UNIVERSIDADE DO ESTADO DO AMAZONAS
ESCOLA NORMAL SUPERIOR
LICENCIATURA EM MATEMATICA

REBECA MENEZES FIRMINO

CONGRUÊNCIA E OS CRITÉRIOS DE DIVISIBILIDADE

MANAUS, MAIO
2022

REBECA MENEZES FIRMINO

CONGRUÊNCIAS E OS CRITÉRIOS DE DIVISIBILIDADE

Trabalho de Conclusão do Curso elaborado junto às disciplinas TCC I e TCC II do Curso de Licenciatura em Matemática da Universidade do Estado do Amazonas para a obtenção do grau de licenciado em Matemática.

Orientador: Prof. Dr. Almir Cunha da Graça Neto.

MANAUS, MAIO

2022

AMAZONAS
GOVERNO DO ESTADO

TERMO DE APROVAÇÃO DE TRABALHO DE CONCLUSÃO DO CURSO

Ata de Defesa do Trabalho de Conclusão de Curso em Licenciatura em Matemática da Escola Normal Superior-UEA de **REBECA MENEZES FIRMINO.**

Em 17 de maio de 2022, às 20:00h, na sala Benito D'Antona na presença da Banca Examinadora composta pelos professores: Dr. Almir Cunha da Graça Neto, Me. Geraldine Silveira Lima e Me. Edson Lopes de Souza a, o(a) aluno(a) **REBECA MENEZES FIRMINO** apresentou o Trabalho de Conclusão do Curso intitulado: "**Congruências e os critérios de divisibilidade.**" A Banca Examinadora deliberou e decidiu pela Aprovação do referido trabalho, com o conceito 9,4 divulgando o resultado ao aluno e demais presentes.

Presidente da Banca Examinadora

Orientador (a)

Avaliador 1

Avaliador 2

Aluno

Escola Normal Superior
Av. Djalma Batista, N° 2470, Chapada
Cep: 69050-010 / Manaus-AM
www.uea.edu.br

UEA
UNIVERSIDADE DO ESTADO DO AMAZONAS

AGRADECIMENTOS

"*Agradeço a meu Deus toda vez que me lembro de vocês*." Filipenses 1:3

Sou grata a Deus Emanuel: sempre presente e sempre conosco. Grata por Seu sustento e Graça. Agradeço a ele por ter estado presente nesta jornada através de pessoas que me acolheram, orientaram e consolaram.

Agradeço aos meus pais, Silvana e Ricardo, a força de vocês me sustenta e é a expressão mais próxima do Senhor por minha vida. Aos meus irmãos, Filipe, André e Débora, por serem meus bons companheiros. Ao de lado de vocês experimento uma fração da eternidade.

A vocês, meus professores, um muito obrigada não basta. Vocês foram cruciais em minha jornada, me ajudaram a construir e desconstruir conceitos, a compreender teorias que antes achava incompreensíveis, compartilharam o conhecimento que possuem e não desistiram quando encontravam uma sala dispersa ou desanimada.

Levarei sempre comigo cada palavra que ouvi, sempre me lembrarei dos seminários, dos cálculos na lousa, dos slides, de tudo aquilo que foi muito bem ensinado por vocês, meus mestres. Sou grata a cada professora e professor que passou no meu caminho, aprendi muito com vocês e dedico a vocês também essa conquista.

Agradeço ao povo brasileiro pelos investimentos durante todo este tempo. Minha oração é que todos os recursos dispostos a mim sejam retribuídos a vocês em forma de uma educação de qualidade.

E um agradecimento especial ao meu orientador, professor Dr. Almir Cunha da Graça Neto, por ter me aceitado como orientanda, pelos conhecimentos que adquiri e as discussões feitas sobre a temática deste trabalho científico. Você se tornou meu exemplo de competência e conhecimento.

Enfim os meus eternos alunos, agradeço por terem sido instrumento para que eu aprendesse que eu não educo ninguém, mas que nos educamos mutuamente. Obrigada pelo privilégio de aprendermos juntos e por terem me proporcionado o frio na barriga de quando fui chamada de professora pela primeira vez.

RESUMO

O tema deste trabalho científico é “Congruências” e a delimitação deste é “Congruências e os Critérios de Divisibilidade”, considerando o seguinte problema: quando que um número inteiro é divisível por 2 ao 11, amparado pelas propriedades de Congruências? Diante disso, o objetivo geral é utilizar as Congruências para provar os Critérios de Divisibilidade por $2, 3, 4, 5, 6, 7, 8, 9, 10$ e 11 e algumas questões norteadoras são exibidas. Para tal fim, foi necessário estudar os conceitos das Congruências, Divisibilidade e os Critérios de Divisibilidade. Em consequência, a elaboração e aplicação do projeto obteve resultados favoráveis dado que foi possível demonstrar todos as regras de divisibilidade propostas utilizando Congruências. Trata-se de um trabalho de grande pertinência, seja para o professor quanto para aluno do Ensino Básico ou Superior. O trabalho é fundamentado teoricamente por Filho (1981); Machado (2018); Santos (1998); Rosen (2011); Durbin (2008); Mcdowell (2022); Domingues e Iezzi (2003); Silva (2015), Rodrigues (2013) e Moura (2015). No capítulo 1, serão apresentadas e demonstradas algumas propriedades básicas de Divisibilidade. No capítulo 2, será definida a congruência módulo m e demonstradas algumas de suas propriedades. No último capítulo, aborda-se os Critérios de Divisibilidade e a prova destes utilizando congruências.

Palavras-Chave: congruências. divisibilidade. critérios. propriedades.

SUMÁRIO

INTRODUÇÃO

Os Critérios de Divisibilidade determinam se um número inteiro é divisível por outro inteiro, sem necessariamente efetuar o algoritmo da divisão. Por exemplo, o Critério de Divisibilidade por 3 afirma que se a soma dos dígitos de um número for divisível por 3, consequentemente o número também é divisível por 3.

Sabe-se também que pela definição das Congruências, o número inteiro a é congruente ao inteiro b módulo m $(m > 0)$ se m divide $a - b$, ou seja $m|(\mathrm{a} - \mathrm{b})$, isto é, $a - b = m \cdot q$ para algum $q \, \epsilon \, \mathbb{Z}$. Diante disso, considera-se a seguinte problemática: amparado pelas propriedades das Congruências, quando que um número inteiro é divisível por $2, 3, 4, 5, 6, 7, 8, 9, 10$ e 11?

É evidente a relevância dos Critérios de Divisibilidade na resolução de problemas, logo a contribuição deste trabalho é esclarecer para a comunidade acadêmica e população em geral a concatenação dos termos anteriormente mencionados, como também aplicar as propriedades das Congruências para provar, pormenorizada e objetivamente, alguns Critérios de Divisibilidade. Desse modo, este trabalho tem como objetivo geral utilizar Congruências para provar os Critérios de Divisibilidade.

As questões norteadoras implicam em expor os Critérios de Divisibilidade por $2, 3, 4, 5, 6, 7, 8, 9, 10$ e 11 e provar tais critérios utilizando Congruências, conforme suas propriedades. Os objetivos específicos compreendem em levantar informações sobre os fundamentos teóricos da Divisibilidade e Congruências; traçar quais propriedades das Congruências serão utilizadas para a prova dos Critérios de Divisibilidade e analisar os argumentos feitos para o cumprimento da proposta do Trabalho.

O trabalho está dividido em 3 capítulos. No capítulo 1, são enfatizados os conceitos que abrangem a Divisibilidade e que foram utilizados ao longo do trabalho, ou seja, as preliminares, que são: Máximo Divisor Comum, Divisibilidade, Algoritmo de Euclides, Mínimo Múltiplo Comum, Números Primos e Representação dos Inteiros em outras bases. O capítulo 2, envolve as propriedades das Congruências, no qual algumas destas foram determinadas para a prova dos Critérios de Divisibilidade. No capítulo, 3 são englobadas as descrições dos Critérios de Divisibilidade, as provas desses critérios utilizando Congruências, juntamente com exemplos e as considerações finais do trabalho.

CAPÍTULO 1

PRELIMINARES

Neste capítulo abordaremos as propriedades de Divisibilidade[1] dos números inteiros bem como suas demonstrações, serão evidenciados a Indução, a noção de Divisibilidade, Máximo Divisor Comum, Números Primos e Mínimo Múltiplo Comum.

1.1 INDUÇÃO MATEMÁTICA

Definição 1.1 (Elemento mínimo do conjunto de inteiros) *Seja A um Subconjunto dos números inteiros. Chama-se elemento mínimo de A um elemento* $a \in A$ *tal que* $a \leq x$ *para todo* $x \in A$.

Representa-se pela notação "minA", que se lê: "mínimo de A". Portanto, simbolicamente: MinA = a $\Leftrightarrow (a \in A \text{ e } (\forall x \in A);\ (a \leq x))$

Teorema 1.1 Se a é *elemento mínimo de* A, então este elemento é *único*.

Demonstração. Com efeito, se existisse um outro elemento mínimo b de A, teríamos

I. $\mathrm{a} \leq \mathrm{b}$, porque $\mathrm{a} = \mathrm{minA}$

II. $\mathrm{b} \leq \mathrm{a}$, porque $\mathrm{b} = \mathrm{minA}$

Logo, pela propriedade anti-simétrica da relação de ordem natural "≤" em Z, temos $\mathrm{a} = \mathrm{b}$.

O elemento mínimo de A, se existe, denomina-se também primeiro elemento de A ou menor elemento de A.

Exemplo 1.1 *O conjunto* $B = \{4, 7, 9, 11, 13, 15, 17\}$ *tem o elemento mínimo, que é 4* $(minB = 4)$, *por que* $4 \in B$ *e* $4 \leq b$ *para todo* $b \in B$.

Exemplo 1.2 *O conjunto* $A = \{a \in Z \,/\, a > 10\}$ *tem o elemento mínimo, que é 11* $(minA = 11)$, *porque* $11 \in A$ *e* $11 \leq x$ *para todo* $x \in A$.

Exemplo 1.3 *O conjunto* $C = \{0, -1, \ldots, -7, -8, \ldots\}$ *não tem o elemento mínimo, porque não existe* $x \in C$ *tal que* $x \leq c$ *para todo* $c \in C$.

Exemplo 1.4 *O conjunto* $D = \{d \in N \,/\, 2 \text{ divide } d^3\}$ *tem o elemento mínimo* 2 $(minD = 2)$, *porque* $2 \in D$ $(2 \text{ divide } 8)$ *e* $2 \leq d$ *para todo* $d \in A$.

Definição 1.2 (Princípio da Boa Ordenação). *Todo conjunto não vazio* A *de inteiros não negativos possui o elemento mínimo*.

[1] Todas Definições, Teoremas, Corolários de Divisibilidades exibidas neste capítulo estão fundamentados por (FILHO, 1981) em sua obra Teoria Elementar dos Números.

Em outros termos, todo o subconjunto não vazio A do conjunto $\mathbb{Z}_+ = \{0,1,2,3,4,\dots\}$ *dos inteiros não negativos (*$\Phi \neq A \subset Z_+$*) possui o elemento mínimo, isto é, simbolicamente: (*$\forall\ A \subset Z_+,\ A \neq \Phi$*)* $\rightarrow \exists$ *minA*

Exemplo 1.5 *O conjunto* $E = \{x \in Z\ /\ 2\ \text{não}\ divide\ x\}$ *é um subconjunto não vazio de* $Z_+(\Phi \neq E \subset Z_+)$*. Logo, pelo Princípio da Boa Ordenação, E possui o elemento mínimo* $(minE = 1)$*.*

Exemplo 1.6 *O conjunto* $F = \{f \in Z\ /\ f\ \text{é}\ divisível\ por\ 1\ e\ f\}$ *é um subconjunto não vazio de* $Z_+(\Phi \neq P \subset Z_+)$*. Logo, pelo "Princípio da Boa Ordenação", F possui o elemento mínimo* $(minF = 2)$*.*

Teorema 1.2 (de Arquimedes) *Se* a *e* b *são dois inteiros positivos quaisquer, então existe um inteiro positivo* n *tal que* $n \cdot a \geq b$*.*

Demonstração. Suponha-se que a e b são dois inteiros positivos para os quais $n \cdot a < b$ para todo inteiro positivo n. Então, todos os elementos do conjunto:

$S = \{b - n \cdot a\ /\ n \in N\}$ são *inteiros positivos* e, pelo "Princípio da Boa Ordenação", S possui o *elemento mínimo* digamos $minS = b - k \cdot a$.

E como $b - (k+1) \cdot a$ pertence a S, porque S contém todos os inteiros positivos desta forma, temos

$$b - (k+1) \cdot a = (b - k \cdot a) - a < b - k \cdot a$$

isto é, $b - k \cdot a$ não é o *elemento mínimo* de S, o que é uma *contradição*. Logo, a *propriedade arquimediana* é verdadeira.

Exemplo 1.7 *Se* $a = 5$ *e* $b = 16$*, então* $n = 4$*, pois* $4 \cdot 5 > 16$*.*

Exemplo 1.8 *Se* $a = 10$ *e* $b = 7$*, então* $n = 1$*, pois* $1 \cdot 10 > 7$*.*

Teorema 1.3 (Princípio de Indução Finita). *Seja* S *um subconjunto do conjunto N dos inteiros positivos* $(S \subset N)$ *que satisfaz as duas seguintes condições:*

I. 1 pertence a S $(1 \in S)$;

II. Para todo inteiro, positivo k*, se* $k \in S$*, então* $k + 1 \in S$*.*

Nestas condições, S é o conjunto N dos inteiros positivos: S = N.

