UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO ERISSON BATISTA GOMES

CRITÉRIOS DE DIVISIBILIDADE PARA NÚMEROS GRANDES

JUAZEIRO DO NORTE
2023

FRANCISCO ERISSON BATISTA GOMES

CRITÉRIOS DE DIVISIBILIDADE PARA NÚMEROS GRANDES

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientador: Dr.Valdir Ferreira de Paula Junior

JUAZEIRO DO NORTE
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

G633c Gomes, Francisco Erisson Batista.
Critérios de divisibilidade para números grandes / Francisco Erisson Batista Gomes –2023.
49 f. il. color.; 30 cm.
(Inclui bibliografia, p. 40).

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia, Programa de Pós-graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2023.

Orientação: Dr.Valdir Ferreira de Paula Junior.

1. Números Primos. 2. Teorema de Divisibilidade. 3. Critérios de divisibilidade. I. Título.

CDD 510

Bibliotecário: João Bosco Dumont do Nascimento – CRB 3/1355

FRANCISCO ERISSON BATISTA GOMES

CRITÉRIOS DE DIVISIBILIDADE PARA NÚMEROS GRANDES

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciênciase Tecnologia da Universidade Federal doCariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada em: 30 de agosto de 2023.

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
VALDIR FERREIRA DE PAULA JUNIOR
Data: 26/10/2023 08:55:16-0300
Verifique em https://validar.iti.gov.br

Prof. D.r. Valdir Ferreira de Paula Junior
CCT/UFCA/Interno

gov.br Documento assinado digitalmente
FRANCISCO PEREIRA CHAVES
Data: 26/10/2023 09:24:21-0300
Verifique em https://validar.iti.gov.br

Prof. D.r. Francico Pereira Chaves
CCT/UFCA/Interno

Prof. Dr. Flávio França Cruz
CCT/URCA/Externo

gov.br Documento assinado digitalmente
PAULO CESAR CAVALCANTE DE OLIVEIRA
Data: 30/10/2023 10:15:59-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Paulo César Cavalcante de Oliveira
CCT/URCA/Externo

Para minha mãe Margarida e
meu pai Valdeci.

Agradecimentos

Agradeço principalmente a minha mãe, Margarida, a meu pai, Valdeci e a meus irmão pela educação e ensinamentos a mim fornecida e pelo apoio. Aos meus professores, pela Excelente orientação no curso de Mestrado Profissional em Matemática da Universidade Federal do Cariri - UFCA, ao professor Leandro e em especial ao professor, e meu orientador, Valdir Ferreira de Paula Júnior pela excelente orientação na construção deste trabalho.

Sou grato ao programa de Bolsas de estudos da CAPES, vinculada a UFCA, pelo apoio financeiro e aos membros da banca examinadora pela contribuição no aperfeiçoamento deste trabalho.

Agradeço a meus amigos e colegas do curso de mestrado pelo companheirismo em momentos difíceis, em especial aos colegas Diógenes, Cléristos, Natálio, kelly e Niwlandes. Por ultimo, mas não menos importante, agradeço a amigos da cidade de Araripina e Exu pelo apoio e acolhimento, bem como a amigos e colegas da Escola estadual de Pernambuco, Moisés Bom De Oliveira, e aos da escola São Vicente de Paula-Exu.

RESUMO

Neste trabalho serão apresentado resultados voltados para divisão nos inteiros, para determinar se um número n, é divisível por p, para $n, p \in \mathbb{Z}$. No decorrer dos capítulos, apresentamos noções elementares sobre conjuntos, indução finita, divisibilidade e números primos para que seja possível desenvolver ferramentas capazes de viabilizar a demonstração do resultado que nos permite atingir o objetivo deste trabalho, intitulado Teorema da Divisibilidade, o qual faremos aplicações ao ensino básico por meio dos Critérios de divisibilidade para números formados por uma grande quantidade de algarismos, e como aplicações ao ensino superior, apresentamos a demonstração de resultados de Aritmética.

Palavras-chave: Números Primos. Teorema de Divisibilidade. Critérios de divisibilidade.

