 6 \ mod \ 11$ então $n \equiv 10 \cdot 6 = 60 \equiv 5 \ mod \ 11$. Essa correlação também se aplica para os primos 13 e 17, isto é, se m deixa resto k na divisão por 13 e 17, então n deixa resto $10k$ na divisão por 13 e 17.

Diante dos critérios de divisibilidade vistos até aqui, apresentaremos a seguir uma generalização desses critérios para qualquer número primo $p \geq 11$.

Teorema 16 *Um natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por um primo positivo $p \geq 11$ se e somente se $m = a_r a_{r-1} \cdots a_1 - x a_0$ é divisível por p, onde x é uma solução inteira da congruência linear $10x \equiv 1 \ mod \ p$.*

Demonstração: Suponhamos que p divide $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$. Como $m = a_r \cdot 10^{r-1} + \cdots + a_2 \cdot 10 + a_1 + x a_0$, segue que

$$10m = n - a_0 + 10x a_0 = n + (10x - 1)a_0. \tag{3.4}$$

Assim, para que p divida m basta que p divida $10x - 1$, visto que $p \mid n$. Isto mostra que basta determinar um inteiro x tal que $10x - 1 \equiv 0 \ mod \ p$, isto é, x é uma solução da congruência linear

$$10x \equiv 1 \ mod \ p.$$

Reciprocamente, se x é uma solução da congruência acima e $p \mid m$ segue de (3.4) que $p \mid n$. ■

3.2 Duas quebras, nas unidades e nas dezenas

Seja $n = a_r a_{r-1} \cdots a_1 a_0$ um número natural. Nesta seção apresentamos alguns critérios de divisibilidade que consistem em "quebrar" o número n no algarismo das unidades e das dezenas, obtendo, a partir deste, o número $m = a_r a_{r-1} \cdots a_2 + ya_1 + xa_0$ para algum inteiro x e y a serem determinados. O objetivo aqui é o mesmo da seção anterior, mostrar que um determinado primo p divide n se, e somente se, p divide m.

3.2.1 Critério de divisibilidade por 13

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 13 *se, e somente se,* $m = a_r a_{r-1} \cdots a_2 + ya_1 + xa_0$ *é divisível por* 13.

Demonstração: Inicialmente suponhamos que $13 \mid m$, ou seja: $m = a_r \cdot 10^{r-2} + \cdots + a_2 + ya_1 + xa_0 \equiv 0 \ mod\ 13$. Multiplicando a congruência por 10^2, obtemos:

$$a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 \ + \ 100ya_1 \ + \ 100xa_0 \equiv 0 \ mod\ 13.$$

Sabendo que $a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 = n - 10a_1 - a_0$, substituindo na última congruência obtemos:

$$\begin{aligned} n - 10a_1 - a_0 + 100ya_1 + 100xa_0 &\equiv 0 \ mod\ 13 \\ n + (100y - 10)a_1 + (100x - 1)a_0 &\equiv 0 \ mod\ 13 \end{aligned} \tag{3.5}$$

Portanto para que $13 \mid n$, nosso problema consiste em resolver o seguinte sistema de congruência independente:

$$\begin{cases} 100y - 10 \equiv 0 \ mod\ 13 \\ 100x - 1 \equiv 0 \ mod\ 13 \end{cases}$$

Como $100 \equiv 9 \ mod\ 13$, obtemos o sistema equivalente:

$$\begin{cases} 9y \equiv 10 \ mod\ 13 \\ 9x \equiv 1 \ mod\ 13 \end{cases}$$

Daí usando a tabela da multiplicação das classes de equivalência módulo 13, encontramos: $y = 4$ e $x = 3$. Portanto, $m = a_r \cdot 10^{r-2} + \cdots + a_2 + 4a_1 + 3a_0$, sendo assim, substituindo $y = 4$ e $x = 3$ em (3.5), obtemos:

$$\begin{aligned} n - 10a_1 - a_0 + 100 \cdot 4a_1 + 100 \cdot 3a_0 &\equiv 0 \ mod\ 13 \Longrightarrow \\ n - 10a_1 - a_0 + 400 \cdot a_1 + 300 \cdot a_0 &\equiv 0 \ mod\ 13 \Longrightarrow \\ n + 390 \cdot a_1 + 299 \cdot a_0 &\equiv 0 \ mod\ 13 \end{aligned}$$

Como $390 \equiv 0 \ mod\ 13$ e $299 \equiv 0 \ mod\ 13$, concluímos que $n \equiv 0 \ mod\ 13$.

Reciprocamente, se $n \equiv 0\ mod\ 13$ e $m = a_r \cdot 10^{r-2} + \cdots + a_2 + xa_1 + ya_0 \equiv 0\ mod\ 13$, segue que:

$100m = n - 10a_1 - a_0 + 100ya_1 + 100xa_0 = n + (100y - 10)a_1 + (100x - 1)a_0 = n + 390a_1 + 299a_0$.