Demonstração. Suponha-se, por absurdo, que S não é conjunto N dos inteiros positivos $(S \neq N)$ e seja X o conjunto de todos os inteiros positivos que não pertencem a S, isto é: $X = \{x\ /\ x \in N\ \text{e}\ x \notin S\} = N - S$

Então, X é um *subconjunto* não vazio de N $(\Phi \neq X \subset N)$ e, pelo "Princípio da Boa Ordenação", existe o *elemento mínimo* x_0 de $X(minX = x_0)$.

Pela condição (I), $1 \in S$, de modo que $x_0 > 1$ e, portanto, $x_0 - 1$ é um inteiro positivo que não pertence a X. Logo $x_0 - 1 \in S$ e, pela condição (II), segue-se que $(x_0 - 1) + 1 = x_0 \in S$, o que é uma *contradição*, pois, $x_0 \in X = N - S$, isto é, $x_0 \notin S$. Assim sendo, $X = \Phi$ e $S = N$.

Consoante este "Princípio de Indução Finita", o único *subconjunto* de N que satisfaz às condições (I) e (II) é o próprio N.

Teorema 1.4 [2](Segundo Princípio de Indução Finita). *Seja P(n) uma proposição associada a cada inteiro positivo n e que satisfaz às duas seguintes condições:*

I. P(1) é verdadeira;

II. Para todo inteiro positivo k, se P(k) é verdadeira, então P($k + 1$) também é verdadeira.

Nestas condições, a proposição P(n) é verdadeira para todo inteiro positivo n.

Demonstração. Seja S o conjunto de todos os inteiros positivos n para os quais a proposição $P(n)$ é verdadeira, isto é: $S = \{n \in N \,/\, P(n)$ é verdadeira $\}$

Pela condição (I), P(1) é verdadeira e, portanto, $1 \in S$. Pela condição (II), para todo o inteiro positivo k, se $k \in S$, então $k + 1 \in S$. Logo, o conjunto S satisfaz às condições (I) e (II) do "Princípio de Indução Finita" e, portanto, $S = N$, isto é, a proposição $P(n)$ é verdadeira para todo inteiro positivo n.

Exemplo 1.9 [3]*Se $S(n)$ é denotado pela soma:*

$$a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$$

dos primeiros n termos de uma progressão geométrica com primeiro termo a e proporção comum $r \neq 1$, então

$$S(n) = \frac{a - a \cdot r^n}{1 - r}$$

Demonstração.

I. P(1) é verdadeira, visto que $S(1)\frac{a - a \cdot r^n}{1 - r} = a$

II. A hipótese de indução é que $P(k)$ é verdadeira. Logo,

$$S(k) = \frac{a - a \cdot r^k}{1 - r}$$

[2] O Teorema 1.4 é conhecido, também, como Indução Matemática ou Princípio da Indução Matemática.

[3] Este exemplo está de acordo com (DURBIN, 2008).

$$S(k+1) = S(k) + a \cdot r^k = \frac{a - a \cdot r^n}{1-r} + a \cdot r^k = \frac{a - a \cdot r^k + (1-r) \cdot a \cdot r^k}{1-r}$$

$$S(k+1) = \frac{a - a \cdot r^{k+1}}{1-r}$$

e isto significa que a tese $P(k+1)$ é verdadeira. Logo, pelo "Segundo Princípio de Indução Finita", $P(k)$ implica $P(k+1)$.

1.2 DIVISIBILIDADE

Definição 1.3 (Relação de Divisibilidade em Z). *Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a divide b se, se e somente, existe um inteiro q tal que $b = a \cdot q$. Se a divide b também se diz que a é um divisor de b, que b é um múltiplo de a, que a é um fator de b ou b é divisível por a.*

Com a notação $a \mid b$ indica-se que $a \neq 0$ divide b e, portanto, a notação $a \nmid b$ significa que $a \neq 0$ não divide b. A relação "a divide b ($a \mid b$)" denomina-se relação de divisibilidade em Z.

Se a é um divisor de b, então $-a$ também é um divisor de b, porque a igualdade $b = a \cdot q$ implica $b = (-a) \cdot (-q)$, de modo que os divisores de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos (simétricos).

Exemplo 1.10

a) $3 \mid 9$, porque $9 = 3 \cdot (3)$

b) $-6 \mid 42$, porque $42 = 7 \cdot (-6)$

c) $3 \mid -21$, porque $-21 = 7 \cdot (-3)$

d) $4 \nmid 19$, porque não existe $q \in Z$ tal que $19 = 4 \cdot q$

Teorema 1.5 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 $a \cdot c \mid b \cdot d$

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 $a \mid (b \cdot x + c \cdot y)$, $\forall\, x, y \in$ Z

Demonstração:

I. Com efeito: $0 = a \cdot 0$, $a = 1 \cdot a$, $a = a \cdot 1$

II. Com efeito, se $a \mid 1$, então $1 = a \cdot q$, com $q \in Z$, o que implica $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, isto é $a = \pm 1$.

III. Com efeito: $a \mid b \rightarrow b = a \cdot q$, com $q \in Z$ e $c \mid d \rightarrow d = c \cdot q_1$, com $q_1 \in Z$.
Portanto: $b \cdot d = (a \cdot c) \cdot (q \cdot q_1) \rightarrow a \cdot c | b \cdot d$

IV. Com efeito: $a \mid b \rightarrow b = a \cdot q$, com $q \in Z$ e $b \mid c \rightarrow c = b \cdot q_1$, com $q_1 \in Z$.
Portanto: $c = a \cdot (q \cdot q - 1) \rightarrow a \mid c$

V. Com efeito: $a \mid b \rightarrow b = a \cdot q$, com $q \in Z$ e $b \mid a \rightarrow a = b \cdot q_1$, com $q_1 \in Z$
Portanto: $a = a \cdot (q \cdot q_1) \rightarrow q \cdot q_1 = 1 \rightarrow q_1 \mid 1$

$$\rightarrow q_1 = \pm 1 \rightarrow a = \pm b$$

VI. Com efeito: $a \mid b, b \neq 0 \rightarrow b = a \cdot q, q \neq 0 \rightarrow |b| = |a| \cdot |q|$
Como $q \neq 0$, segue-se que $|q| \geq 1$ e, portanto: $|b| \geq |a|$

VII. Com efeito: $a \mid b \rightarrow b = a \cdot q$, com $q \in Z$ e $a \mid c \rightarrow c = a \cdot q_1$, com $q_1 \in Z$.
Portanto, quaisquer que sejam os inteiros x e y: $b \cdot x + c \cdot y = a \cdot q \cdot x + a \cdot q_1 \cdot y = a \cdot (q \cdot x + q_1 \cdot y) \rightarrow a \mid (b \cdot x + c \cdot y)$. Esta propriedade (VII) admite uma óbvia generalização; isto é, se $a | b_k$, para $k = 1,2,3,\ldots,n$ então, quaisquer que sejam os inteiros $x_1, x_2, \ldots, x_n$: $a \mid (b_1 \cdot x_1 + b_2 \cdot x_2 + \ldots + b_n \cdot x_n$.
Consoante as propriedades (I) e (IV), a relação de divisibilidade Z é *reflexiva* e *transitiva*, mas não simétrica, porque, por exemplo, $2 \mid 8$ e $8 \nmid 2$.

Definição 1.4 (Conjunto dos Divisores de um inteiro) *O conjunto de todos os divisores de um inteiro qualquer a indica-se por $D(a)$, isto é: $D(a) = \{x \in Z^* / \ x \mid a\}$ no qual Z^* denota o conjunto dos inteiros não nulos ($\neq 0$).*

Definição 1.5 (Conjunto dos Divisores de dois inteiro*) Chama-se divisor comum de dois inteiros a e b todo inteiro $d \neq 0$ tal que $d \mid a$ e $d \mid b$.*

Em outros termos, divisor comum de dois inteiros a e b é todo inteiro $d \neq 0$ que pertence simultaneamente aos conjuntos $D(a)$ e $D(b)$. O conjunto de todos os divisores comuns a dois inteiros a e b indica-se por $D(a,b)$. Portanto, simbolicamente: $D(a,b) = \{x \in Z / x \mid a \text{ e } x \mid b\}$
ou seja: $D(a,b) = \{x \epsilon Z^* / \ x \epsilon D(a)$ *e* $x \epsilon D(b)\}$ *e, portanto:* $D(a,b) = D(a) \cap D(b)$

A interseção (∩) é uma operação comutativa, de modo que $D(a,b)$ não depende a ordem dos inteiros dados a e b, isto é: $D(a,b) = D(b,a)$.

Como -1 e 1 são divisores comuns de dois inteiros quaisquer a e b, segue-se que o conjunto $D(a,b)$ dos divisores comuns de a e b nunca é vazio: $D(a,b) \neq 0$. Em

particular, se $a = b = 0$*, então todo inteiro não nulo é um divisor comum de* a *e* b*, isto é:* $D(a,b) = Z^*$*.*

Exemplo 1.11 *Sejam os inteiros* $a = 10$ *e* $b = 20$*. Tem-se:* $D(10) = \{+1, +2, +5, +10\}$ *e* $D(20) = \{+1, +2, +4, +5, +10, +20\}$*. Portanto:* $D(10,20) = D(10) \cap D(20) = \{+1, +2, +5, +10\}$.

Teorema 1.6 (O Algorítimo da divisão) *Se* a *e* b *são dois inteiros,* $b > 0$*, então existem e são únicos os inteiros* q *e* r *que satisfazem às condições*

$$a = b \cdot q + r \text{ e } 0 \leq r < b$$

Demonstração. Seja S o conjunto dos números inteiros não negativos, que são da forma de $a - b \cdot x$, com $x \in Z$, isto é: $Z = \{a - b \cdot x \,/\, x \in Z, a - b \cdot x \geq 0\}$. Este conjunto S não é vazio ($S \neq \emptyset$), porque, sendo $b > 0$, então $b \geq 1$ e portanto, para $x = -|a|$, resulta $a - b \cdot x = a + b \cdot |a| \geq a + |a| \geq 0$.

Assim sendo, pelo Princípio da Boa Ordenação, existe o *elemento mínimo* r de S tal que $r \geq 0$ e $r = a - b \cdot q$ e com $q \in Z$. Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos $0 \leq r - b = a - b \cdot q - b = a - b \cdot (q + 1) < r$, isto é, r não seria o *elemento mínimo* de S.

Para demonstrar a *unicidade* de q e r, suponha-se que existem dois outros inteiros q_1 e r_1 tais que $a = bq_1 + r_1$ e $0 \leq r_1 < b$. Então, teremos: $b \cdot q_1 + r_1 = b \cdot q + r \rightarrow r_1 - r = (q - q_1) \cdot b \rightarrow b \mid (r_1 - r)$.

Por outro lado, temos: $-b < -r \leq 0$ e $\mid r_1 - r \mid < b$, o que implica: $-b < r_1 - r < b$, isto é, $\mid r_1 - r \mid < b$.

Assim, $b \mid (r_1 - R)$ e $\mid r_1 - r \mid < b$ e portanto: $r_1 - r = 0$, e como $b \neq 0$, também temos $q - q_1 = 0$. Logo, $r_1 = r$ e $q_1 = q$.

Corolário 1.1 *Se* a *e* b *são dois inteiros, com* $b \neq 0$*, existem e são únicos os inteiros* q *e* r *que satisfazem as condições:* $a = b \cdot q + r$ *e* $0 \leq r < |b|$

Demonstração. Com efeito, se $b > 0$, nada há que demonstrar, e se $b < 0$, então $|b| > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r tais que $a = |b| \cdot q_1 + r$ e $0 \leq r < |b|$, ou seja, por ser $|b| = -b$: $a = b \cdot (-q_1) + r$ e $0 \leq r < |b|$.

Portanto, existem e são únicos os inteiros $q = -q_1$ e r tais que $a = b \cdot q + r$ e $0 \leq r < |b|$. Os inteiros q e r chamam-se respectivamente o *quociente* e o *resto* na divisão de a por b.

Observe-se que b é divisor de a se, e somente se, o resto $r = 0$. Neste caso, tem-se $a = b \cdot q$ e o quociente q na divisão exata de a por b indica-se também por $\frac{a}{b}$ ou a/b $(q = \frac{a}{b} = a/b)$ que se lê "a sobre b".

Exemplo 1.12 *Achar o quociente q e o resto r na divisão de $a = 66$ por $b = 12$ que satisfazem às condições do algoritmo da divisão.*

Efetuando a divisão usual dos valores absolutos de a e b, obtemos: $66 = 12 \cdot 5 + 6$ e $0 \leq r < 12$. Logo, o quociente $q = 5$ e o resto $r = 6$.

Definição 1.6 (Paridade de um Inteiro). *Na divisão de um inteiro qualquer a por $b = 2$ os possíveis restos são $r = 0$ e $r = 1$. Se $r = 0$, então o inteiro $a = 2 \cdot q$ e é denominado par; e se $r = 1$, então o inteiro $a = 2 \cdot q + 1$ e é denominado ímpar.*

Exemplo 1.13 *Mostre que o quadrado de qualquer inteiro positivo é da forma $6 \cdot k$ ou $6 \cdot k + 1$ para algum inteiro m.*

Temos as seguintes condições:

Condição 1: Quando $m = 6 \cdot q$, para todo $q \in Z$.

$$m^2 = (6 \cdot q)^2 = 36 \cdot q^2 = 6 \cdot (6 \cdot q^2) = 6 \cdot k \text{ quando } k = 6 \cdot q^2.$$

Condição 2: Quando $m = 6 \cdot q + 1$

$m^2 = (6 \cdot q + 1)^2 = 36 \cdot q^2 + 12 \cdot q + 1 = 6 \cdot q \cdot (6 \cdot q + 2) + 1 = 6 \cdot k + 1$ *quando* $k = q \cdot (6 \cdot q + 2)$.