ABSTRACT

This work will present results focused on division in integers, to determine whether a number n, is divisible by p, for $n, p \in \mathbb{Z}$. Throughout the chapters, we present elementary notions about sets, finite induction, divisibility and prime numbers so that it is possible to develop tools capable of enabling the demonstration of the result that allows us to achieve the objective of this work, entitled Divisibility Theorem, which we will apply to the basic education through the divisibility criteria for numbers formed by a large number of digits, and as applications to higher education, we present the demonstration of Arithmetic results.

Keywords: Prime Numbers. Divisibility Theorem. Divisibility criteria.

Sumário

1 Introdução **1**

2 Conjuntos Numéricos **3**

2.1 Conjuntos 3

2.2 Indução Finita 7

3 Divisibilidade e Números Primos **12**

3.1 Divisibilidade em $\mathbb{Z}$ 12

3.2 Números Primos 14

4 O Teorema Divisibilidade e Aplicações **18**

4.1 Números do tipo 9_n 18

4.2 Teorema do Período 26

4.3 Teorema de Divisibilidade 32

5 Critérios de Divisibilidade **35**

6 Considerações Finais **39**

Referências Bibliográficas **40**

Capítulo 1

Introdução

Neste trabalho, pretende-se apresentar um método de divisibilidade aplicável no sistema de numeração decimal, apresentar aplicações em conteúdos de matemática básica e utilizá-lo para apresentar novas abordagens em demonstrações de resultados elementares em Teoria dos Números. De forma específica, pretende-se apresentar e demonstrar o Teorema de Divisibilidade, o qual permite criar Critérios de Divisibilidade e demonstrar teoremas sobre números primos de formas diferenciadas das abordagens dos materiais de referência utilizadas. Este trabalho está organizado em seis capítulos, sendo este o capítulo introdutório.

No Capítulo 2, apresentamos noções e propriedades de conjuntos, bem como operações entre dois conjuntos e entre elemento e conjunto. Serão expostos alguns conjuntos especiais de fundamental importância para o desenvolvimento das ideias que pretendemos expor. Mostraremos operações entre elementos do conjunto dos números inteiros, e serão apresentadas aplicações do método de demonstração por absurdo por meio do Princípio de Indução Finita e do Princípio da Boa Ordenação.

No Capítulo 3 falamos sobre divisibilidade no conjunto dos números inteiros, trazendo algumas aplicações do Princípio de Indução no que diz respeito ao Binômio de Newton e o Teorema do Cociente e do Resto, conhecido também como Divisão Euclidiana. Posteriormente, apresentamos a noção de Mínimo Divisor Comum e Máximo Divisor Comum abordamos o conceito de números primos, provamos o Teorema da Infinitude dos Números Primos e o Teorema Fundamental da Aritmética, bem como o Pequeno Teorema de Fermat que é de fundamental importância para o desenvolvimento dos Teoremas do Período e de Divisibilidade.

Nos Capítulos 4 e 5, abordamos a parte principal deste trabalho. No Capítulo 4, desenvolvemos as ideias relacionadas aos Teoremas do Período e Divisibilidade. Além disso, apresentamos exemplos práticos da utilidade dos resultados apresentados para números não divisíveis por 2 e por 5. Já no Capítulo 5, apresentamos resultados de Aritmética como o Teorema da Infinitude dos Números Primos e critérios de divisibilidade para números grandes.

No Capítulo 6, fazemos uma abordagem geral de todo o trabalho, apresentando o que conseguimos demonstrar a partir do Teorema de Divisibilidade. Vale ressaltar que foram consultados quatro livros, os quais estão descritos nas Referências Bibliográficas, sendo um de Aritmética, um de Análise Matemática e dois livros sobre Teoria dos Números.

Capítulo 2

Conjuntos Numéricos

Neste capítulo, vamos apresentar noções elementares sobre conjunto e apresentar operações neste tipo de estrutura. Pretende-se apresentar o Método de demonstração por Absurdo, demonstrações do Princípio de Indução Finita e Princípio da Boa Ordenação bem como definir o conjunto dos números Naturais e Inteiros e suas respectivas propriedades.

O livro texto que utilizamos como referência, ou mesmo como material complementar é o do autor Lima[1], o qual faz uma abordagem sobre os assuntos tratados neste capítulo e serve como material complementar referente ao conteúdo de conjuntos.