Daí, segue que $m \equiv 0\ mod\ 13$, assim concluímos que o critério é de fato verdadeiro para $x = 3$ e $y = 4$. ■

Exemplo: Verifique se o número $n = 13728$ é divisível por 13.

Aplicando o critério sucessivas vezes, temos:

$$13728 \Longrightarrow 137 + 4 \cdot 2 + 3 \cdot 8 = 169 \Longrightarrow 1 + 4 \cdot 6 + 3 \cdot 9 = 52$$

Como 52 é divisível por 13, segue que 13728 também é divisível por 13.

3.2.2 Critério de divisibilidade por 17

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 17 *se, e somente se,* $m = a_r a_{r-1} \cdots a_2 + ya_1 + xa_0$ *é divisível por* 17.

Demonstração: Inicialmente suponhamos que $17 \mid m$, ou seja: $m = a_r \cdot 10^{r-2} + \cdots + a_2 + ya_1 + xa_0 \equiv 0\ mod\ 17$. Multiplicando a congruência por 10^2, obtemos:

$$a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 \ + \ 100ya_1 \ + \ 100xa_0 \equiv 0\ mod\ 17.$$

Note que $a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 = n - 10a_1 - a_0$, substituindo na última congruência obtemos:

$$n - 10a_1 - a_0 + 100ya_1 + 100xa_0 \equiv 0\ mod\ 17 \tag{3.6}$$
$$n + (100y - 10)a_1 + (100x - 1)a_0 \equiv 0\ mod\ 17$$

Daí, para que $17 \mid n$, nosso problema consiste em resolver o seguinte sistema de congruência independente:

$$\begin{cases} 100y - 10 \equiv 0\ mod\ 17 \\ 100x - 1 \equiv 0\ mod\ 17 \end{cases}$$

Como $100 \equiv 15\ mod\ 17$, obtemos o sistema equivalente:

$$\begin{cases} 15y \equiv 10\ mod\ 17 \\ 15x \equiv 1\ mod\ 17 \end{cases}$$

Daí usando a tabela da multiplicação das classes de equivalência módulo 17, encontramos: $y = 12$ ou $y = -5$ e $x = 8$. Portanto, $m = a_r \cdot 10^{r-2} + \cdots + a_2 - 5a_1 + 8a_0$, sendo assim,

substituindo $y = -5$ e $x = 8$ em (3.6), obtemos:

$$\begin{aligned} n - 10a_1 - a_0 + 100 \cdot (-5)a_1 + 100 \cdot 8a_0 &\equiv 0 \ mod\ 17 \Longrightarrow \\ n - 10a_1 - a_0 - 500 \cdot a_1 + 800 \cdot a_0 &\equiv 0 \ mod\ 17 \Longrightarrow \\ n - 510 \cdot a_1 + 799 \cdot a_0 &\equiv 0 \ mod\ 17 \end{aligned}$$

Como $-510 \equiv 0\ mod\ 17$ e $799 \equiv 0\ mod\ 17$, concluímos que $n \equiv 0\ mod\ 17$. Reciprocamente, se $n \equiv 0\ mod\ 17$ e $m = a_r \cdot 10^{r-2} + \cdots + a_2 + ya_1 + xa_0 \equiv 0\ mod\ 17$, segue que:

$$100m = n - 10a_1 - a_0 + 100ya_1 + 100xa_0 = n + (100y - 10)a_1 + (100x - 1)a_0 = n - 510a_1 + 799a_0.$$

Daí, segue que $m \equiv 0\ mod\ 17$, assim concluímos que o critério é de fato verdadeiro para $x = 8$ e $y = -5$. ■

Exemplo: Verifique se o número $n = 65790$ é divisível por 17. Aplicando o critério sucessivas vezes, temos:

$$65790 \Longrightarrow 657 - 5 \cdot 9 + 8 \cdot 0 = 612 \Longrightarrow 6 - 5 \cdot 1 + 8 \cdot 2 = 17$$

Como 17 é divisível por 17, segue que 65790 também é divisível por 17.

3.2.3 Critério de divisibilidade por 19

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 19 *se, e somente se,* $m = a_r a_{r-1} \cdots a_2 + ya_1 + xa_0$ *é divisível por* 19.