1.3 MÁXIMO DIVISOR COMUM

Definição 1.7 *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se de Máximo Divisor Comum de a e b o inteiro positivo d $(d > 0)$ que satisfaz às condições:*

I. $d \mid a$ e $d \mid b$;

II. Se $c \mid a$ e $c \mid b$, então $c \leq d$.

O Máximo Divisor Comum de a e b indica-se pela notação $mdc(a, b)$.

É imediato que o $mdc(a, b) = mdc(b, a)$. Em particular:

a) O $mdc(0,0)$ não existe;

b) O $mdc(a, 1) = 1$

c) Se $a \neq 0$, então o $mdc(a, 0) = |a|$

d) Se $a|b$, então o $mdc(a, b) = |a|$

Exemplo 1.14 *Sejam os inteiros* $a = 28$ *e* $b = 36$*. Os divisores comuns positivos de* 28 *e* 36 *são 1, 2 e 4, e como o maior deles é 4, segue-se que o* $mdc(28, 36) = 4$*. E o* $mdc(-28, 36) = mdc(28, -36) = mdc(-28, -36) = 4$*.*

Exemplo 1.15 O $mdc(98,1) = 1$*;* $mdc(-27,0) = |-27| = 27$*;* $mdc(-12, 36) = |-12| = 12$

Exemplo 1.16 *Sejam os inteiros* $a = -64$ *e* $b = 72$*. Os divisores comuns positivos de -64 e 72 são 1, 2 ,4 e 8, e como maior deles é 8, segue-se que o* $mdc(-64, 72) = 8$*.*

Teorema 1.7 (Existência e Unicidade do MDC). Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então *existe* e é *único* o $mdc(a, b)$; além disso, *existem* inteiros x e y tais que $mdc(a, b) = a \cdot x + b \cdot y$, isto é, o $mdc(a, b)$ é uma *combinação linear* de a e b.

Demonstração. Seja S o conjunto de todos os inteiros positivos da forma $a \cdot u + b \cdot v$, com $u, v \in Z$, isto é, $S = \{a \cdot u + b \cdot v \,/\, a \cdot u + b \cdot v > 0 \text{ e } u, v \in Z\}$.

Este conjunto S *não é vazio* $(S \neq 0)$, porque, por exemplo, se $a \neq 0$, então um dos dois inteiros $a = a \cdot 1 + b \cdot 0$ e $-a = a \cdot (-1) + b \cdot 0$ é *positivo* e pertence a S.

Logo pelo "Princípio da boa ordenação", *existe* e é *único* existe o elemento mínimo d de S: $minS = d > 0$. E, consoante a definição de S, existem inteiros x e y tais que $d = a \cdot x + b \cdot x$.

Segue-se, pelo *algorítimo da divisão*, que $a = d \cdot q + r$, com $0 \leq r < d$, o que dá $r = a - d \cdot q = a - (a \cdot x + b \cdot y) \cdot q = (1 - q \cdot x) \cdot a + (-q \cdot y) \cdot b$, isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o *elemento mínimo* de S, sucede que $r = 0$ e $a = d \cdot q$, isto é, $d|a$.

Com raciocínio inteiramente análogo se conclui que também $d \mid b$. Logo, d é um *divisor comum positivo* de a e b.

Finalmente, se c é um divisor comum postivo qualquer de a e b ($c \mid a$ e $c \mid b$, c > 0, então $c \mid (a \cdot z + b \cdot y) \rightarrow c \mid d \rightarrow c \leq d$, isto é, d é um *divisor comum positivo* de a e b, ou seja:

$$mdc(a, b) = d = a \cdot x + b \cdot y, x, y \in Z$$

e o teorema fica demonstrado.

Exemplo 1.17 *Sejam os inteiros a = 198 e b = 88. Temos que o* $mdc(198, 88) = 22 = 198 \cdot (1) + 88 \cdot (-2)$*.*

Exemplo 1.18 *Sejam os inteiros a = 8 e b = 34. Temos que o* $mdc(8, 34) = 2 = 8 \cdot (-4) + 34 \cdot (1)$*.*

Teorema 1.8 *Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então o conjunto de todos os múltiplos do $mdc(a,b) = d$ é*

$$T = \{a \cdot x + b \cdot y \,/\, x, y \in Z\}$$

Demonstração. Como $d \mid a$ e $d \mid b$, segue-se que $d \mid (a \cdot x + b \cdot y)$, quaisquer que sejam os inteiros x e y, e por conseguinte todo elemento do conjunto T é um *múltiplo* de d.

Por outro lado, existem inteiros x_0 e y_0 tais que $d = a \cdot x_0 + b \cdot y_0$ de modo que todo *múltiplo* $K \cdot d$ de d é da forma $K \cdot d = K \cdot (a \cdot x_0 + b \cdot y_0) = a \cdot (K \cdot x_0) + b \cdot (K \cdot y_0)$.

isto é, $K \cdot d$ é uma *combinação linear* de a e b e, portanto, $K \cdot d$ é o elemento do conjunto T.

Definição 1.8 (Inteiros primos entre si) *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Diz-se que a e b são primos entre si se, e somente se, o $mdc(a,b) = 1$.*

Teorema 1.9 Dois inteiros a e b, não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), são *primos entre si* se, e somente se, existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$.

Demonstração.

(→) Se a e b são *primos entre si*, então o $mdc(a,b) = 1$ e por conseguinte existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$.

(←) Reciprocamente, se existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$ e se o $mdc(a,b) = d$, então $d|a$ e $d|b$. Logo $d|(a \cdot x + b \cdot y)$ e $d|1$, o que implica $d = 1$ ou $mdc(a,b) = 1$, isto é, a e b *são primos entre si*.

Corolário 1.2 *Se o $mdc = (a,b) = d$, então o mdc $(a \mid d,\ b \mid d)$ são inteiros, porque d é um divisor comum de a e b.*

Demonstração. Preliminarmente, observe-se que $a \mid d$ e $b \mid d$ são *inteiros*, porque d é um *divisor comum* de a e b.

Posto isto, se o $mdc(a,b) = d$, então existem inteiros x e y tais que $a \cdot x + b \cdot y = d$, ou seja, dividindo ambos os membros desta igualdade por d:

$$(a \mid d) \cdot x + (b \mid d) \cdot y = 1$$

Logo, pelo teorema anterior, os inteiros $a \mid d$ e $b \mid d$ são *primos entre si*, isto é, o $mdc(a \mid d,\ b \mid d) = 1$.

Exemplo 1.19 *O $mdc(16,84) = 4$ e $mdc(\frac{16}{4}, \frac{84}{4}) = mdc(4,21) = 1$*

Corolário 1.3 *Se $a \mid b$ e se $mdc(b,c) = 1$, então o $mdc(a,c) = 1$.*

Demonstração. Com efeito: $a|b \rightarrow b = a \cdot q$, com $q \in Z$ e o $mdc(b,c) = 1 \rightarrow b \cdot x + c \cdot y = 1$, com $x, y \in Z$. Portanto, $a \cdot (q \cdot x) + c \cdot y = 1 \rightarrow mdc(a,c) = 1$

Corolário 1.4 *Se a | c, se b | c e se o $mdc(a,b) = 1$, então $a \cdot b|c$.*

Demonstração.

Com efeito, $a|c \rightarrow c = a \cdot q_1$, com $q_1 \in Z$ e $b|c \rightarrow c = a \cdot q_2$, com $q_2 \in Z$ o $mdc(a,b) = 1 \rightarrow a \cdot x + b \cdot y = 1$, com $x, y \in Z \rightarrow a \cdot c \cdot x + b \cdot c \cdot y = c$

Portanto: $c = a \cdot (b \cdot q_2) \cdot x + b \cdot (a \cdot q_1) \cdot y = a \cdot b \cdot (q_2 \cdot x + q_1 \cdot y) \rightarrow a \cdot b|c$

Observe-se que somente as condições $a|c$ e $b|c$ não implicam $a \cdot b|c$.

Exemplo 1.20 $7 \mid 56$ *e* $14 \mid 56$, *mas* $7 \cdot 14 \nmid 56$ *pois o* $mdc(7,14) = 7 \neq 1$.

Corolário 1.5 *Se $mdc(a,b) = 1 = mdc(a,c)$, então o $mdc(a, b \cdot c) = 1$.*

Demonstração. Com efeito, $mdc(a,b) = 1 \rightarrow a \cdot x + b \cdot y = 1$, com $x, y \in Z$ e o $mdc(a,c) = 1 \rightarrow a \cdot z + c \cdot t = 1$, com $z, t \in Z$. Portanto: $1 = a \cdot x + b \cdot y \cdot (a \cdot z + c \cdot t) = a \cdot (x + b \cdot y \cdot z) + b \cdot c \cdot (y \cdot t)$. O que implica $mdc(a, \mathrm{b} \cdot c) = 1$

Corolário 1.6 *Se o $mdc\,(a, b \cdot c) = 1$, então o $mdc\,(a,b) = 1 = mdc\,(a,c)$.*

Demonstração. Com efeito, $mdc(a, b \cdot c) = 1 \rightarrow a \cdot x + (b \cdot c) \cdot y = 1$, com $x, y \in Z$. Portanto, $a \cdot x + b \cdot (c \cdot y) = 1 \rightarrow mdc(a,b) = 1$ e $a \cdot x + c \cdot (b \cdot y) = 1 \rightarrow mdc(a,c) = 1$. Note-se que esta proposição é a *recíproca* da anterior.

Teorema 1.10 (De Euclides) *Se $a|b \cdot c$ e se o $mdc(a,b) = 1$ então $a|c$.*

Demonstração. Com efeito: $a|b \cdot c \rightarrow b \cdot c = a \cdot q$, com $q \in Z$ e o $mdc(a,b) = 1 \rightarrow a \cdot x + b \cdot y = 1$, com $x, y \in Z \rightarrow a \cdot c \cdot x + b \cdot c \cdot y = c$

Portanto, $c = a \cdot c \cdot x + a \cdot q \cdot y = a(c \cdot x + q \cdot y) \rightarrow a|c$. Note-se que somente a condição $a|b \cdot c$ não implica que $a|c$.

Exemplo 1.21 $26 \mid 13 \cdot 6$, mas $26 \nmid 13$ e $26 \nmid 6$ e o $mdc(26,6) \neq 1$ e $mdc(26,13) \neq 13$.

Teorema 1.11 (Caracterização do MDC de dois inteiros). *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Um inteiro positivo d $(d > 0)$ é o $mdc(a,b)$ se, e somente se, satisfaz às seguintes condições:*

I. $d|a$ e $d|b$

II. Se $c|a$ e se $c|b$, então $c|d$

Demonstração.

($\rightarrow$) Suponha-se que o $mdc(a,b) = d$. Então, $d|a$ e $d|b$, isto é, a condição (I) é satisfeita. Por outra parte, existem inteiros x e y tais que $a \cdot x + b \cdot y = d$ e, portanto, se $c|a$ e se $c|b$, então $c|(a \cdot x + b \cdot y)$ e $c|d$, isto é, a condição (II) também é satisfeita.

(←) Reciprocamente, seja d um inteiro postivo qualquer que satisfaz (I) e (II). Então, pela condição (II), todo divisor comum c de a e b também é divisor comum de d, isto é, $c|d$, e isto implica $c \leq d$. Logo, d é o divisor o $mdc(a,b)$.

Definição 1.9 (MDC de vários inteiros) *O conceito de Máximo Divisor Comum, definido para dois inteiros a e b, estende-se de maneira natural a mais de dois inteiros. No caso de três inteiros a, b e c, não todos nulos, o $mdc(a,b,c)$ é o inteiro positivo d $(d > 0)$ que satisfaz às condições:*

I. $d|a$, $d|b$ e $d|c$;

II. Se $g|a$, se $g|b$ e se $g|c$, então $g \leq d$

Exemplo 1.22 *O $mdc(45,26,77) = 1$ e $mdc(26,254,18) = 2$*

Teorema 1.12 O $mdc(a,b,c) = mdc(mdc(a,b),c)$.

Demonstração. Com efeito, seja $mdc(a,b,c) = d$ e $mdc(a,b) = e$. Então, $d|a$, $d|b$, $d|c$, e como existem inteiros x e y tais que $a \cdot x + b \cdot y = g$, segue-se que $d|(a \cdot x + b \cdot y)$ ou $d|g$, isto é, d é um *divisor comum* de g e c ($d|$g e $d \mid c$).

Por outro lado, se f e um *divisor comum* qualquer de g e c ($f|g$ e $f|c$), então $f|g$, $f|b$ e $f|c$, o que implica $f \leq d$. Assim sendo, o $mdc(mdc(a,b),c) = mdc(a,b,c)$.

Exemplo 1.23 Determinar o $mdc(570,810,495)$.

Pelo teorema anterior, temos que o $mdc\ (240,564,348) =\ mdc\ (mdc(240,564),348)$. E como o $mdc(240,\ 564) = 12$, segue-se que o $mdc(240,564,348) = mdc(12,348) = 12$.

1.4 ALGORITMO DE EUCLIDES

Lema 1.1 *Se $a = b \cdot q + r$, então o $mdc(a,b) = mdc(b,r)$.*

Demonstração. Se o $mdc(a,b) = d$, então $d|a$ e $d|a$, o que implica $d \mid (a - b \cdot q)$, isto é, d é um *divisor comum* de b e r ($d \mid b$ e $d \mid r$).