2.1 Conjuntos

Um conjunto é uma coleção de objetos concretos ou abstratos, os quais são denominados seus elementos. Para um elemento fazer parte desta coleção, ele deve ter todas as propriedades que caracteriza o conjunto.

Pode-se estabelecer uma relação entre conjunto e objeto, a qual é denominada de relação de pertencimento. Esta relação indica se um determinado elemento está, ou não, em um determinado conjunto.

Dado um conjunto representado por A, este possui uma ou mais regras que o caracterizam e essas regras podem ser descritas como uma propriedade γ. A partir desta propriedade podemos verificar se determinado objeto tem a propriedade γ, ou não, e assim estabelecer qual relação existe entre objeto e conjunto.

Quando um elemento x cumpre a propriedade γ que caracteriza o conjunto A, dizemos que x pertence a A e denotamos por $x \in A$, caso contrário, dizemos que x não pertence a A e denotamos por $x \notin A$. Vale salientar que dizermos que A é um conjunto formado por elementos x, tais que estes atendem uma propriedade γ, é equivalente a representar o conjunto A da seguinte forma:

$$A = \{\text{x; x atende a propriedade } \gamma\}.$$

Geralmente uma propriedade que caracteriza determinado conjunto é uma proposição, a qual é uma afirmação que podemos julgar como verdadeira ou falsa de acordo com as propriedades e definições estabelecidas inicialmente. Vale ressaltar que quando um conjunto não possui elementos esse é chamado de conjunto Vazio.

Definição 1. *Um conjunto é chamado de vazio, denotado por $\varnothing$, quando qualquer que seja o elemento x, temos que $x \notin \varnothing$.*

Uma estrutura importante na teoria de conjuntos é a notação de conjunto Universo, representada geralmente por U. Quando trabalhamos alguma situação envolvendo elementos e estabelecemos características sobre estes, o conjunto universo será formado por todos os elementos da situação.

Vejamos um exemplo prático de como fazer operações entre elementos e conjuntos, bem como aplicar as definições de conjunto vazio e universo.

Exemplo 1. *Expresse os conjuntos a seguir:*

(I) $X = \{a;$ *a é sigla de estado do Nordeste Brasileiro formado por vogal e consoante*$\}$,

(II) $Y = \{b;$ *b é sigla de estado do Nordeste Brasileiro formado somente por consoantes ou que tenha a vogal "E"em sua composição*$\}$,

(III) $Z = \{c;$ *c é sigla de estado do Nordeste Brasileiro formado exclusivamente por vogais*$\}$.

Note que neste exemplo, podemos considerar como conjunto Universo U, ao conjunto formado por todas as siglas dos estados do Nordeste Brasileiro, logo:

(a) $U = \{\text{MA, PI, CE, RN, PB, PE, AL, SE, BA}\}$,

(b) $X = \{\text{MA, PI, CE, PE, AL, SE, BA}\}$,

(c) $Y = \{\text{RN, PB, CE, PE, SE}\}$,

(d) $Z = \varnothing$.

Note que $CE \in X$, $AL \notin Y$ e devido nenhum elemento de U ser formado somente por vogais, segue que Z é vazio. Como já estabelecemos a relação entre elemento e conjunto, vamos apresentar relações entre conjuntos: estar contido ou contém, união , interseção, igualdade, diferença e complementar.

Definição 2. *Dados dois conjuntos A e B, diremos que A está contido em B, descrito por $A \subset B$, quando todo elemento pertencente a A também pertence a B, do contrário, dizemos que A não está contido em B, representa-se por $A \not\subset B$. Por outro lado, diremos que A contém B, $A \supset B$, quando todo elemento que pertence a B também pertence a A, do contrário, dizemos que A não contém B e denota-se por $A \not\supset B$.*

Em particular, temos que todo conjunto é subconjunto de si. Utilizando o Exemplo 1, é fácil ver que $X \subset U$ e $Y \not\supset X$. Vale ressaltar que devido a definição de conjunto Universo e Vazio, temos que todo conjunto de uma discussão sempre está contido em U, que $\varnothing$ está contido em qualquer outro, além disso, qualquer conjunto está contido em si.