Demonstração: Suponhamos que $19 \mid m$, ou seja: $m = a_r \cdot 10^{r-2} + \cdots + a_2 + ya_1 + xa_0 \equiv 0\ mod\ 19$. Multiplicando a congruência por 10^2, obtemos:

$$a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 \ + \ 100ya_1 \ + \ 100xa_0 \equiv 0\ mod\ 19.$$

Note que $a_r \cdot 10^r + \cdots + \ a_2 \cdot 10^2 = n - 10a_1 - a_0$, substituindo na última congruência obtemos:

$$n - 10a_1 - a_0 + 100ya_1 + 100xa_0 \equiv 0\ mod\ 19 \tag{3.7}$$

$$n + (100y - 10)a_1 + (100x - 1)a_0 \equiv 0\ mod\ 19$$

Daí, para que $17 \mid n$, nosso problema consiste em resolver o seguinte sistema de congruência independente:

$$\begin{cases} 100y - 10 \equiv 0\ mod\ 19 \\ 100x - 1 \equiv 0\ mod\ 19 \end{cases}$$

Como $100 \equiv 5 \ mod \ 19$, obtemos o sistema equivalente:

$$\begin{cases} 5y \equiv 10 \ mod \ 19 \\ 5x \equiv 1 \ mod \ 19 \end{cases}$$

Transformando essas congruências num sistema de equações Diofantinos independente, temos:

$$\begin{cases} 5y - 19k = 10 \\ 5x - 19k' = 1 \end{cases} \quad \text{com } k, k' \in \mathbf{Z}$$

Usaremos o algoritmo de Euclides para resolver essas equações Diofantinas, conforme explorado no capítulo 1, resolvendo a primeira equação temos:

Quociente	3	1	1
19	5	4	4
Resto	4	1	0

Reescrevendo esses números de forma conveniente, obtemos as igualdades a seguir:

$$\begin{aligned} 4 &= 19 - 3 \cdot 5 \quad (1) \\ 1 &= 5 - 1 \cdot 4 \quad (2) \end{aligned}$$

Substituindo (1) em (2), ficamos com:

$$\begin{aligned} 1 &= 5 - 1 \cdot (19 - 3 \cdot 5) \\ 1 &= 5 - 1 \cdot 19 + 3 \cdot 5 \\ 1 &= 4 \cdot 5 - 1 \cdot 19. \end{aligned}$$

Multiplicando a última igualdade por 10 teremos: $40 \cdot 5 - 10 \cdot 19 = 10$, logo temos a solução particular $y = 40$ ou $y = 2$, pois $40 \equiv 2 \ mod \ 19$ e $k = 10$, de maneira análoga resolveremos a segunda equação, ou seja:

Quociente	3	1	1
19	5	4	4
Resto	4	1	0

reescrevendo obtemos as igualdades a seguir:

$$\begin{aligned} 4 &= 19 - 3 \cdot 5 \quad (3) \\ 1 &= 5 - 1 \cdot 4 \quad (4) \end{aligned}$$

Substituindo (3) em (4), ficamos com:

$$\begin{aligned} 1 &= 5 - 1 \cdot (19 - 3 \cdot 5) \\ 1 &= 5 - 1 \cdot 19 + 3 \cdot 5 \\ 1 &= 4 \cdot 5 - 1 \cdot 19. \end{aligned}$$

O que resulta na solução particular $x = 4$ e $k' = 1$. Daí, encontramos finalmente $x = 4$ e $y = 2$. Logo podemos reescrever m da seguinte forma: $m = a_r \cdot 10^{r-2} + \cdots + a_2 + 2a_1 + 4a_0$, sendo assim, substituindo $y = 2$ e $x = 4$ em (3.7), obtemos:

$$\begin{aligned} n - 10a_1 - a_0 + 100 \cdot 2a_1 + 100 \cdot 4a_0 &\equiv 0 \ mod\ 19 \Longrightarrow \\ n - 10a_1 - a_0 + 200 \cdot a_1 + 400 \cdot a_0 &\equiv 0 \ mod\ 19 \Longrightarrow \\ n + 190 \cdot a_1 + 399 \cdot a_0 &\equiv 0 \ mod\ 19 \end{aligned}$$

Como $190 \equiv 0\ mod\ 19$ e $399 \equiv 0\ mod\ 19$, concluímos que $n \equiv 0\ mod\ 19$. Reciprocamente, se $n \equiv 0\ mod\ 19$ e $m = a_r \cdot 10^{r-2} + \cdots + a_2 + ya_1 + xa_0 \equiv 0\ mod\ 19$, segue que:

$$100m = n - 10a_1 - a_0 + 100ya_1 + 100xa_0 = n + (100y - 10)a_1 + (100x - 1)a_0 = n + 190a_1 + 399a_0.$$

Daí, segue que $m \equiv 0\ mod\ 19$, assim concluímos que o critério é de fato verdadeiro para $x = 4$ e $y = 2$. ■

Exemplo: Verifique se o número $n = 14991$ é divisível por 19.

Aplicando o critério sucessivas vezes, temos:

$$14991 \Longrightarrow 149 + 2 \cdot 9 + 4 \cdot 1 = 149 + 18 + 4 = 171 \Longrightarrow 1 + 2 \cdot 7 + 4 \cdot 1 = 19.$$

Como 19 é divisível por 19, segue que 14991 também é divisível por 19.