Por outro lado, se c é um *divisor comum* qualquer de b e r ($c \mid b$ e $c \mid r$), então $c \mid (b \cdot q + r)$, isto é, c é um *divisor comum* de a e b, o que implica $c \leq d$. Assim sendo, o $mdc(b,r) = d$.

Definição 1.20 (Algoritmo de Euclides). *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$) cujo máximo divisor comum se deseja determinar. É imediato:*

I.Se $a \neq 0$, então o $mdc(a,0) = |a|$

II.Se $a \neq 0$, então o $mdc(a,a) = |a|$

III.Se $b \mid a$, então o $mdc(a,b) = |b|$

Além disso, por ser $mdc(a,b) = md(|a|,|b|)$*, a determinação do* $mdc(a,b)$ *reduz - se ao caso em que* a *e* b *são inteiros positivos distintos, por exemplos, com* $a > b$*, tais que* b *não divide* a*, isto é:* $a > b > 0$ *e* $b \nmid a$*. Nestas condições, a aplicação repetida do algorítmo da divisão dá-nos as igualdades:*

$$a = b \cdot q_1 + r_1,\ 0 < r_1 < b$$
$$b = r_1 \cdot q_2 + r_2,\ 0 < r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3,\ 0 < r_3 < r_2$$
$$r_2 = r_3 \cdot q_4 + r_4,\ 0 < r_4 < r_3$$
$$.$$
$$.$$
$$.$$

Com os restos $r_1, r_2, r_3, r_4, \ldots$ *são todos inteiros positivos tais que* $b > r_1 > r_2 > r_3 > r_4 > \ldots$ *e existem apenas* $b - 1$ *inteiros positivos menores que* b*, necessariamente se chega a uma divisão cujo resto* $r_{n+1} = 0$*, isto é, finalmente, teremos* $r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}\ r_{n-1} = r_n q_{n+1} + r_{n+1}, r_{n+1} = 0.$

O último resto $r_n \neq 0$ *que aparece nesta sequência da divisão é o máximo divisor comum procurado de* a *e* b*, isto é, o* $mdc(a,b) = r_n$*, visto que, pelo lema anterior, temos:*

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \ldots = mdc(a,b) = mdc(r_{n-2},r_{n-1})$$
$$= mdc(r_{n-1},r_n) = r_n$$

Este processo prático para o cálculo do máximo divisor comum de dois inteiros positivos a *e* b *é denominado Algorítimo de Euclides.*

Exemplo 1.24 Achar o $mdc(864, 598)$ pelo *Algoritimo de Euclides* e sua expressão como combinação linear de 963 e 657.

Tem-se, sucessivamente:

$$864 = 598 \cdot 1 + 266$$
$$598 = 266 \cdot 2 + 66$$
$$266 = 66 \cdot 4 + 2$$
$$66 = 2 \cdot 33 + 0$$

Portanto, $mdc(864, 598) = 2$ e sua expressão como combinação linear de 864 e 598 se obtém eliminando os *restos* 266, 66 e 2 entre as três primeiras igualdades anteriores do seguinte modo:

$$2 = 266 - 4 \cdot 66 = 266 - 4 \cdot (598 - 266 \cdot 2) =$$

$$9 \cdot 266 - 4 \cdot 598$$

Isto é, $2 = mdc(864, 598) = x \cdot 266 - y \cdot 598$, no qual $x = 9$ e $y = -4$.

Teorema 1.13 *Se $k > 0$, então o $mdc(k \cdot a, k \cdot b) = k \cdot mdc(a, b)$.*

Demonstração. Multiplicando ambos os membros de cada uma das $n + 1$ igualdades que dão o $mdc(a, b) = r_n$ pelo *Algoritimo de Euclides* por k, obtemos:

$$ak = (b \cdot k) \cdot q_1 + r_1 \cdot k, \quad 0 < r_1 \cdot k < b \cdot k$$
$$b \cdot k = (r_1 \cdot k) \cdot q_2 + r_2 \cdot k, \quad 0 < r_2 \cdot k < r_1 \cdot k$$
$$r_1.k = (r_2 \cdot k) \cdot q_3 + r_3 \cdot k, \quad 0 < r_3 \cdot k < r_2 \cdot k$$
$$.$$
$$.$$
$$.$$
$$r_{n-2}k = (r_{n-1}k) \cdot q - n + r_n \cdot k, \quad 0 < r_n \cdot k < r_{n-1} \cdot k$$
$$r_{n-1} \cdot k = (r_n \cdot k) \cdot q_{n+1} + 0,$$

Obviamente, estas $n + 1$ igualdades é o *Algoritimo de Euclides* aplicado aos inteiros $a \cdot k$ e $b \cdot k$, e por conseguinte o $mdc(a \cdot k, b \cdot k)$ é último resto $r_n \cdot k \neq 0$, isto é, $mdc(a \cdot k, b \cdot k) = r_n \cdot k = k \cdot mdc(a, b)$.

Exemplo 1.25 *O* $mdc(16, 36) = mdc(2 \cdot 8, 2 \cdot 18) = 2 \cdot mdc(8, 18) = 6 \cdot 2 = 12$

Corolário 1.7 *Para todo $k \neq 0$, o $mdc(k \cdot a, k \cdot b) = |k| \cdot mdc(a, b)$.*

Demonstração. Se $k > 0$, nada há que demonstrar, e se k < 0, então $-k = |k| > 0$ e, pelo Teorema anterior, temos que o $mdc(a \cdot k, b \cdot k) = mdc(-a \cdot k, -b \cdot k) = mdc(a \cdot |k|, b \cdot |k|) = |k| \cdot mdc(a, b)$.

1.5 MÍNIMO MÚLTIPLO COMUM

Definição 1.21 (Múltiplos Comuns de dois Inteiros). *O conjunto de todos os múltiplos de um inteiro qualquer $a \neq 0$ indica-se por $M(a)$, isto é, $M(a) = \{x \in Z / \ a|x\} = \{a \cdot q / \ q \in Z\}$*

Exemplo 1.26 $M(7) = \{7 \cdot q / \ q \in Z\} = 0, 7, 14, 21, 28, \ldots$

É imediato que, para todo inteiro $a \neq 0$, se tem $M(a) = M(-a)$.

Definição 1.22 *Sejam a e b dois inteiros diferentes de zero ($a \neq 0$ e $b \neq 0$). Chama-se Multiplo Comum de a e b todo inteiro x tal que $a \mid x$ e $b \mid x$.*

Em outros termos, múltiplo comum de a e b é todo inteiro que pertence simultaneamente aos conjuntos $M(a)$ e $M(b)$. O conjunto de todos os múltiplos comuns de a e de b indica-se por $M(a,b)$. Portanto, simbolicamente:

$$M(a,b) = \{x \in Z/\ a|x \text{ e } b|x\}$$

ou seja, $M(a,b) = \{x \in Z/\ x \in M(a) \text{ e } x \in M(b)\}$. A interseção $(\cap)$ é uma operação comutativa, de modo que $M(a,b)$ não depende da ordem dos inteiros dados a e b, isto é: $M(a,b) = M(b,a)$. Obviamente, 0 é um múltiplo comum de a e b: $0 \in M(a,b)$. E os produtos $a \cdot b$ e $-(a \cdot b)$ também são múltiplos comuns de a e b.

Exemplo 1.27 *Sejam os inteiros $a = 19$ e $b = -26$. Temos:*

$M(19) = \{19 \cdot q/\ q \in Z = 0, 19, 38, 57, 76, 95, 114, \dots\}$

$M(-26) = \{-26 \cdot q/\ q \in Z = 0, 26, 52, 78, 104, 130, \dots\}$

portanto, $M(19, -26) = M(19) \cap M(-26) = 0, 494, \dots$

Definição 1.23 (Mínimo Múltiplo Comum de dois Inteiros). *Sejam a e b dois inteiros diferentes de zero $(a \neq 0 \text{ e } b \neq 0)$. Chama-se mínimo múltiplo comum de a e b o inteiro positivo* m $(m > 0)$ *que satisfaz às condições:*

I. $a \mid m$ *e* $b \mid m$

II. Se $a \mid c$ *e se* $b \mid c$*, com* $c > 0$*, então* $m \leq c$.

Observe que, pela condição (I), m é um múltiplo comum de a e b, e pela condição (II), m é o menor dentre todos os múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b indica-se pela notação $mmc(a,b)$.

Pelo "Princípio da boa ordenação", o conjunto dos múltiplos comuns positivos de a e b possui o elemento mínimo e, portanto, o $mmc(a,b)$ existe sempre e é único. Além disso, por ser o produto $a \cdot b$ um múltiplo comum de a e b, segue-se que o $mmc(a,b) \leq |a \cdot b|$.

Em particular, se $a|b$, então o $mmc(a,b) = |b|$.

Exemplo 1.28 *Sejam os inteiros $a = 14$ e $b = 21$. Os múltiplos comuns de 14 e 21 são 42, 84, 126,... e como o menor deles é 42, segue-se que o $mmc(14,21) = 42$.*

Teorema 1.14 (Relação entre MDC e o MMC). *Para todo par de inteiros positivos a e b subsiste a relação:*

$$mdc(a,b) \cdot mmc(a,b) = a \cdot b$$

Demonstração. Seja $mdc(a,b) = d$ e $mmc(a,b) = m$. Como $a \mid a \cdot (b/d)$ e $b \mid b \cdot (a/d)$ segue-se que $a \cdot b/d$ é um múltiplo comum de a e b. Portanto, existe um inteiro positivo

k tal que $a \cdot b/d = m \cdot k$, $k \in N$, o que implica $a/d = (m/b) \cdot k$ e $b/d = (m/a) \cdot k$, isto é, k é um *divisor comum* dos inteiros a/d e b/d. Mas a/d e b/d são *primos entre si* (Corolário 1.2), de modo que $k = 1$. Assim sendo, temos que

$$a \cdot b/d = m \text{ ou } a \cdot b = d \cdot m,$$

isto é $a \cdot b = mdc(a,b) \cdot mmc(a,b)$. Esta importante relação permite determinar o mmc de dois inteiros quando se conhece o seu mdc, e vice-versa.

Exemplo 1.29 *Determinar o* $mmc(837, 921)$.

Pelo Algorítimo de Euclides, temos $mdc(837, 921) = 3$. *Portanto,* $mmc(837, 921) = \frac{837 \cdot 921}{3} = 256959$.

Corolário 1.8 *Para todo par de inteiros positivos* a *e* b, *o* $mmc(a,b) = a \cdot b$ *se, e somente se, o* $mdc(a,b) = 1$

Demonstração.

(→) Se o $mdc(a,b) = 1$, então: $a \cdot b = 1 \cdot mmc(a,b) = mmc(a,b)$

(→) Reciprocamente, se o $mmc(a,b) = a \cdot b$, então, $mdc(a,b) \cdot a \cdot b = a \cdot b \rightarrow mdc(a,b) = 1$

Definição 1.24 (MMC de vários inteiros). *O conceito de mínimo múltiplo comum, definido para dois inteiros* a *e* b, *estende-se de maneira natural a mais de dois inteiros. No caso de três inteiros* a, b *e* c, *diferentes de zero, o* $mmc(a,b,c)$ *é o inteiro positivo* m $(m > 0)$ *que satisfaz às condições:*

I. $a \mid m$, $b \mid m$ *e* $c \mid m$

II. Se $a \mid g$, *se* $b \mid g$ *e se* $c \mid g$, *com* $g > 0$, *então* $m \leq g$.

Exemplo 1.30 O $mmc(29, 48, 97) = 135024$.

1.6 NÚMEROS PRIMOS

Definição 1.25 (Números Primos e Compostos) *Diz-se que um inteiro* $p > 1$ *é um número primo ou apenas um primo se, e somente se, 1 e* p *são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se composto. O inteiro positivo 1 não é nem primo nem composto, e por conseguinte se* a *é um o inteiro positivo qualquer, então* a *é primo, ou* a *é composto ou* $a = 1$.

Exemplo 1.*31* *Os números 7,13,17, 19 e 23 são números primos e 6, 18, 22, 24 são números compostos. Enquanto 2 é o único inteiro positivo par e primo.*

Teorema 1.15 *Se um primo* p *não divide um inteiro* a, *então* a *e* p *são primos entre si.*

Demonstração. Seja d o mdc de a e p. Então $d \mid a$ e $d \mid p$. Da relação $d \mid p$, resulta que $d = 1$ ou $d = p$, por que p é *primo*, e como a segunda igualdade é impossível, porque p não divide a, segue-se que $d = 1$, isto é, o $mdc(a,p) = 1$. Logo, a e p são *primos entre si*.

Corolário 1.9 *Se p é um primo tal que $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid a$, nada há que demonstrar, e se, ao invés, p não divide a, então, pelo teorema anterior, o $mdc(p,a) = 1$. Logo, pelo Teorema 1.10 (Euclides), $p|b$.

Corolário 1.10 *Se p é um primo tal que $p \mid a_1, a_2, \ldots, a_n$, então existe um índice k, com $1 \leq k \leq n$, tal que $p \mid a_k$.*

Demonstração. Usando o "Segundo Princípio da Indução Finita", a proposição é verdadeira $p \mid n = 1$ (imediato) e para $n = 2$ (pelo Corolário 1.9). Suponha-se, posi, $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (*hipótese de indução*).