Definição 3. *Chama-se de conjunto união entre os conjuntos A e B, em notação $A \cup B$, ao conjunto formado por todos os elementos que está em A ou em B.*

Note que quando dois conjuntos tem elementos repetidos não ha necessidade de repeti-lo na união, uma vez que dizer n vezes que um elemento está em um conjunto é o mesmo que dizer uma única vez que ele pertence ao conjunto.

Do Exemplo 1, temos que:

(I) $X \cup Y = \{\text{MA, PI, CE, RN, PB, PE, AL, SE, BA}\}$,

(II) $X \cup X = \{\text{MA, PI, CE, PE, AL, SE, BA}\}$,

(III) $X \cup \varnothing = \{\text{MA, PI, CE, PE, AL, SE, BA}\}$,

(IV) $X \cup U = \{\text{MA, PI, CE, RN, PB, PE, AL, SE, BA}\}$.

Definição 4. *Chama-se de conjunto interseção entre os conjuntos A e B, em notação $A \cap B$, ao conjunto formado por todos os elementos que está em A e em B.*

Do Exemplo 1, temos que:

(I) $X \cap Y = \{\text{CE, PE, SE}\}$.

Agora apresentaremos a definição de igualdade entre conjuntos e esta tem como base as estruturas de contido e conter.

Definição 5. *Dizemos que dois conjuntos A e B são iguais, em notação $A = B$, quando $A \subset B$ e $B \subset A$. Caso contrário, dizemos que $A \neq B$.*

Temos, pelo Exemplo 1, que $X \cup Y = U$ e $X \cap Y \neq U$ pois $U \not\subset X \cap Y$. Quando $A \subset B$ dizemos que A é subconjunto de B. Temos que todo conjunto é subconjunto de si, no caso em que $A \subset B$ e $A \neq B$ dizemos que A é subconjunto próprio de B. Vamos falar sobre complementar, que funciona basicamente como uma subtração entre conjuntos.

Definição 6. *Dados A e B conjuntos contidos em um determinado universo U. Definimos o complemento de B com relação a A, denotado por $A\backslash B$, como sendo o conjunto formado por todo elemento do Universo, que está em A e não está em B. Em particular, quando $A = U$ denotaremos $U\backslash B$ como B^C e este é chamado simplesmente de complementar de B.*

Temos que, usando o Exemplo 1, que $X\backslash Y = \{\text{MA, PI, AL, BA}\}$, $X^C = \{\text{RN, PB}\}$, $U^C = \varnothing$ e $\varnothing^C = U$. A seguir descreveremos três conjuntos de fundamental importância para nossa discussão, já que se trata dos conjuntos numéricos. Eles são o conjunto dos números naturais, inteiros e racionais:

O conjunto dos números naturais, representados por $\mathbb{N}$, é formado pelos números positivos $1, 2, 3, ...$, portanto:

$$\mathbb{N} = \{1, 2, 3, 4, ...\}.$$

O conjunto dos números inteiros, representados por $\mathbb{Z}$, é formado pelos números $1, 2, 3, ...$, 0 e $-1, -2, -3, ...$ Portanto:

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}\ .$$

Denotamos $\mathbb{Z}^- = \{-1, -2, ...\}$ e $\mathbb{Z}^+ = \{0, 1, 2, ...\}$, assim temos que $\mathbb{Z} = \mathbb{Z}^- \cup \mathbb{Z}^+$ onde $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ é o conjunto dos inteiros positivos e $\mathbb{Z}^- = \mathbb{Z}\backslash\mathbb{Z}^+$ é conhecido como o conjunto dos inteiros negativos.

O conjunto dos números racionais, descrito por $\mathbb{Q}$, é formado por todo número que pode ser escrito em forma de fração p/q onde $p \in \mathbb{Z}$ e $q \in \mathbb{Z}\backslash\{0\}$. Este conjunto é dado por:

$$\mathbb{Q} = \{p/q\ ;\ p \in \mathbb{Z} \text{ e } q \in \mathbb{Z}\backslash\{0\}\}.$$

Houve a necessidade de definir outro conjunto numérico que contém todo número do sistema decimal, o qual é denotado por $\mathbb{R}$ e é chamado de conjunto dos números Reais, pois foi comprovado a existência de números do sistema decimal, por exemplo π e $\sqrt{2}$, que não estão em $\mathbb{Q}$.