Por outro lado, assim como na seção anterior aqui também existe uma correlação entre os restos que m e n deixam na divisão por um primo p, analisaremos a correlação entre os restos que m e n deixam na divisão por 13 quando $13 \nmid m$, considerando que $x = 4$ e $y = 3$, suponhamos que:

$$m = a_r \cdot 10^{r-2} + \cdots + a_2 + 4a_1 + 3a_0 \equiv k\ mod\ 13 \quad (1')$$

Onde: $k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ Fazendo a multiplicação dessa congruência por 100, obtemos: $a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + 400a_1 + 300a_0 \equiv 100k\ mod\ 13$. Sabendo que $a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 = n - 10a_1 - a_0$, substituindo na última congruência obtemos:

$$\begin{aligned} n - 10a_1 - a_0 + 400a_1 + 300a_0 &\equiv 100k\ mod\ 13 \Longrightarrow \\ n + 390a_1 + 299a_0 &\equiv 100k\ mod\ 13 \quad como \quad 13 \mid 390 \ \ e \ \ 13 \mid 299 \Longrightarrow \\ n &\equiv 100k\ mod 13 \quad (2'). \end{aligned}$$

Daí concluímos que (2') é múltipla de (1').

Em outras palavras se $m \equiv 4\ mod\ 13 \Longrightarrow n \equiv 400\ mod\ 13$, se $m \equiv 9\ mod\ 13 \Longrightarrow n \equiv 900\ mod\ 13$, portanto se m deixa resto 9 na divisão por 13, então n deixa resto 3 na

divisão por 13, pois $900 \equiv 3 \ mod\ 13$. Podemos observar isso resumidamente na seguinte tabela:

k	Resto de m na divisão por 13	Resto de n na divisão por 13
0	0	0
1	1	9
2	2	5
3	3	1
4	4	10
5	5	6
6	6	2
7	7	11
8	8	7
9	9	3
10	10	12
11	11	8
12	12	4

Faremos o seguinte exemplo: Sejam $n = 8973$ e $m = 89 + 4 \cdot 7 + 3 \cdot 3 = 126$, logo $m \equiv k = 9 \ mod\ 13$, então $n \equiv 100 \cdot 9 = 900 \equiv 3 \ mod\ 13$. Os primos 17 e 19 também possui essa correlação.

Encerraremos esta seção apresentando uma generalização desses critérios de divisibilidade.

Teorema 17 *Um natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por um primo positivo $p \geq 13$ se, e somente se $m = a_r a_{r-1} \cdots a_2 + y a_1 + x a_0$ é divisível por p, onde x e y são soluções inteiras do sistema de congruência lineares independentes:*

$$\begin{cases} 100y - 10 \equiv 0 \ mod\ p \\ 100x - 1 \equiv 0 \ mod\ p \end{cases}$$

Demonstração: Suponhamos que p divide $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$. Como $m = a_r \cdot 10^{r-2} + \cdots + a_2 + y a_1 + x a_0$, segue que:

$$100m = n - 10a_1 - a_0 + 100y a_1 + 100x a_0 = n + (100y - 10)a_1 + (100x - 1)a_0. \quad (3.8)$$

Assim, para que p divida m basta que p divida $100y - 10$ e $100x - 1$, visto que $p \mid n$. Isto mostra que basta determinar os inteiros x e y tais que $100y - 10 \equiv 0 \ mod\ p$ e $100x - 1 \equiv 0 \ mod\ p$, isto é, x e y são soluções do sistema de congruência linear:

$$\begin{cases} 100y - 10 \equiv 0 \ mod\ p \\ 100x - 1 \equiv 0 \ mod\ p \end{cases}$$

Reciprocamente, se x e y são soluções das congruências acima e $p \mid m$ segue de (3.8) que $p \mid n$. ■

3.3 Três quebras, nas unidades, nas dezenas e nas centenas

Seja $n = a_r a_{r-1} \cdots a_1 a_0$ um número natural. Nesta seção apresentamos um critério de divisibilidade que consistem em "quebrar" o número n no algarismo das unidades, das dezenas e das centenas, obtendo, a partir deste, o número $m = a_r a_{r-1} \cdots a_3 + za_2 + ya_1 + xa_0$ para alguns inteiros x, y e z a serem determinados. O objetivo aqui é o mesmo das seções anteriores, mostrar que um determinado primo p divide n se, e somente se, p divide m.

3.3.1 Critério de divisibilidade por 23

Um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ *é divisível por* 23 *se, e somente se,* $m = a_r a_{r-1} \cdots a_3 + za_2 + ya_1 + xa_0$ *é divisível por* 23.