Pelo corolário 1.9, se $p|a_1, a_2, \ldots, a_n$, então $p \mid a_n$ $p|a_1, a_2, \ldots, a_n$. Se $p \mid a_n$, a proposição está demonstrada, e se, ao inés, $p \mid a_1, a_2, \ldots, a_{n-1}$, então a *hipótese de indução* assegura que $p|a_k$, com $1 \leq k \leq n-1$, em qualquer dos dois casos, p divide um dos inteiros $a_1, a_2, \ldots, a_n$.

Corolário 1.11 *Se os inteiros $p, q_1, q_2, \ldots, q_n$ são todos primos e se $p \mid q_1, q_2, \ldots, q_n$, então existe um índice k, com $1 \leq k \leq n$, tal que $p = a_k$.*

Demonstração. Com efeito, pelo Corolário 1.10, existe um índice k, com $1 \leq k \leq n$, tal que $p \mid q_k$, e como os únicos divisores positivos de q_k são 1 e q_k, porque q_k é primo, segue-se que $p = 1$ ou $p = q_k$. Mas, $p > 1$, porque p é primo. Logo, $p = q_k$.

Teorema 1.16 *Todo inteiro composto possui um divisor primo.*

Demonstração. Seja a um inteiro *composto*. Consideremos o conjunto A de todos *divisores positivos* de a exceto os *divisores triviais* 1 e a, isto é, $A = \{x \mid a \,/\, a < x < a\}$. Pelo "Princípio da boa ordenação" existe o *elemento mínimo* p de A, que vamos mostrar ser *primo*. Com efeito, se p fosse *composto* admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d|p$ e $d|a$, o que implica $d \mid a$, isto é, p não seria o e*elemento mínimo* de A. Logo p é *primo*.

1.7 REPRESENTAÇÃO DOS INTEIROS EM OUTRAS BASES

Teorema 1.17 *Dado um inteiro qualquer $b \geq 2$, todo inteiro positivo, todo inteiro positivo n admite uma única representação da forma*

$$n = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0 \cdot b^0$$

Em que os a_i são tais que $0 \leq a_i < b$, i=0,1,2,...,m.

Demonstração. Pelo algorítmo da divisão aos inteiros n e b, tem-se que $n = b \cdot q_1 + a_0$ sendo $0 \leq a_0 < b$. Aplicando, agora, o algorítimo da divisão ao quociente q_1 e ao inteiro b, tem-se $q_1 = b \cdot q_2 + q_1$, $0 \leq a_1 < b$ (1).

Analogamente, continuando a aplicar o algoritimo da divisão aos quocientes obtidos q_1 e ao inteiro b, tem-se

$$q_2 = b \cdot q_3 + q_2,\ 0 \leq a_2 < b \qquad (2)$$

$$q_3 = b \cdot q_4 + q_3,\ 0 \leq a_3 < b \qquad (3)$$

, assim por diante.

Como $n > q_1 > q_2 > q_3 > \cdots$ e cada $q_1 \geq 0$ esta sequência dos quocientes q_i é finita, isto é, existe um índice m tal que

$$q_{m-1} = b \cdot q_m + q_{m-1},\ 0 \leq a_{m-1} < b \qquad (m-1)$$

$$q_m = b \cdot 0 + a_m = a_m,\ 0 \leq a_m < b \qquad (m)$$

Multiplicando por b ambos os membros de (1), por b^2 ambos os mebros de (1), por b^3 ambos os membros de (3)..., por b^{m-1} ambos os membros de $(m-1)$, obtemos o conjunto de igualdades:

$$n = b \cdot q_1 + a_0, \qquad 0 \leq a_0 < b$$

$$b \cdot q_1 = b^2 \cdot q_2 + a_1 \cdot b, \qquad 0 \leq a_1 < b$$

$$b^2 \cdot q_2 = b^3 \cdot q_3 + a_2 \cdot b^2, \qquad 0 \leq a_2 < b$$

$$b^3 \cdot q_3 = b^4 \cdot q_4 + a_3 \cdot b^3, \qquad 0 \leq a_3 < b$$

$$\vdots$$

$$b^{m-1} \cdot q_{m-1} = b^m \cdot q_m + a_{m-1} \cdot b^{m-1}, \qquad 0 \leq a_{m-1} < b$$

Somando ordenadamente todas essas m igualdades, terá-se

$$n + (b \cdot q_1 + b^2 q_2 + \cdots + b^{m-1} \cdot b_{m-1})$$

$$= (b \cdot q_1 + b^2 \cdot q_2 + \cdots + b^{m-1} \cdot b_{m-1}) +$$

$$a_0 + a_1 \cdot b^1 + a_2 \cdot b^2 + \cdots + b^{m-1} \cdot b_{m-1} + a_m \cdot b^m$$

Ou, finalmente:

$$n = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0 \cdot b^0$$

Assim, dado inteiro qualquer $b \geq 2$, todo inteiro positivo n pode ser representado por um polinômio inteiro em b do grau m (porque $a_m \neq 0$), ordenado segundo as potências descrecentes de b e cujo os coeficiente a_i são inteiros que satisfazem às seguintes condições:

$$0 \leq a_i < b \quad (i = 0,1,2,3, \ldots, m), \text{ sendo } a_m \neq 0$$

Este polinômio representa-se, de modo abreviado, pela notação $n = (a_m \cdot a_{m-1} \cdot \ldots \cdot a_2 \cdot a_1 \cdot a_0)$ em que os coeficientes a_i são indicados ordem respectiva, figurando o inteiro b como índice. A unicidade dessa representação é uma consequência imediata do Teorema 1.6.

O inteiro b chama-se *base* e é costume dizer que n está escrito no sistema de base b.

Exemplo 1.32 $105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ *ou sob forma abreviada* $105 = (1101001)_2$.

Por outro lado, tem-se $(1101001)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 39$.

Exemplo 1.33 *Escrever 34789 no sistema de base 7. Sucessivamente, pelo algoritmo da divisão, tem-se*

$$34789 = 4969 \cdot 7 + 6$$
$$4969 = 709 \cdot 7 + 6$$
$$709 = 101 \cdot 7 + 2$$
$$101 = 14 \cdot 7 + 3$$
$$14 = 2 \cdot 7 + 0$$
$$2 = 0 \cdot 7 + 2.$$

Logo, $34789 = 2 + 7^5 + 0 \cdot 7^4 + 3 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7^1 + 6 \cdot 7^0 = (203266)_7$.

Exemplo 1.34 $103057 = 1 \cdot 10^5 + 0 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0 = (103057)_{10}$

CAPÍTULO 2

CONGRUÊNCIAS

A maioria das propriedades da Congruência Modular apresentadas neste capítulo foi introduzida no século XIX por Carl Friedrich Gauss (1777- 1855) em seu livro *Disquisitiones Arithmeticae*[4]*,* um dos livros mais importantes da história sobre a Teoria dos Números escrita de forma metódica e lógica. A publicação dessa obra contribuiu para manipulação e o rápido desenvolvimento das relações de Divisibilidade com a utilização da notação (mod) criada por Gauss.

Gauss percebeu que dois inteiros a e b são congruentes módulo m, se m é um inteiro positivo que divide $\boldsymbol{a-b}$**,** dessa forma, ele escreveu $a \equiv b\ (mod\ m)$ em que ≡ é o símbolo de equivalência. E nos anos seguintes, no Brasil, alguns autores se destacam com seus livros sobre o referente tema, dentre eles o Edgard de Alencar Filho em Teoria Elementar dos Números no qual aborda a Congruência de maneira coerente e organizada em uma sistematização lógica de conceitos.

A seguir serão apresentados os resultados das Congruências considerados importantes para o desenvolvimento deste Trabalho[5].

Definição 2.1 (Congruência*) Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se, e somente se, m divide $a - b$.*

Em outros termos, a é congruente a b módulo m se, e somente se, existe um inteiro k tal que $a - b = k \cdot m$.

Com a notação $a \equiv b\ (mod\ m)$ indica-se que a é congruente a b módulo m. Portanto, simbolicamente: $a \equiv b\ (mod\ m) \leftrightarrow m|(a-b)$*, ou seja,* $a \equiv b\ (mod\ m) \leftrightarrow \exists k \in Z\ /\ a - b = k \cdot m.$ E se m não divide a diferença a – b, então diz-se que a é incongruente a b módulo m, o que se indica pela notação: $a \equiv\ b\ (mod\ m)$.

Exemplo 2.1

$10 \equiv 24\ (mod\ 2)$*, porque* $2|(10-24)$

$34 \equiv 10\ (mod\ 6)$*, porque* $6|(34-10)$

---

[4] Livro-texto sobre teoria dos números escrito em latim por Carl Friedrich Gauss e publicado primeira vez em 1801 (ROSEN, 2011).

[5] As definições, corolários e os teoremas sobre Congruência Modular destacadas neste capítulo se baseiam em (FILHO, 1981) e o Exemplo 2.2 foi retirado do livro *Modern Algebra: An Introduction* de (DURBIN, 2008).

$-56 \equiv -24\ (mod\ 8)$, *porque* $8|[-56-(-24)]$

$24 \not\equiv 5\ (mod\ 3)$, *porque* $3 \nmid (24-5)$

$-38 \not\equiv 12\ (mod\ 5)$, *porque* $5 \nmid (-38-12)$

Exemplo 2.2 *Qual valor de* n *que satisfaz* $25 \equiv 4\ (mod\ n)$?

$n \mid (25-4) = n \mid 21$ *e um número que é divisível por 21 é 7 ou 3. Logo,* $n = 7\ ou\ 3$, uma vez que $n > 0$.

Exemplo 2.3 *Mostrar* $n^2 \equiv 0\ (mod\ 6)$ *ou* $n^2 \equiv 1(mod\ 6)$, $\forall\ n \in Z$

Com efeito

I. n *par:* $n = 6 \cdot k \rightarrow n^2 = 36 \cdot k^2 \rightarrow 6|n^2 = 6|n^2 - 0 \rightarrow n^2 \equiv 0\ (mod\ 6)$.

II. n *ímpar:* $n = 6 \cdot k + 1 \rightarrow n^2 = 6 \cdot (6 \cdot k^2 + 2 \cdot k) + 1 \rightarrow\ n^2 - 1 = 6 \cdot (6 \cdot k^2 + 2 \cdot k)\ \rightarrow 6|(n^2 - 1) \rightarrow n^2 \equiv 1\ (mod\ 6)$.

Teorema 2.1 (Caracterização de Inteiros Congruentes). *Dois inteiros* a *e* b *são congruentes módulo* m *se, e somente se,* a *e* b *deixam o mesmo resto quando divididos por* m.

Demonstração.

(→) *Suponha-se que* $a \equiv b$ *(mod m). Então, por definição* $a - b = k.m$, *com* $k \in Z$. *Seja r o resto da divisão de* b *por* m; *então, pelo algorítmo da divisão* $b = m.q + r$, *o qual* $0 \neq r < m$.

Portanto, $a = k.m + b = k.m + m.q + r = (k+q)m + r$ *e isso significa que* r *é o resto da divisão de* a *por* m, *isto é, os inteiros* a *e* b *divididos por* m *deixam o mesmo resto* r.

(←) *Reciprocamente, suponhamos que* a *e* b *divididos por* m *deixam o mesmo resto* r. *Então, podemos escrever*

$$a = m.q_1 + r \text{ e } b = m.q_2, \text{ o qual } 0 \neq r < m$$

e, portanto, $a - b = (q_1 - q_2) \cdot m \rightarrow m|(a-b) \rightarrow a \equiv b$ *(mod m).*

Exemplo 2.4 *Sejam os inteiros* 10 *e* 24, *pelo algoritmo da divisão,* $10 = 2 \cdot (5) + 0$ *e* $24 = 2 \cdot (12) + 0$, *isto é,* 10 *e* 24 *divididos por 2 deixam o mesmo resto 0. Logo, pelo teorema anterior:* $10 \equiv 24$ *(mod 2).*

Agora, dois inteiros que deixam o mesmo resto quando divididos por 6 são 34 *e* 10. *Tem-se a congruência:*

$$34 \equiv 10\ (mod\ 6)$$

de modo que, pelo teorema anterior, 34 *e* 10 *divididos por* 6 *deixam o mesmo resto 4:* $34 = 6 \cdot (5) + 4$ *e* $10 = 6 \cdot (0) + 4$.

Teorema 2.2 (Propriedades das Congruências) *Seja* m *um inteiro positivo fixo (*$m > 0$*) e sejam* a, b *e* c *inteiros quaisquer. Subsistem as seguintes propriedades:*

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 se* $b \equiv c\ (mod\ m)$*, então* $a \equiv c\ (mod\ m)$.

Demonstração.

I. Com efeito: $\mathrm{m} \mid 0$ ou $\mathrm{m} \mid (\mathrm{a} - \mathrm{a}) \rightarrow \mathrm{a} \equiv \mathrm{a}\ (mod\ m)$

II. Com efeito, se $\mathrm{a} \equiv \mathrm{b}\ (mod\ m)$, então $\mathrm{a} - \mathrm{b} = \mathrm{k} \cdot \mathrm{m}$, com $\mathrm{k} \in \mathrm{Z}$. Portanto, $\mathrm{b} - \mathrm{a} = -(\mathrm{k} \cdot \mathrm{m}) = (-\mathrm{k}) \cdot \mathrm{m} \rightarrow \mathrm{b} \equiv \mathrm{a}\ (mod\ m)$

III. Com efeito, se $\mathrm{a} \equiv \mathrm{b}\ (mod\ m)$ e se $\mathrm{b} \equiv \mathrm{c}\ (mod\ m)$, então existem inteiros h e k tais que $\mathrm{a} - \mathrm{b} = \mathrm{h} \cdot \mathrm{m}$ e $\mathrm{b} - \mathrm{c} = \mathrm{k} \cdot \mathrm{m}$. Portanto: $\mathrm{a} - \mathrm{c} = (\mathrm{a} - \mathrm{b}) + (\mathrm{b} - \mathrm{c}) = \mathrm{h} \cdot \mathrm{m} + \mathrm{k} \cdot \mathrm{m} = (\mathrm{h} + \mathrm{k}) \cdot \mathrm{m}$ e isto significa que $\mathrm{a} \equiv \mathrm{c}$ (mod m).