Na seção seguinte, estaremos apresentando problemas numéricos envolvendo igualdades, ou desigualdades, e métodos eficientes para solucionar esse tipo de problema.

2.2 Indução Finita

Iniciamos esta seção apresentando um axioma que tem fundamentação na lógica matemática. Este axioma será de grande utilidade para verificar a veracidade de resultados envolvendo conjuntos e problemas de Aritmética.

Uma proposição é toda afirmação que pode ser julgada como verdadeira ou falsa. Como os problemas que procuramos abordar são proposições, utilizaremos este axioma a seguir para prova-los, e este método de demonstração chamamos de método de demonstração por absurdo.

Axioma 1. *Uma proposição verdadeira sempre implicará algo verdadeiro.*

Vamos aplicar este resultado na proposição a seguir:

Exemplo 2. *Sendo X um conjunto não vazio, temos que $\varnothing \subset X$.*

Demonstração: De fato, suponha por absurdo que $\varnothing \not\subset X$. Então, pela Definição 2, existe $x \in \varnothing$ e $x \notin X$. chegamos assim a um absurdo, pois não pode existir elemento x, tal que $x \in \varnothing$. Portanto, segue que $\varnothing \subset X$. ■

Podemos fazer três observações importantes a respeito do conjunto $\mathbb{N}$. Elas estão descritas no Axioma 2 descrito a seguir:

Axioma 2. *O conjunto $\mathbb{N}$ possui as seguintes características:*

(I) Existe uma relação de sucessão em $\mathbb{N}$, onde $s(n) = n+1$ e representa o inteiro sucessor de n.

(II) Existe um menor elemento, denotado por 1, onde todo inteiro positivo não pode ser menor que 1.

(III) Se X é um subconjunto de $\mathbb{N}$ onde $1 \in X$ e se Para todo n inteiro pertencente a X temos que $n+1$ também pertence a X então $X = \mathbb{N}$.

O Axioma2 é conhecido como Axioma de Peano. Com base no livro de Hefez [2], em $\mathbb{Z}$ existem duas operações denominadas de soma, denotada por "$+$", e produto, denotada por "$\cdot$", e satisfazem as proposições a seguir:

Proposição 2.1. *(I) Para todo a, b, c e d inteiros, se $a = c$ e $b = d$ então $a + b = c + d$ e $a \cdot b = c \cdot d$.*

(II) Para todo a e b inteiros temos que $a + b = b + a$ e $a \cdot b = b \cdot a$.

(III) Para todo a, b e c inteiros temos que $a+(b+c) = (a+b)+c$ e $a\cdot(b\cdot c) = (a\cdot b)\cdot c$.

(IV) Existem elementos neutros, onde o da soma é 0 e o do produto é 1, de modo que $a + 0 = a$ e $a \cdot 1 = a$.

(V) Para todo a existe um elemento simétrico b, $b = -a$, tal que $a + b = 0$.

(VI) Para todo a, b e c inteiros temos que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Além dessa Ultima proposição, para $a, b \in \mathbb{Z}$, temos que:

(I) a é menor que b, denotado por $a < b$ quando $b - a \in \mathbb{N}$.

(II) a é maior que b, denotado por $a > b$ quando $a - b \in \mathbb{N}$.

(III) a é menor ou igual a b, denotado por $a \leq b$ quando $b - a \in \mathbb{Z}^+$.

(IV) a é maior ou igual a b, denotado por $a \geq b$ quando $a - b \in \mathbb{Z}^+$.

A seguir apresentamos a Proposição 2.2 que apresenta alguns fatos que ocorrem com elementos de $\mathbb{Z}$.

Proposição 2.2. *Para a, b e c inteiros, os seguintes resultados são verdadeiros:*

(I) $a \cdot 0 = 0$,

(II) $a = b \Leftrightarrow a + c = b + c$,

(III) $a < b$ *e* $b < c \Rightarrow a < c$,

(IV) $a < b \Leftrightarrow a + c < b + c$,

(V) Se $c \in \mathbb{N}$, $a < b \Leftrightarrow a \cdot c < b \cdot c$,

(VI) Se $c \in \mathbb{N}$, $a = b \Leftrightarrow a \cdot c = b \cdot c$.