Demonstração: Inicialmente suponhamos que $23 \mid m$, ou seja: $m = a_r \cdot 10^{r-3} + \cdots + a_3 + za_2 + ya_1 + xa_0 \equiv 0 \ mod\ 23$. Multiplicando a congruência por 10^3, obtemos: $a_r \cdot 10^r + \cdots + a_3 \cdot 10^3 + 1000za_2 + 1000ya_1 + 1000xa_0 \equiv 0 \ mod\ 23$. Note que $a_r \cdot 10^r + \cdots + a_3 \cdot 10^3 = n - 100a_2 - 10a_1 - a_0$, substituindo na última congruência obtemos:

$$n - 100a_2 - 10a_1 - a_0 + 1000za_2 + 1000ya_1 + 1000xa_0 \equiv 0 \ mod\ 23 \tag{3.9}$$

$$n + (1000z - 100)a_2 + (1000y - 10)a_1 + (1000x - 1)a_0 \equiv 0 \ mod\ 19$$

Daí, para que $23 \mid n$, nosso problema consiste em resolver o seguinte sistema de congruência independente:

$$\begin{cases} 1000z - 100 \equiv 0 \ mod\ 23 \\ 1000y - 10 \equiv 0 \ mod\ 23 \\ 1000x - 1 \equiv 0 \ mod\ 23 \end{cases}$$

Como $1000 \equiv 11 \ mod\ 23$, obtemos o sistema equivalente:

$$\begin{cases} 11z \equiv 8 \ mod\ 23 \\ 11y \equiv 10 \ mod\ 23 \\ 11x \equiv 1 \ mod\ 23 \end{cases}$$

Transformando essas congruências num sistema de equações Diofantinos independente, temos:

$$\begin{cases} 11z - 23k = 8 \\ 11y - 23k = 10 \qquad \text{com } k, k', k" \in \mathbf{Z} \\ 11x - 23k' = 1 \end{cases}$$

Todas essas equações têm solução, pois $(11, 23) = 1$ e $1 \mid 8, 1 \mid 10$ e $1 \mid 1$, usando novamente o algoritmo de Euclides para resolver essas equações Diofantinos, temos:

Quociente	2	11
23	11	1
Resto	1	0

ou seja, $1 = 23 - 2 \cdot 11$.

Multiplicando essa igualdade por 8 encontramos:

$8 = 11 \cdot (-16) + 23 \cdot 8 = 11 \cdot (-16) - 23 \cdot (-8)$ o que implica em $z = -16$, realizando o mesmo procedimento para as outras equações encontramos: $y = -20$ e $x = -2$, mas como $-16 \equiv 7 \ mod\ 23$ e $-20 \equiv 3 \ mod\ 23$ segue que $z = 7$ e $y = 3$. Portanto n é divisível por 23 se, e somente se, $m = a_r 10^{r-3} + \cdots + a_3 + 7a_2 + 3a_1 - 2a_0$ também for. Substituindo $x = 7$, $y = 3$ e $z = -2$ em (3.9), obtemos:

$$\begin{aligned} n - 100a_2 - 10a_1 - a_0 + 1000 \cdot 7a_2 + 1000 \cdot 3a_1 + 1000 \cdot (-2)a_0 &\equiv \ mod\ 23 \Longrightarrow \\ n - 100a_2 - 10a_1 - a_0 + 7000\ a_2 + 3000\ a_1 - 2000\ a_0 &\equiv \ mod\ 23 \Longrightarrow \\ n + 6900a_2 + 2990a_1 - 2001a_0 &\equiv 0 \ mod\ 23 \end{aligned}$$

Daí, como $6900 \equiv 0 \ mod\ 23$, $2990 \equiv 0 \ mod\ 23$ e $-2001 \equiv 0 \ mod\ 23$, concluímos que $n \equiv 0 \ mod\ 23$. Reciprocamente, se $n \equiv 0 \ mod\ 23$ e $m = a_r \cdot 10^{r-3} + \cdots + a_3 + za_2 + ya_1 + xa_0 \equiv 0 \ mod\ 23$, segue que:

$$1000m = n - 100a_2 - 10a_1 - a_0 + 1000za_2 + 1000ya_1 + 1000xa_0 \Longrightarrow$$

$n + (1000z - 100)a_2 + (1000y - 10)a_1 + (1000x - 1)a_0 = n + 6900a_2 + 2990a_1 - 2001a_0$.

Daí, segue que $m \equiv 0 \ mod\ 23$, assim concluímos que o critério é de fato verdadeiro para $x = -2, y = 3$ e $z = 7$. ■

Exemplo: Verifique se o número $n = 9867359812$ é divisível por 23.

Aplicando o critério sucessivas vezes, temos: $9867359812 \Longrightarrow 9867359 + 7{\cdot}8 + 3{\cdot}1 - 2{\cdot}2 = 9867414 \Longrightarrow 9867 + 7 \cdot 4 + 3 \cdot 1 - 2 \cdot 4 = 9890 \Longrightarrow 9 + 7 \cdot 8 + 3 \cdot 9 - 2 \cdot 0 = 92 \Longrightarrow 7 \cdot 0 + 3 \cdot 9 - 2 \cdot 2 = 27 - 4 = 23$. Portanto como 23 é divisível por 23, segue que 9867359812 também é divisível por 23 como queríamos verificar.