E, consoante este teorema, a relação R *no conjunto* Z *dos inteiros definida por* $aRb \leftrightarrow a \equiv b$ *(mod m) é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em Z. Esta relação de equivalência R em Z é denominada "congruência módulo* m*".*

Teorema 2.3 *Seja* m *um inteiro positivo fixo (*$m > 0$*) e sejam* a *e* b *dois inteiros quaisquer. Subsistem as seguintes propriedades:*

I. Se $a \equiv b\ (mod\ m)$ *e se* $n|m$*, com* $n > 0$*, então* $a \equiv b\ (mod\ n)$.

II. Se $a \equiv b\ (mod\ m)$ *e se* $c > 0$*, então* $a \cdot c \equiv b \cdot c\ (mod\ m \cdot c)$

III. Se $a \equiv b$ *(mod m) e se* a*,* b *e* m *são todos divisíveis pelo inteiro* $d > 0$*, então* $\frac{a}{d} \equiv \frac{b}{d}\ (mod\ \frac{m}{d})$.

Demonstração.

I. Com efeito: $a \equiv b\ (mod\ m) \rightarrow a - b = k \cdot m$ e $n|m \rightarrow m = n \cdot q$ o qual k e $\mathrm{q} > 0$ são inteiros. Portanto: $a - b = (k \cdot q) \cdot n \rightarrow a \equiv b\ (mod\ n)$.

II. Com efeito: $a \equiv b\ (mod\ m) \rightarrow a - b = k \cdot m \rightarrow a \cdot c - b \cdot c = k \cdot (m \cdot c) \rightarrow a \cdot c \equiv b \cdot c\ (mod\ m \cdot c)$.

III. Com efeito: $a \equiv b\ (mod\ m) \rightarrow a - b = k \cdot m \rightarrow \frac{a}{d} - \frac{b}{d} = k \cdot (\frac{m}{d}) \rightarrow \frac{a}{d} \equiv \frac{b}{d}\ (mod\ \frac{m}{d})$.

Exemplo 2.5

$-56 \equiv -24\ (\mathrm{mod}\ 8)$, ou seja, -56 e -24 deixam o mesmo resto quando divididos por 8, assim como $-56 \equiv -24\ (\mathrm{mod}\ 4)$.

$34 \equiv 10\ (\mathrm{mod}\ 6)$ e ao multiplicar $k = 5$ em ambos os lados da Congruência $\rightarrow 68 \equiv 20\ (\mathrm{mod}\ 12)$.

$16 \equiv -32\ (\mathrm{mod}\ 16)$ e ao dividir $q = 4$ em ambos os lados da Congruência $\rightarrow 4 \equiv -8\ (\mathrm{mod}\ 4)$.

Teorema 2.4 *Seja m um inteiro positivo fixo ($m > 0$) e sejam a, b, c e d inteiros quaisquer. Subsistem as seguintes propriedades:*

I. Se $a \equiv b\ (mod\ m)$ e se $c \equiv d\ (mod\ m)$, então $a + c \equiv b + d\ (mod\ m)$ e $a \cdot c \equiv b \cdot d\ (mod\ m)$

II. Se $a \equiv b\ (mod\ m)$, então $a + c \equiv b + c\ (mod\ m)$ e $a \cdot c \equiv b \cdot c\ (mod\ m)$

III. Se $a \equiv b\ (mod\ m)$, então $a^n \equiv b^n (mod\ m)$ para todo inteiro positivo n.

Demonstração.

I. Com efeito, se $a \equiv b\ (mod\ m)$ e se $c \equiv d\ (mod\ m)$, então existem inteiros h e k tais que $a - b = h \cdot m$ e $c - d = k \cdot m$. Portanto:

$$(a + c) - (b + d) = (a - b) + (c - d) = h \cdot m + k \cdot m = (h + k) \cdot m$$

e $(a \cdot c) - (b \cdot d) = (b + h \cdot m) + (d + k \cdot m) - b \cdot d = (b \cdot k + d \cdot h + h \cdot k \cdot m) \cdot m$

o que implica:

$$(a + c) \equiv b + d\ (\mathrm{mod\ m}) \text{ e } a \cdot c \equiv b \cdot d\ (\mathrm{mod\ m})$$

II. Com efeito, se $a \equiv b\ (\mathrm{mod\ m})$, como $c \equiv c\ (\mathrm{mod\ m})$, tem-se, pela propriedade anterior: $a + c \equiv b + c\ (\mathrm{mod\ m})$ e $a \cdot c \equiv b \cdot c\ (\mathrm{mod\ m})$

III. Usando o "Segundo princípio da Indução Finita", a proposição é verdadeira para $n = 1$, e suposta verdadeira para um inteiro positivo k, temos: $a^k \equiv b^k\ (\mathrm{mod\ m})$ e $a \equiv b\ (\mathrm{mod\ m})$.

Portanto, pela propriedade (I), $a^k . a \equiv b^k . b\ (\mathrm{mod\ m})$ ou $a^{k+1} \equiv b^{k+1}\ (\mathrm{mod\ m})$, isto é, a proposição é verdadeira para o inteiro positivo $k + 1$. Logo, proposição é verdadeira para todo inteiro positivo m.

Exemplo 2.6

I. $44 \equiv 17\ (mod\ 9)$ *e* $27 \equiv 9\ (mod\ 5)$ *implica:* $44 + 27 \equiv 17 + 9\ (mod\ 9)$ *ou* $71 \equiv 26\ (mod\ 9)$ *e* $44 \cdot 27 \equiv 17 \cdot 9\ (mod\ 9)$ *ou* $1188 \equiv 153\ (mod\ 9)$.

II. $52 \equiv 28\ (mod\ 8)$ *implica:* $52 + 3 \equiv 28 + 3\ (mod\ 8)$ *ou* $55 \equiv 31\ (mod\ 8)$ *e* $52 \cdot (5) \equiv 28 \cdot (5)\ (mod\ 8)$ *ou* $126 \equiv 140\ (mod\ 8)$

III. $48 \equiv 8\ (mod\ 8)$ *implica:* $(48)^2 \equiv 8^2\ (mod\ 8)$ *ou* $2304 \equiv 64\ (mod\ 8)$.

Teorema 2.5 *Se* $a \cdot c \equiv b \cdot c\ (mod\ m)$ *e se o* $mdc(c, m) = d$*, então* $a \equiv b\ (mod\ \frac{m}{d})$.

Demonstração. Com efeito, se $\mathrm{a} \cdot \mathrm{c} \equiv \mathrm{b} \cdot \mathrm{c}\ (\mathrm{mod}\ \mathrm{m})$, então, $\mathrm{a} \cdot \mathrm{c} - \mathrm{b} \cdot \mathrm{c} = (\mathrm{a} - \mathrm{b}) \cdot \mathrm{c} = \mathrm{k} \cdot \mathrm{m}$, com $\mathrm{k} \in \mathrm{Z}$. E se o $\mathrm{mdc}(\mathrm{c}, \mathrm{m}) = \mathrm{d}$, existem inteiros r e s tais que $\mathrm{c} = \mathrm{d} \cdot \mathrm{r}$ e $\mathrm{m} = \mathrm{d} \cdot \mathrm{s}$, em que r e s são primos entre si.

Portanto: $(\mathrm{a} - \mathrm{b}) \cdot \mathrm{d} \cdot \mathrm{r} = \mathrm{k} \cdot \mathrm{d} \cdot \mathrm{r}$ ou $(\mathrm{a} - \mathrm{b}) \cdot \mathrm{r} = \mathrm{k} \cdot \mathrm{s}$ o que implica que $\mathrm{s} | (\mathrm{a} - \mathrm{b}) \cdot \mathrm{r}$, com o $\mathrm{mdc}(\mathrm{r}, \mathrm{s}) = 1$. Logo, pelo Teorema 3.4 (De Euclides) $\mathrm{s} | (\mathrm{a} - \mathrm{b})$ e $\mathrm{a} \equiv \mathrm{b}\ (mod\ s)$ ou, por ser $\mathrm{s} = \frac{\mathrm{m}}{\mathrm{d}}$, $\mathrm{a} \equiv \mathrm{b}\ (\mathrm{mod}\ \frac{\mathrm{m}}{\mathrm{d}})$.

Corolário 2.1 *Se* $a \cdot c \equiv b \cdot c\ (mod\ m)$ *e se* $mdc(c, m) = 1$*, então* $a \equiv b\ (mod\ m)$*. Esta propriedade mostra que é permitido dividir os fatores de ambos de uma congruência que são primos com módulo por c.*

Corolário 2.2 *Se* $a.c \equiv b.c\ (mod\ p)$ *, com* p *primo, e se* p *não divide* c $(p \nmid c)$*, então* $a \equiv b\ (mod\ p)$.

Demonstração. Com efeito, as condições: p não divide c $(p \nmid c)$ e p é primo, implicam que o $mdc(c, p) = 1$.

Exemplo 2.7 [6]*Considera-se a congruência* $52 \equiv 28\ (mod\ 8)$ *ou* $4 \cdot 13 \equiv 4 \cdot 7\ (mod\ 8)$*. Como o* $mdc(4, 8) = 4$*, pelo Teorema 2.5, tem-se* $13 \equiv 7\ (mod\ 2)$.

Definição 2.2 (Sistemas Completos de Restos) *Chama-se sistemas sompletos de restos módulo* m *todo conjunto* $S = \{r_1, r_2, \dots, r_m\}$ *de* m *inteiros tal que um inteiro qualquer* a *é congruente módulo* m *a um único elemento de* S.

Exemplo 2.8 *Cada um dos conjuntos:* $\{1, 2, 3\}, \{0, 1, 2\}, \{-1, 0, 1\}, \{1, 5, 9\}$ *é um sistema completo de restos módulo 3.*

Teorema 2.6 *O conjunto* $S = \{0, 1, 2, \dots, m - 1\}$ *é um sistema completo completo de restos módulo m.*

Demonstração. Seja a um inteiro qualquer e sejam q e r o quociente e o resto na divisão de a pelo inteiro positivo m, isto é, $a = m \cdot q + r$ em que $0 \leq r < m$.

[6] Os exemplos 2.7; 2.8; 2.9; 2.10 são de (FILHO, 1981).

Então, pela definição de inteiros congruentes módulo m, tem-se $a \equiv r\ (mod\ m)$. E como r só pode assumir os valores $0, 1, 2, \dots, m-1$, segue-se que o inteiro a é congruente módulo m a um único elemento do conjunto S, e por conseguinte este conjunto é um sistema completo de resto módulo m.

Exemplo 2.9 *O conjunto $S = \{0, 1, 2, 3, 4\}$ é um sistema completo de restos módulo 5.*

Corolário 2.3 *Se $S = \{r_1,\ r_1, \dots, r_m\}$ é um sistema completo de restos módulo m, então os elementos de S são congruentes módulo m aos inteiros $0, 1, 2, \dots, m-1$, tomados em um certa ordem.*

Demonstração. Com efeito, qualquer que seja o inteiro a, tem-se

$$a \equiv r_1\ (mod\ m), \text{ com } r_1 \epsilon\ S$$

$$a \equiv k\ (mod\ m), \text{ com } 0 \leq k \leq m-1$$

Logo, pela propriedade transitiva da "Congruência Módulo m", tem-se $r_1 \equiv k\ (mod\ m)$.

Exemplo 2.10 *O conjunto $S = \{-12, -4, 11, 13, 22, 82, 91\}$ é um sistema completo de restos módulo 7, e tem-se*

$$-12 \equiv 2\ (mod\ 7), -4 \equiv 3\ (mod\ 7), 11 \equiv 4\ (mod\ 7)$$

$$13 \equiv 6\ (mod\ 7), 22 \equiv 1\ (mod\ 7), 82 \equiv 5\ (mod\ 7)$$

$$91 \equiv 0\ (mod\ 7)$$

Isto é, os elementos de S são congruentes módulo 7 aos inteiros 2, 3, 4 ,6, 1, 5, 0.

CAPITULO 3

3.1 CRITÉRIOS DE DIVISIBILIDADE

O estudo das Congruências proporcionou a demonstração dos Critérios de Divisibilidade do número 2 ao 11. Esses Critérios são regras que servem para identificar, de antemão, se um número é divisível por outro número inteiro, ou seja, se a divisão é exata.

De acordo com McDowell (2018)[7] essas regras de divisibilidade datam a $500\ a.C.$ e muitos matemáticos, como Blaise Pascal e Joseph-Louis Lagrange, contribuíram aperfeiçoando-os no decorrer da história. A seguir serão apresentados os Critérios de Divisibilidade[8] que foram analisados para demonstrá-los utilizando Congruências.

- Critério de Divisibilidade por 2

Um número N é divisível por 2 quando o último algarismo desse número for par"

- Critério de Divisibilidade por 3

Um número N é divisível por 3 se, e somente se, a soma de seus dígitos é divisível por 3

- Critério de Divisibilidade por 4

Um número N é divisível por 4 quando seus dois últimos algarismos são divisíveis por 4

- Critério de Divisibilidade por 5

Um número N é divisível por 5 se, e somente se, o seu último algarismo é 0 ou 5

- Critério de Divisibilidade por 6

Um número N é divisível por 6 se, e somente, se é divisível por 2 e 3

---

[7] Eric L. McDowell (Berry College) em Divisibility Tests: A History and User's Guide apresenta suas pesquisas sobre Critérios de Divisibilidade mais recentes.