Utilizando esta última proposição, vamos provar uma importante desigualdade em $\mathbb{Z}$ que é de fundamental importância para a prova do princípio da boa ordenação.

Proposição 2.3. *Para todo inteiro n, não existe um valor inteiro x tal que $n < x < n + 1$.*

Demonstração: Suponha, por absurdo, que para certo valor de n existe $x \in \mathbb{Z}$ de modo que $n < x < n + 1$. Daí, existe um número $a \in \mathbb{N}$, $a = x - n$, onde $0 < a < 1$. como a é inteiro positivo, chegamos aqui a um absurdo, já que $a < 1$ e temos que não pode existir nenhum número natural menor que 1. Portanto, segue que o inteiro x não pode existir e pelo princípio de demonstração por absurdo concluímos que o resultado é verdadeiro. ■

Temos que cardinalidade de um conjunto corresponde a quantidade de elementos que ele possui, assim um subconjunto de $\mathbb{N}$ é finito, quando a cardinalidade deste é um valor numérico de $\mathbb{Z}^+$.

Note que o conjunto $\mathbb{N}$ não é finito, pois para todo número inteiro n que tomamos, sempre existe um número em $\mathbb{N}$ que é maior que n. Neste caso dizemos que o conjunto é infinito. Logo, X é infinito se, e só se, não é limitado por um $n \in \mathbb{Z}$.

Em posse das ferramentas apresentadas nesta seção até o momento, provaremos agora o Princípio da Boa Ordenação. Esse resultado mostra que todo subconjunto não vazio de $\mathbb{N}$ tem um menor elemento.

Teorema 2.4. *(Princípio da Boa Ordenação) Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração: Seja X um subconjunto não vazio de $\mathbb{N}$. Se $1 \in X$ este será o menor elemento de X. Suponha, por absurdo, que X não possui elemento mínimo, daí existe um inteiro a diferente de 1 de modo que $a \in X$, já que este é não vazio. Seja Y o subconjunto de $\mathbb{N}$ formado por todos os inteiros consecutivos, menores ou iguais a a e que não são elementos mínimos de X.

Temos que $1 \in Y$ e se $y \in Y$ temos que $y + 1 \in Y$, pois X não possui um menor elemento e se existir y em Y onde $y + 1 \notin Y$, teríamos que $y + 1$ estaria em X e seria o seu menor elemento, o que não pode ocorrer por hipótese.

Temos que Y é limitado por $s(a)$ e pela característica de Y devemos ter que $Y = \mathbb{N}$, logo $\mathbb{N}$ é limitado por $s(a)$. Chegamos aqui a um absurdo gerado por supormos que X não tem elemento mínimo. Portanto, concluímos que o resultado é verdadeiro. ■

Esse resultado é útil na verificação de igualdades e desigualdades envolvendo números inteiros e utilizaremos fortemente nos capítulos seguintes.

Teorema 2.5. *(Princípio de Indução Finita) Seja* X *um subconjunto de* $\mathbb{Z}$*, infinito,* $X = \{x_1, x_2, ..., x_n, ...\}$ *com* $x_1 < x_2 < ... < x_n < ...$*, e* $P(x)$ *Uma proposição envolvendo números inteiros. Se* $P(x_1)$ *é verdadeiro e se para certo* x_n*,* $x_1 \leq x_n$*, a validade de* $P(x_n)$ *implica a validade de* $P(x_{n+1})$ *então* $P(x)$ *é válida para todo elemento de* X*.*

Demonstração: Suponha, por absurdo, que em X existe um elemento mínimo x_m, $1 < m$, onde $P(x_m)$ não é verdadeiro. Daí, como x_m é mínimo, segue que $P(x_{m-1})$ é verdadeiro. Sendo assim, devido as características da propriedade $P(x)$, teremos que $P(x_{(m-1)+1})$ também é verdadeiro, ou seja, $P(x_m)$ é verdadeiro e chegamos assim a um absurdo. Portanto, segue que este x_m não pode existir e concluímos que o resultado é verdadeiro. ■