Generalizando esse resultado para qualquer primo p, obtemos o seguinte teorema:

Teorema 18 *Um natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por um primo positivo $p \geq 23$ se, e somente se $m = a_r a_{r-1} \cdots a_3 + za_3 + ya_1 + xa_0$ é divisível por p, onde x, y e z são soluções inteiras do sistema de congruência lineares independentes:*

$$\begin{cases} 1000z - 100 \equiv 0 \ mod\ p \\ 1000y - 10 \equiv 0 \ mod\ p \\ 1000x - 1 \equiv 0 \ mod\ p \end{cases}$$

Demonstração: Suponhamos que p divide $n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$. Como $m = a_r \cdot 10^{r-3} + \cdots + a_3 + za_2 + ya_1 + xa_0$, segue que:

$$1000m = n - 100a_2 - 10a_1 - a_0 + 1000za_2 + 1000ya_1 + 1000xa_0 \Longrightarrow \tag{3.10}$$

$$n + (1000z - 100)a_2 + (1000y - 10)a_1 + (1000x - 1)a_0.$$

Assim, para que p divida m basta que p divida $1000z-100$, $1000y-10$ e $1000x-1$, visto que $p \mid n$. Isto mostra que basta determinar os inteiros x, y e z tais que $1000z-100 \equiv 0\ mod\ p$ $1000y - 10 \equiv 0\ mod\ p$ e $1000x - 1 \equiv 0\ mod\ p$, isto é, x, y e z são soluções do sistema de congruência linear:

$$\begin{cases} 1000z - 100 \equiv 0\ mod\ p \\ 1000y - 10 \equiv 0\ mod\ p \\ 1000x - 1 \equiv 0\ mod\ p \end{cases}$$

Reciprocamente, se x, y e z são soluções das congruências acima e $p \mid m$ segue de (3.10) que $p \mid n$. ■

Antes de encerrar esta seção, chamamos a atenção para um fato curioso sobre tais critérios. Observamos que a incógnita usada para multiplicar o algarismo das unidades nos critérios com uma quebra é sempre a mesma que multiplica as dezenas nos critérios com duas quebras, isso não é simplesmente uma coincidência, pelo contrário percebemos que as equações modulares gerada com uma quebra pelo algarismo das unidades é igual as equações geradas com duas quebras pelo algarismo das dezenas. Para ficar mais claro vejamos o seguinte exemplo, note que as equações modulares: $10x \equiv 1\ mod\ 13$ e $10x \equiv 1\ mod\ 17$ são iguais, respectivamente as equações $9y \equiv 10\ mod\ 13$ e $15y \equiv 10\ mod\ 17$, ou seja, tanto a primeira e a terceira equações possui soluções iguais ($x = y = 4$), quanto a segunda e quarta equações possui soluções iguais ($x = y - 5$).

3.4 Exercícios de fixação

Com objetivo de fixar mais os temas que foram tratados nesse trabalho. Apresentaremos nesta seção uma lista de exercícios com as respostas comentadas, encontraremos aqui questões de vestibulares e de olimpíadas, bem como outras elaboradas pelo próprio autor.

Questão [01] O algarismo das unidades do número $w = 1 \cdot 3 \cdot 5 \cdot 7 \cdots 2013$ é:
a) 2 b) 3 c) 5 d) 6 e) zero

Solução: Esse número w só pode ser ímpar, uma vez que todos os fatores envolvido na multiplicação são ímpares, notemos que um dos seus fatores é o 5 o que implica pelo critério de divisibilidade que o último algarismo só pode ser o 5. Daí, a alternativa correta é a letra C.

Questão [02] Qual o valor de α para que $500\alpha2\alpha$ seja divisível por 66?

Solução: Notemos que um número será divisível por 66, se ele for divisível simultaneamente por 2, 3 e 11, como o último algarismo é 6, então 66 é divisível por 2, como a soma dos algarismos de 66 é divisível por 3, então 66 também é, analisaremos agora o critério de divisibilidade por 11, usando o critério temos que a diferença entre a soma dos algarismos de ordem ímpar e dos algarismos de ordem par é:

$$(5 + \alpha + \alpha) - (0 + 2) = 3 + 2\alpha$$

Como, $\alpha \in (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$, e queremos que a expressão $3 + 2\alpha$ seja um múltiplo de 11, temos: $3 + 2\alpha = 11 \implies \alpha = 4$.