[8] Os Critérios de Divisibilidade por 3, 4, 7, 9 e 11 tem como base (SANTOS, 1998); os de 6, 8 e 10 estão conforme (MACHADO; IEZZI; DOLCE, 2018) e o 2 e 5 estão de acordo com (DOMINGUES; IEZZI, 2003).

- Critério de Divisibilidade por 7

Para identificar se um número N é divisível por 7 é necessário seguir o seguinte passo a passo:

Passo 1: Separar o dígito das unidades dos restantes do número N;

Passo 2: Subtrair o restante do número N pelo dobro do dígito das unidades;

Passo 3: Se o resultado da subtração for divisível por 7 então o número N é divisível por 7, caso resultado ainda for um número grande retorne para o passo 1 até obter um número pequeno o suficiente para efetuar a divisão.

Salienta-se que este Critério de Divisibilidade é mais complexo do que os demais em virtude de não haver uma regra geral para o número 7, tal como considera Rodrigues (2013). É um critério em desenvolvimento e assim sendo, um exemplo é o caso do estudante nigeriano Chika Ofili por ganhar o prêmio Trulittle Leadership Hero de 2019 por ter elaborado o mais novo Critério de Divisibilidade por 7 que consiste em multiplicar por 5 o último algarismo do número N e somar o produto pelo restante N, se o resultado for divisível por 7 conclui-se que o número original é divisível por 7.

Logo, percebe-se que não há exatamente uma “regra” e sim várias possibilidades de identificação se um número inteiro é divisível por 7.

- Critério de Divisibilidade por 8

O número N é divisível por 8 se, e somente se, os seus três últimos algarismos são divisíveis por 8

- Critério de Divisibilidade por 9

Um número é divisível por 9 se, e somente se, a soma de seus dígitos é divisível por 9

- Critério de Divisibilidade por 10

O número N é divisível por 10 quando seu último algarismo termina em 0

- Critério de Divisibilidade por 11

Um número é divisível por 11 se a soma dos algarismos de ordem par menos a soma dos algarismos de ordem ímpar é um número divisível por 11.

3.2 DEMONSTRAÇÃO DOS CRITÉRIOS DE DIVISIBILIDADE UTILIZANDO CONGRUÊNCIAS

3.2.1 Critério de Divisibilidade por 2

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$. Assim sendo, tem-se que N é divisível por 2 ($2 \mid N$) se, e somente se, a_0 é divisível por 2 ($2 \mid a_0$), ou seja, a_0 é par".

Demonstração: É verdadeiro que $10 \equiv 0\ (mod\ 2)$.

Pela propriedade 3 do Teorema 2.4

$$\mathbf{10^1 \equiv 0\ (mod\ 2)}$$

$$\mathbf{10^2 \equiv 0\ (mod\ 2).}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{10^k \equiv 0\ (mod\ 2);\ k \geq 1}$$

E segundo a propriedade 2 do Teorema 2.4, a multiplicação por $a_m\ \forall\ m = 1, 2, 3, \ldots, k$.

$$\mathbf{a_1 \cdot 10^1 \equiv 0\ (mod\ 2)}$$

$$\mathbf{a_2 \cdot 10^2 \equiv 0\ (mod\ 2).}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{a_k \cdot 10^k \equiv 0\ (mod\ 2)}$$

Soma-se as congruências, conforme a propriedade 1 do Teorema 2.4, segue que $\mathbf{a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 \equiv 0\ (mod\ 2)}$. O lado esquerdo da Congruência está formando o número N na base decimal e, para completa-lo, adiciona-se o escalar $a_0 \cdot 10^0$ conforme a propriedade 2 do Teorema 2.4

$$\boldsymbol{a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0 \cdot 10^0 \ (mod\ 2).}$$

Portando, por Congruências, N e a_0 possuem o mesmo resto quando divididos por 2. Como resultado, N é divisível por 2 se, e somente se,

a_0 também for divisível por 2. E isso sucede se a_0 é par.

Exemplo 3.2.1 *53658 é divisível por 2, pois o último dígito 8 é divisível por 2.*

3.2.2 Critério de Divisibilidade por 3

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja S a soma dos algarismos N:

$$S = a_k \cdot 1 + \ldots + a_3 \cdot 1 + a_2 \cdot 1 + a_1 \cdot 1 + a_0$$

Assim sendo, tem-se que N é divisível por 3 $(3 \mid N)$ se, e somente se, S é divisível por 3 $(3 \mid S)$".

Demonstração: Como $10 \equiv 1\ (mod\ 3)$, ao aplicar a propriedade 3 do Teorema 2.4 a essa Congruência

$$\boldsymbol{10^1 \equiv 1 (mod\ 3)}$$
$$\boldsymbol{10^2 \equiv 1 (mod\ 3)}$$
$$\boldsymbol{10^3 \equiv 1 (mod\ 3)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{10^k \equiv 1 (mod\ 3)\ \forall\ k \geq 1.}$$

E multiplicando $a_m \forall\ m = 1, 2, 3, \ldots, k$, seguindo a propriedade 2 do Teorema 2.4

$$\boldsymbol{a_1 \cdot 10^1 \equiv a_1 \cdot 1 (mod\ 3)}$$
$$\boldsymbol{a_2 \cdot 10^{\,2} \equiv a_2 \cdot 1 (mod\ 3)}$$
$$\boldsymbol{a_3 \cdot 10^3 \equiv a_3 \cdot 1 (mod\ 3)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{a_k \cdot 10^k \equiv a_k \cdot 1 (mod\ 3).}$$

Ao somar essas Congruências, aplicando a propriedade 1 do Teorema 2.4, obtém-se a Congruência

$\boldsymbol{a_k \cdot 10^k + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 \equiv a_k \cdot 1 + \ldots + a_3 \cdot 1 + a_2 \cdot 1 + a_1 \cdot}$

$\mathbf{1}(\boldsymbol{mod}\ \mathbf{3})$**.** Por fim, soma-se o escalar $a_0 \cdot 10^0$ em ambos os lados da Congruência para completar a representação do N na base decimal:

$$\boldsymbol{a_k \cdot 10^k} + \ldots + \boldsymbol{a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_k \cdot 1} + \ldots + \boldsymbol{a_3 \cdot 1 + a_2 \cdot 1 + a_1 \cdot 1 + a_0 \cdot 10^0 (mod\ 3).}$$

Portanto, por Congruências, N e $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ possuem o mesmo resto quando dividido por três. Como resultado, N é divisível por 3 se, e somente se, a soma dos algarismos de N é divisível por 3.

Exemplo 3.2.2 474831 *é divisível por* 3 *pois* $4 + 7 + 4 + 8 + 3 + 1 = 27$ *e* 27 *é divisível por* 3*.*

3.2.3 Critério de Divisibilidade por 4

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja S a soma dos dois últimos algarismos de N:

$$S = a_1 \cdot 10^1 + a_0$$

Assim sendo, N é divisível por 4 ($4 \mid N$) se, e somente se, S é divisível por 4 ($4 \mid S$)".

Demonstração: É verdadeiro que $10 \equiv 2\ (mod\ 4)$, da mesma maneira que $10^2 \equiv 0\ (mod\ 4)$ também o é. Portanto, tem-se:

$$\boldsymbol{10^2 \equiv 0 (mod\ 4)}$$
$$\boldsymbol{10^3 \equiv 0 (mod\ 4)}$$
$$\vdots$$
$$\boldsymbol{10^k \equiv 0 (mod\ 4)\ \forall\ k \geq 2}$$

Posteriormente é multiplicado em cada Congruência o termo $a_m\ \forall\ m = 2, 3,\ 4, 5, \ldots, k$ e somado as Congruências de acordo com a propriedade 2 e 1 do Teorema 2.4, respectivamente. E adiciona-se também ao resultado os termos $a_0 \cdot 10^0$ e $a_1 \cdot 10^1$, pela propriedade 1 do Teorema citado anteriormente, que sucede em

$$\boldsymbol{a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0} \equiv \boldsymbol{a_1 \cdot 10^1 + a_0 \cdot 10^0\ (mod\ 7)}$$

Deste modo, por Congruência, N e $a_1 \cdot 10^1 + a_0$ possuem o mesmo resto quando divididos por 4. Em consequência, N é divisível por 4 se, e somente se, o $a_1 \cdot 10^1 + a_0$ também for divisível.

Exemplo 3.2.3 562824 *é divisível por* 4 *pois os dois últimos algarismos são divisíveis por* 4 $(4|24)$.

3.2.4 Critério de Divisibilidade por 5

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$. Assim sendo, N é divisível por 5 $(5 \mid N)$ se, e somente se, $a_0 = 0$ ou $a_0 = 5$".

Demonstração: Como $10 \equiv 0\ (mod\ 5)$, aplica-se a propriedade 3 do Teorema 2.4:

$$\mathbf{10} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\mathbf{10^2} \equiv \mathbf{0^2}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\mathbf{10^3} \equiv \mathbf{0^2}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\vdots$$
$$\mathbf{10^k} \equiv \mathbf{0^2}\ (\boldsymbol{mod}\ \mathbf{5})\ \forall\ k \geq 1$$

E multiplica-se $a_m\ \forall\ m = 1, 2, 3, \ldots, k$ conforme a propriedade 2 do Teorema 2.4

$$\boldsymbol{a_1} \cdot \mathbf{10} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\boldsymbol{a_2} \cdot \mathbf{10^2} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\boldsymbol{a_3} \cdot \mathbf{10^3} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$
$$\vdots$$
$$\boldsymbol{a_k} \cdot \mathbf{10^k} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$

Pela propriedade 1 do Teorema 2.4, a soma das Congruências será

$$\boldsymbol{a_k} \cdot \mathbf{10^k} + \ldots + \boldsymbol{a_3} \cdot \mathbf{10^3} + \boldsymbol{a_2} \cdot \mathbf{10^2} + \boldsymbol{a_1} \cdot \mathbf{10} \equiv \mathbf{0}\ (\boldsymbol{mod}\ \mathbf{5})$$

Por último, ao somar o escalar $a_0 \cdot 10^0$ na Congruência ficará igual a $a_k \cdot 10^k + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \cdot 10^0 \equiv a_0 \cdot 10^0\ (mod\ 5)$. Nota-se que o termo esquerdo é semelhante ao número N na potência de base 10, logo, conclui-se que N e a_0 possuem o mesmo resto quando divididos por 5. À vista disso, N é divisível por 5 se, e somente se, $a_0 = 0$ ou $a_0 = 5$.

Exemplo 3.2.4 29370 *é divisível por* 5 *pois o número termina em* 0*. Assim como* 837835 *também é divisível por* 5 *pois o último algarismo termina em* 5*.*

3.2.5 Critério de Divisibilidade por 6

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$. Assim sendo, N é divisível por 6 $(6 \mid N)$ se, e somente se, N for divisível por 2 $(2 \mid N)$ e 3 $(3 \mid N)$".

Demonstração: De acordo com o Corolário 1.4 se $2 \mid N$ e $3 \mid N$ e se o $mdc\ (2,3) = 1$, então $2 \cdot 3 = 6 \mid N$. Portanto, para um número ser divisível por 6 é necessário que ele seja divisível por 2 e 3.

Exemplo 3.2.5 53412 *é divisível por* 6 *pois é divisível por* 2 *e* 3 *simultaneamente.*

3.2.6 Critério de Divisibilidade por 7

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja D a subtração do número N sem a_0 pelo produto de 2 e a_0 :

$$D = (a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1) - 2 \cdot a_0$$

Assim sendo, N é divisível por 7 $(7 \mid N)$ se, e somente se, D for divisível por 7 $(7 \mid N)$".

Demonstração:

Considera-se o N na forma $10 \cdot (a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1 \cdot 10^0) + a_0$. Aplicando a propriedade 2 do Teorema 2.4, soma-se o escalar $(-20 \cdot a_0)$ pelos algarismos em parênteses e soma-se $20 \cdot a_0$ por a_0.

$$N = 10 \cdot (a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1 \cdot 10^0) + a_0 =$$

$$10 \cdot (a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1 \cdot 10^0 - \mathbf{20 \cdot a_0}) + a_0 + \mathbf{20 \cdot a_0} =$$

$$10 \cdot (a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1 \cdot 10^0 - 2 \cdot a_0) + 21 \cdot a_0 =$$

Seja $N_1 = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_1 \cdot 10^0$, então, $N = 10 \cdot (N_1 - 2 \cdot a_0) + 21 \cdot a_0$. Ou seja, $\boldsymbol{N \equiv 10 \cdot (N_1 - 2 \cdot a_0)\ (mod\ 7)}$**.** Por Congruência, para N ser divisível por 7, $(N_1 - 2 \cdot a_0)$ deve ser divisível por 7.

Exemplo 3.2.6 1176 *é divisível por* 7*, pois, se separarmos* 117 *e* 6*, multiplicar* 6 *por* 2*, subtrair o* 12 *por* 117*, o resultado é* 105*.* 105 *é divisível por* 7*.*

3.2.7 Critério de Divisibilidade 8

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja S a soma dos três algarismos de N:

$$S = a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$$

Assim sendo, N é divisível por 8 $(8 \mid N)$ se, e somente se, S for divisível por 8 $(8 \mid S)$.".