Utilizando o princípio de indução, provaremos O Binômio de Newton. Vale lembrar que $n!$ significa o produto de todos os inteiros de 1 a n e temos também que $0! = 1! = 1$. Para $i, n \in \mathbb{N}$, $0 \leq i \leq n$, a relação de Stifel descrita a seguir é

verdadeira:

$$\frac{n!}{(n-i)!\cdot(i!)}+\frac{n!}{(n-(i+1))!\cdot(i+1)!}=\frac{(n+1)!}{(n-i)!\cdot(i+1)!}. \tag{2.1}$$

Teorema 2.6. *(Binômio de Newton) Para a e b números reais e $n\in\mathbb{N}$ temos sempre que:*

$$(a+b)^n=\sum_{i=0}^{n}\left(\frac{n!}{(n-i)!\cdot i!}\cdot a^{n-i}\cdot b^i\right).$$

Demonstração: Vamos aplicar indução finita sobre n: Para $n=1$ obtemos de fato que:

$$(a+b)^1=\sum_{i=0}^{1}\left(\frac{1!}{(1-i)!\cdot i!}\cdot a^{1-i}\cdot b^i\right).$$

Suponha que o resultado é válido para certo valor n inteiro maior ou igual a 1, ou seja:

$$(a+b)^n=\sum_{i=0}^{n}\left(\frac{n!}{(n-i)!\cdot i!}\cdot a^{n-i}\cdot b^i\right).$$

Para $n+1$ temos que:

$$(a+b)^{n+1} \;=\; (a+b)\cdot(a+b)^n,$$

utilizando a hipótese de indução obtemos:

$$(a+b)^{n+1} \;=\; (a+b)\cdot\left(\sum_{i=0}^{n}\frac{n!}{(n-i)!\cdot i!}\cdot a^{n-i}\cdot b^i\right).$$

Fazendo o caso $i=0$ no somatório e multiplicando o mesmo por $(a+b)$ obtemos:

$$(a+b)^{n+1} \;=\; a^{n+1}+\sum_{i=1}^{n+1}\left(\left[\frac{n!}{(n-i)!\cdot i!}+\frac{n!}{(n-(i+1))!\cdot(i+1)!}\right]\cdot(a^{n+1-i}\cdot b^i)\right).$$

Devido a relação de Stifel, Equação 2.1, e as propriedades do somatório, segue que:

$$(a+b)^{n+1}=\sum_{i=0}^{n+1}\left(\frac{(n+1)!}{(n+1-i)!\cdot(i)!}\cdot a^{n+1-i}\cdot b^i\right).$$

Portanto, segue que o resultado é verdadeiro

■

No capítulo a seguir, faremos a abordagem de alguns resultados envolvendo divisibilidade em $\mathbb{Z}$. O Binômio de Newton será de fundamental importância para

a demonstração do Pequeno Teorema de Fermat, o qual apresenta características importantes relacionadas a números primos.

Capítulo 3

Divisibilidade e Números Primos

Neste capítulo, serão apresentados alguns resultados relacionados à divisibilidade e números primos. Como veremos a seguir, os números primos são capazes de gerar quase todos os números inteiros quando associados à relação de multiplicação. Este capítulo está distribuído em duas seções, sendo a primeira a parte que apresenta o conceito de divisibilidade, tendo como foco principal o teorema da divisão euclidiana e a segunda é voltada para números primos, tendo como principais resultados o Teorema da Infinitude dos Números Primos, o Teorema Fundamental da Aritmética e o Pequeno Teorema de Fermat.

3.1 Divisibilidade em $\mathbb{Z}$

Dados dois números inteiros a e b, quando existe um inteiro c onde $a \cdot c = b$, dizemos que a divide b. Sendo assim, nesta seção apresentaremos algumas resultados sobre divisibilidade.

Definição 7. *Dados dois inteiros a e b, diremos que a divide b, $a \mid b$, se existe um inteiro c de modo que $a \cdot c = b$. Do contrário, dizemos que a não divide b e denotamos por $a \nmid b$.*

Partindo da definição de números inteiros pode ser verificada uma série de resultados relacionados a propriedades da divisão. Não faremos aqui a demonstração dos resultados a seguir, no entanto, a prova destes fatos pode ser encontrada no livro do autor [Hefez 2], Capítulo 3.