Questão [03] (EPCAR - 2000) Seja o número $m = 488a9b$, onde b é o algarismo das unidades e a o algarismo das centenas. Sabendo - se que m é divisível por 45, então $a + b$ é igual a:
a) 1 b) 7 c) 9 d) 16

Solução: Como m é divisível por 45, então m será divisível por 9 e 5, o número m será divisível por 5 se:

$$\begin{cases} b = 0 \\ \text{ou} \\ b = 5 \end{cases}$$

Como, a e $b \in (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$ temos que analisar os dois casos a seguir, se $b = 0$, então m será divisível por 9 se: $4 + 8 + 8 + a + 9 + 0 = 29 + a = 9k$, onde k é um número inteiro. Se $b = 5$, então m será divisível por 9 se: $4 + 8 + 8 + a + 9 + 5 = 34 + a = 9k'$, onde k' é um número inteiro. Portanto, para que $29 + a$ e $34 + a$ sejam múltiplos de 9, segue que $a = 7$ ou $a = 2$, nas duas situações temos que a soma $a + b = 7$, a resposta é a alternativa B.

Questão [04] (ESA) Se o número $7x4$ é divisível por 18, então o algarismo x:
a) não existe b) vale 4 c) vale 7 d) vale 9 e) vale 0

Solução: Como $x \in (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$, então $7x4$ é divisível por 18 se for divisível por 2 e 9, daí: $7 + x + 4 = 18 \implies x = 7$. Portanto, a resposta certa é a alternativa C.

Questão [05] O resto da divisão por 11 do resultado da expressão: $1211^{20} + 9119^{32} \cdot 343^{26}$ é: a) 0 b) 1 c) 2 d) 3 e) 4

Solução: Perceba que $1211 \equiv 1 \ mod\ 11$, $9119 \equiv 0 \ mod\ 11$ e $343 \equiv 2 \ mod\ 11$, daí temos:

$$1211^{20} + 9119^{32} \cdot 343^{26} = 1^{20} + 0^{32} \cdot 2^{26} = 1 + 0 = 1$$

Portanto a alternativa B é a correta.
Questão [06] Conforme estudado nesse trabalho, responda o que se pede abaixo:

A) Construa um critério de divisibilidade para o primo $p = 7$;
B) Faça a demonstração do critério criado;
C) Usando o critério criado, verifique se o número $n = 1785$ e $m = 1786$ são divisíveis por 7.
Solução: A) Um número $n \in \mathbb{N}$ é divisível por 7 se, e somente se, a diferença entre o número obtido de n retirando - se o algarismo das unidades e o dobro dos algarismo das unidades for divisível por 7, isto é: $n = 10b + a_0$ é divisível por 7 se, e somente se $b - 2a_0$ é divisível por 7.

B) Fazendo a volta primeiro temos que, se $b - 2a_0 = 7k, \in \mathbb{Z}$, multiplicando essa última igualdade por por 10, obtemos $10b - 20a_0 = 70k \Rightarrow 10b - 20a_0 = 7k'$, onde $k' = 10k$, adicionando $21a_0$ dos dois lados da igualdade, ficamos com $10b - 20a_0 + 21a_0 = 7k' + 21a_0 \Rightarrow 10b + a_0 = 7q$, onde $q = (k' + 3a_0)$, logo se $b - 2a_0$ é divisível por 7, então $10b + a_0$ também é divisível por 7. Por outro lado, se $10b + a_0 = 7k, k \in \mathbb{Z}$ reescrevendo essa equação da seguinte forma $10b + 21a_0 - 20a_0 = 7k \Rightarrow 10b - 20a_0 = 7k - 21a_0 \Rightarrow 10b - 20a_0 = 7k' \Rightarrow 10(b - 2a_0) = 7k'$, de (13), como (7,10) =1, então $7 \mid b - 2a_0$, ou seja, $b - 2a_0 = 7k", k" \in \mathbb{Z}$. ■

C) Aplicando o critério, segue que: $178 - 2 \cdot 5 = 168$, repetindo o critério mais uma vez temos: $16 - 2 \cdot 8 = 0$, como 0 é divisível por qualquer número, então 1785 é divisível por 7. Já o número m não é divisível por 7, pois $178 - 2 \cdot 6 = 166 \Rightarrow 16 - 2 \cdot 6 = 4$, mas o 4 não é divisível por 7, assim o número m não é divisível por 7. Observemos que o 4 não é o resto da divisão de 1786 por 7, tendo em vista que 1786 é o sucessor de 1785 e nesse caso o resto seria 1. O critério não preserva o resto ele indica apenas que o número m não é divisível por 7.

Questão[07] Qual o resto de 743^{48} por 6?

Solução: Sabemos que $743 \equiv 5 \ mod\ 6$, como $5 \equiv -1 \ mod\ 6$, segue que $743 \equiv -1 \ mod\ 6$, daí obtemos $743^{48} \equiv (-1)^{48} = 1 \ mod\ 6$, logo 1 é o resto que 743^{48} deixa na divisão por 6.

Questão [08] Conforme visto no teorema 1, prove o corolário: um natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por 19 se, e somente se, $m = a_r a_{r-1} \cdots a_1 + 2a_0$ é divisível por 19.

Solução: Basta encontrar x tal que $10x \equiv 1 \pmod{19}$. Como $20 \equiv 1 \pmod{19}$, segue que $x \equiv 2 \pmod{19}$, assim basta considerar $x = 2$.