Demonstração: Observe que $10 \equiv 2\ (mod\ 8)$ e seguindo a propriedade 3 do Teorema 2.4 $10^2 \equiv 2^2\ (mod\ 8)$ também possui resto *4*. Já o $10^3 \equiv 0\ (mod\ 8)$ dispõe de resto 0, isto posto:

$$\mathbf{10^3 \equiv 0\ (mod\ 8)}$$
$$\mathbf{10^4 \equiv 0\ (mod\ 8)}$$
$$\mathbf{10^5 \equiv\ 0\ (mod\ 8)}$$
$$\mathbf{.}$$
$$\mathbf{.}$$
$$\mathbf{.}$$
$$\mathbf{10^k \equiv 0\ (mod\ 8) \forall\ k \geq 3}$$

Na sequência multiplica-se em cada Congruência o termo $a_m\ \forall\ m = 3,\ 4, 5, \dots, k$

$$\mathbf{a_3\ \cdot 10^3 \equiv 0\ (mod\ 8)}$$
$$\mathbf{a_4 \cdot 10^4 \equiv 0\ (mod\ 8)}$$
$$\mathbf{a_5 \cdot 10^5 \equiv\ 0\ (mod\ 8)}$$
$$\mathbf{.}$$
$$\mathbf{.}$$
$$\mathbf{.}$$
$$\mathbf{a_k \cdot 10^k \equiv 0\ (mod\ 8) \forall\ k \geq 3}$$

Executando a propriedade 3 do Teorema 2.4 é inserindo os termos $a_2 \cdot 10^2$, $a_1 \cdot 10^1$ e $a_0 \cdot 10^0$ em $\mathbf{a_k \cdot 10^k + \cdots + a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3\ \cdot 10^3 \equiv 0\ (mod\ 8)}$, a soma das Congruências.

$$\mathbf{a_k \cdot 10^k + \cdots + a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3\ \cdot 10^3}$$
$$\mathbf{\equiv a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0\ (mod\ 8)}$$

Por Congruência, N e $a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$ possuem o mesmo resto quando divididos por 8. Em vista disso, N é divisível por 8 se, e somente se, o $a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$ também for divisível por 8.

Exemplo 3.2.7 935576 *é divisível por* 8 *pois os três últimos algarismos* 576 *é divisível por* 8.

3.2.8 Critério de Divisibilidade por 9

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja S a soma dos três algarismos de N:

$$S = a_k \cdot 1^k + \cdots + a_3 \cdot 1^3 + a_2 \cdot 1^2 + a_1 \cdot 1 + a_0$$

Assim sendo, N é divisível por 9 $(9 \mid N)$ se, e somente se, S for divisível por 9 $(9 \mid S)$".

Demonstração: Essa demonstração é análoga ao Critério de Divisibilidade por 3. Dado que $10 \equiv 1\ (mod\ 9)$, segundo a propriedade 3 do Teorema 2.4

$$\boldsymbol{10 \equiv 1\ (mod\ 9)}$$
$$\boldsymbol{10^2 \equiv 1^2\ (mod\ 9)}$$
$$\boldsymbol{10^3 \equiv 1^3\ (mod\ 9)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{10^k \equiv 1^k\ (mod\ 9)\ \forall\ k \geq 1}$$

Efetua-se a propriedade 2 do Teorema 2.4

$$\boldsymbol{a_1 \cdot 10^1 \equiv a_1 \cdot 1\ (mod\ 9)}$$
$$\boldsymbol{a_2 \cdot 10^2 \equiv a_2 \cdot 1^2\ (mod\ 9)}$$
$$\boldsymbol{a_3 \cdot 10^3 \equiv a_3 \cdot 1^3\ (mod\ 9)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{a_k \cdot 10^k \equiv a_k \cdot 1^k\ (mod\ 9)\ ;\ a_m\ \forall\ m = 1, 2, 3, \ldots, k}$$

O somatório das Congruências é

$$\boldsymbol{a_k \cdot 10^k + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1}$$
$$\boldsymbol{\equiv a_k \cdot 1^k + \cdots + a_3 \cdot 1^3 + a_2 \cdot 1^2 + a_1 \cdot 1\ (mod\ 9)}$$

Para terminar e completar a forma da representação do número N acrescenta-se o termo $a_0 \cdot 10^0$

$$\boldsymbol{a_k \cdot 10^k + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0}$$
$$\boldsymbol{\equiv a_k \cdot 1^k + \cdots + a_3 \cdot 1^3 + a_2 \cdot 1^2 + a_1 \cdot 1 + a_0 \cdot 10^0\ (mod\ 9)}$$

O qual é semelhante a $\boldsymbol{N \equiv a_k \cdot 1^k + \cdots + a_3 \cdot 1^3 + a_2 \cdot 1^2 + a_1 \cdot 1 + a_0 \cdot 10^0\ (mod\ 9)}$. Por Congruência, N e $a_k \cdot 1^k + \cdots + a_3 \cdot 1^3 + a_2 \cdot 1^2 + a_1 \cdot 1 + a_0$

possuem o mesmo quando divididos por 9. Dessarte, N é divisível por 9 se, e somente se, a soma de seus dígitos for divisível por 9.

Exemplo 3.2.8 864486 *é divisível por* 9 *pois* $8+6+4+4+8+6=36$ *e* 36 *é divisível por 9.*

3.2.9 Critério de Divisibilidade por 10

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$. Assim sendo, N é divisível por 10 ($10 \mid N$) se, e somente se, $a_0 = 0$".

Demonstração: É evidente que $10 \equiv 0\ (mod\ 10)$ e aplicando a propriedade 3 do Teorema 2.4

$$\boldsymbol{10^1 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{10^2 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{10^3 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{10^k \equiv 0\ (mod\ 10)\ \forall\ k \geq 1}$$

Manipula-se as Congruências conforme a propriedade 2 do Teorema 2.4

$$\boldsymbol{a_1 \cdot 10^1 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{a_2 \cdot 10^2 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{a_3 \cdot 10^3 \equiv 0\ (mod\ 10)}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{.}$$
$$\boldsymbol{a_k \cdot 10^k \equiv 0\ (mod\ 10)\ ;\ a_m\ \forall\ m = 1, 2, 3, \ldots, k}$$

A fim de obter o N no lado esquerdo da Congruência é preciso somá-las e inserir o termo $a_0 \cdot 10^0$

$$\boldsymbol{a_k \cdot 10^k + \cdots +\ a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 +\ a_0 \cdot 10^0 \equiv a_0 \cdot 10^0\ (mod\ 9)}$$

Por definição, N e a_0 possuem o mesmo resto quando divididos por 10. Conclui-se que se o $10 \mid\ a_0 \rightarrow\ a_0 = 0$.

Exemplo 3.2.9 *500 é divisível por 10 por o último algarismo é 0.*

3.2.10 Critério de Divisibilidade por 11

"Seja $N = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$ o número inteiro no sistema decimal (base 10) tal que $0 \leq a_k < 10$ e seja S a soma dos algarismos de N de ordem par menos a de ordem ímpar:

$$S = a_k \cdot (-1)^k + \cdots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0$$

Assim sendo, N é divisível por 11 $(11 \mid N)$ se, e somente se, S for divisível por 11 $(11 \mid S)$".

Demonstração: Primeiramente, percebe-se que:

$$\mathbf{10 + 1 = 11}$$

$$\mathbf{100 - 1 = 99 = 9 \cdot 11}$$

$$\mathbf{1000 + 1 = 1001 = 91 \cdot 11}$$

$$\mathbf{10000 - 1 = 9999 = 909 \cdot 11}$$

$$\mathbf{100000 + 1 = 1000001 = 9091 \cdot 11}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

Pela propriedade 3 do Teorema 2.4, tem-se que:

$$\mathbf{10^1 \equiv (-1) (mod\ 11)}$$

$$\mathbf{10^2 \equiv 1\ (mod\ 11)}$$

$$\mathbf{10^3 \equiv (-1) (mod\ 11)}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{.}$$

$$\mathbf{10^k \equiv (-1)^k (mod\ 11)}$$

Aplicando a propriedade 2 do Teorema 2.4 multiplica-se as congruências por $a_m \forall\, m = 1, 2, 3, \ldots, k$

$$\boldsymbol{a_1 \cdot 10^1 \equiv a_1 \cdot (-1)(mod\ 11)}$$

$$\boldsymbol{a_2 \cdot 10^2 \equiv a_2 \cdot 1\ (mod\ 11)}$$

$$\boldsymbol{a_3 \cdot 10^3 \equiv a_3 \cdot (-1)(mod\ 11)}$$

$$\boldsymbol{.}$$

$$\boldsymbol{.}$$

$$\boldsymbol{.}$$

$$\boldsymbol{a_k \cdot 10^k \equiv a_k \cdot (-1)^k (mod\ 11)}$$

E pela propriedade 1 do Teorema 2.2.1 a soma de todas as Congruências é

$$\boldsymbol{a_k \cdot 10^k + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1} \equiv \boldsymbol{a_k \cdot (-1)^k + \cdots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1)\ (mod\ 11)}$$

Aplicando a propriedade 2 do Teorema 2.4 soma-se o escalar Congruências $a_0 \cdot 10^0$ e a Congruência anterior:

$$\boldsymbol{a_k \cdot 10^k + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_k \cdot (-1)^k + \cdots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 10^0\ (mod\ 11) = N \equiv a_k \cdot (-1)^k + \cdots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 10^0\ (mod\ 11)}$$

Portanto, pela definição de Congruências, N e $a_k \cdot (-1)^k + \cdots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0$ possuem o mesmo resto quando divididos por 11. Como resultado, N é divisível por 11 se, e somente se, se a soma dos algarismos de ordem par menos a soma dos algarismos de ordem ímpar é um número divisível por 11.

Exemplo 2.2 2530 é divisível por 11 pois $5 + 0 = 5$ e $2 + 3 = 5$, $5 - 5 = 5$ e 0 é divisível por 11.

CONSIDERAÇÕES FINAIS

A prova dos Critérios de Divisibilidade dos inteiros 2 ao 11 utilizando Congruências é realizado por intermédio de propriedades selecionadas junto com exemplos para melhor assimilação dos argumentos feitos. Inicialmente estudou-se as

premissas necessárias para dar continuidade ao trabalho: Divisibilidade e Congruências.

Em seguida, a partir pesquisa bibliográfica, apurou-se de quais Teoremas, Definições e Corolários suficientes para apresentação da prova dos Critérios de Divisibilidade utilizando Congruências de maneira coerente. Então, na maioria dos Critérios manteve-se a lógica de encontrar a Congruência do respectivo módulo, elevar – expoente – e multiplicar por um escalar e somar todos os parâmetros da Congruência de modo que o termo esquerdo gerasse o número inteiro N na base decimal e o direito o que cada Critério de Divisibilidade determinava.

Foi possível verificar ao término do trabalho, a proficiência das Congruências em provas de Critérios de Divisibilidade. Ademais, os procedimentos utilizados evidenciam a facilidade ou dificuldade das demonstrações dos Critérios de Divisibilidade.

As provas apresentadas neste trabalho visam fornecer a relação entre os Critérios de Divisibilidade e Congruências, o entendimento de regras práticas provadas por Congruência. Dessa forma, proporcionando aos alunos e professores do Ensino Básico ou Superior explanações relativas à temática, e também, para os que anseiam fazer pós-graduação em Matemática Pura, especificamente na área desta pesquisa. Aperceber que, outros estudos científicos poderão surgir trazendo mais luz a este tema de modo que nesse trabalho o que se abordou não é absoluto, mas um singelo aporte às pesquisas futuras.

REFERÊNCIAS

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003.

DURBIN, John R. Equivalence, Congruence, Divisibility. In: **Modern Algebra: An Introduction.** 6 ed. Texas: Wiley, 2008. P. 52-70.

FILHO, Edgard de Alencar. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

Gauss, Carl Friedrich. ***Disquisitiones Arithmeticae***. Lipsiae, in commission apvd G. Fleischer, jun, 1801.Pdf. https://www.loc.gov/item/36021572/.

MACHADO, Antônio et al. **Matemática e Realidade**. 9. ed. São Paulo: Editora, 2018.

MCDOWELL, Eric L. (Berry. Divisibility Tests: A History and User's Guide. **MAA Convergence,** Washington, D.C., v. 15, mai. 2018 Disponível em: https://www.maa.org/press/periodicals/convergence/divisibility-tests-a-history-and-users-guide. Acesso em: 8 fev. 2022.

MOURA, RAFAEL NOGUEIRA DE. CONGRUÊNCIAS MODULARES E ALGUMAS APLICAÇÕES PARA A EDUCAÇÃO BÁSICA. 2015. 55 f. Dissertação (Mestrado Acadêmico ou Profissional em 2015) - Universidade Estadual do Ceará, , 2015. Disponível em: SidUece - Sistema de Informação e Documentação Acesso em: 11 de maio de 2022

ROSEN, Kenneth H. **Elementary number theory and its applications**. 6. ed. New York, N.y: Pearson, 2011.

RODRIGUES, A. **Sistemas de numeração: evolução histórica, fundamentos e sugestões para o ensino**. Dissertação de Mestrado Profissional em Matemática. Universidade Federal do Oeste do Pará, Santarém, 2013. Disponível em: Dissertação_SistemaDeNumeração.pdf (ufopa.edu.br). Acesso em: 13 mar. 2022.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Brasília: IMPA, 1998.

SILVA, L. H. P. **Uma aplicação da congruência na determinação de critérios de divisibilidade**. 2015. 52 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal de Goiás, Goiânia, 2015. Disponível em: Dissertação - Luis Henrique Pereira da Silva - 2015.pdf (ufg.br). Acesso em: 5 set. 2021