Questão [09] Conforme visto no teorema 2, prove o corolário: um natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por 23 se, e somente se, $m = a_r a_{r-1} \cdots a_2 + ya_1 + xa_0$ é divisível por 23.

Solução: A prova é feita de maneira análoga as estudadas na seção 2 deste capítulo.

Questão [10] Conforme visto no teorema 3, prove o corolário: um número natural $n = a_r a_{r-1} \cdots a_1 a_0$ é divisível por 29 se, e somente se, $m = a_r a_{r-1} \cdots a_3 + za_2 + ya_1 + xa_0$ é divisível por 29.

Solução: A prova é feita de maneira análoga as estudadas na seção 3 deste capítulo.

4 Considerações Finais

Neste trabalho apresentamos como são criados os critérios de divisibilidade de alguns números primos, ressaltamos que a criação desses critérios podem ser expandidos para quaisquer primo como ficou apresentado nas generalizações, tínhamos como objetivo principal despertar o interesse e a curiosidade tanto dos alunos de cursos de matemática, quanto os da educação básica para o estudo da aritmética.

A metodologia usada no último capítulo estruturou - se principalmente da ideia de mostrar que um determinado primo p divide n se, e somente se, p divide m. Portanto, nosso objetivo era identificar e aproveitar os elementos presentes nos critérios de divisibilidade usuais e implementá - los no desenvolvimento dos critérios incomuns e curiosos.

Inicialmente revisitamos o conjunto dos números inteiros, estudamos suas principais propriedades tais como princípio da boa ordem, princípio de indução matemática, algoritmo da divisão, aritmética modular entre outras.

Observamos que a eficiência deste método não se caracteriza apenas em afirmar se o número n é ou não divisível por p mais também pela redução de uma ordem de magnitude em cada etapa de sua aplicação. Caso n não for divisível por p esse processo não garante a preservação do resto de n em todas as etapas, ou seja, o resto que n deixa na divisão por p não será necessariamente igual a resto que m deixa na divisão por p.

Embora alguns assuntos tratados aqui sejam de matemática superior, os teoremas básicos da aritmética se mostram de fácil entendimento, além do mais compreendidas as proposições, tais critérios de divisibilidade, antes apresentados de forma mecânica e sem justificativa, passam a fazer mais sentido.

Além disso, esta pesquisa também tem a finalidade de servir como material de apoio para ser utilizado em formação inicial e continuada de docentes, bem como servir de material didático para ser usado pelos alunos em sala de aula, com objetivo de praticar a aritmética básica de maneira curiosa e divertida.

Finalizamos esse trabalho deixando o seguinte desafio, será que é possível desenvolver critérios de divisibilidade para qualquer número com método de quebra de algarismos em diferentes posições sem levar em consideração necessariamente a sua ordem?

Referências

[1] ALENCAR FILHO, E. A. *Teoria Elementar dos Números*. São Paulo, Nobel, 1989. 12, 17, 18, 32, 33

[2] BARRETO, R.C.P.P. *Aritimética Modular, Códigos Elementares e Criptografia*. Dissertação(TCC) - Universidade Federal de Sergipe, São Cristovão, 2014. 12, 30

[3] CLUBE DE MATEMÁTICA DA OBMEP, *Disseminando o estudo da matemática*, disponível em: http://clubes.obmep.org.br/blog/teoria-dos-numeros-um-pouco-sobre-divisibilidade-parte-2/um-pouco-sobre-divisibilidade-criterios-de-divisibilidade/, acesso em 09/06/2019. 12, 23, 34

[4] COUTINHO, S. C. *Número Inteiros e Criptografia RSA*, Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA. 2013. 10, 12, 14

[5] FONSECA, M.A.G. *Divisão de Polinômios em Várias Variáveis.*(TCC) - Fundação de Ensino Superior de Olinda - FUNESO, Olinda, 2003. 12, 14, 24

[6] FRANCO, T.R.R. *Divisibilidade e Congruências: Aplicações no ensino fundamental 2*. Dissertação(TCC) - Universidade Federal de Goiás, Jataí, 2016. 20, 24

[7] GONÇALVES, A. *Introdução à Álgebra*.5 ed. (Projeto Euclides). Rio de Janeiro. in, 2012. 10, 12

[8] HEFEZ, A. *Um curso de Álgebra*, Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA. 2002. 15, 20, 21, 25

[9] HEFEZ, A. *Aritmética*, Coleção do PROFMAT - SBM. Rio de Janeiro, 2012. 12, 19, 23, 26, 28

[10] LORENSATTI, E.J.C. *Aritmética: um pouco de história*.in; ANPEDSUL, Seminário em educação da região sul. Caxias do Sul, 2012. 10, 12

[11] NETO, H.J.D. *Critérios de divisibilidade*. Dissertação(TCC) - Universidade Federal de Dourados, Dourados, 2016. 34