Proposição 3.1. *Sejam a, b, c e d números inteiros. As seguintes afirmações são verdadeiras:*

(I) $1 \mid a$, $a \mid a$ *e* $a \mid 0$,

(II) $0 \nmid a$ *para todo* $a \neq 0$,

(III) Se $a \mid b$ *e* $b \mid c$ *então* $a \mid c$,

(IV) Se $a \mid b$ *e* $c \mid d$ *então* $a \cdot c \mid b \cdot d$,

(V) Sempre que $a \mid (b + c)$ *temos que* $a \mid b$ *se, e só se,* $a \mid c$,

(VI) Se $a \mid b$ *e* $a \mid c$ *então, para quaisquer inteiros* x *e* y, $a \mid (xb + yc)$.

Um resultado que utilizaremos para desenvolver critérios de divisibilidade será descrito a seguir. Para prová-lo utilizamos alguns itens da proposição anterior.

Proposição 3.2. *Dados os números inteiros* r, s, t *e* u. *Então:*

$$r \mid (s + u \cdot t) \text{ se, e somente se, } r \mid (s - (r - u) \cdot t).$$

Demonstração: Se r divide $s + u \cdot t$ então existe um inteiro v de modo que

$$r \cdot v \;=\; s + u \cdot t,$$

somando o $-r \cdot t$ em ambos os lados da ultima igualdade obtemos:

$$r \cdot v - r \cdot t = -r \cdot t + s + u \cdot t$$

tomando em evidencia r, no primeiro lado da igualdade, e t no segundo lado, obtemos:

$$r \cdot (v - t) = s - (r - u) \cdot t,$$

segue, da definição de divisão, que $r \mid s - (r - u) \cdot t$.

Reciprocamente, se r divide $s - (r - u) \cdot t$, pela definição de divisão, existe um inteiro v de modo que.

$$r \cdot v \;=\; s - (r - u) \cdot t,$$

somando $r \cdot t$ nos dois lados da ultima igualdade, obtemos:

$$r \cdot v + r \cdot t \;=\; s + u \cdot t,$$

tomando r em evidencia no primeiro lado da igualdade, obtemos:

$$r \cdot (v + t) \;=\; s + u \cdot t,$$

segue, pela definição de divisão, que $r \mid (s + u \cdot t)$. Terminando assim a prova desta proposição. ■

Para a não negativo temos que $\mid a \mid = a$ e para a negativo temos que $\mid a \mid = -a$. Assim, podemos enunciar o teorema da divisão Euclidiana:

Teorema 3.3. *(Divisão Euclidiana) Dados dois inteiros a e b, com $b \neq 0$, existem sempre inteiros u e v de modo que:*

$$a = b \cdot u + v \text{ com } 0 \leq v <\mid b \mid.$$

Demonstração: Veja o livro do autor Hefez[2], p.46. ■

Vale ressaltar que para a e b inteiros, O máximo divisor comum entre eles é denotado por $mdc(a, b)$ e é igual ao maior inteiro que divide a e b. Já o mínimo múltiplo comum é denotado por $mmc(a, b)$ e é igual ao menor inteiro divisível por a e b. Falaremos na seção seguinte sobre números primos.

3.2 Números Primos

Vamos inicialmente definir quais características um número inteiro deve ter para que seja considerado primo.

Definição 8. *Um inteiro p maior que 1 é um número primo quando tem apenas dois divisores inteiros positivos.*

Agora enunciaremos e provaremos o teorema fundamental da aritmética que mostra a relação entre números primos e elementos de $\mathbb{N}$.

Teorema 3.4. *(Teorema Fundamental da Aritmética) Todo número inteiro maior que 1 é primo ou é escrito como produto de números primos.*

Demonstração: Para $n = 2$ o resultado é satisfeito, já que 2 é um número primo.

Suponha, por absurdo, que existe um inteiro n, que não é um número primo e que não pode ser escrito como um produto de números primos. Daí, temos que n é um número composto e $n = u \cdot v$, para u e v inteiros maiores que 1.

Como u e v são menores que n, temos que eles são primos ou escrito como produto de números primos. Logo:

$$u = p_1 \cdot p_2 \cdot ... \cdot p_r \text{ e } v = q_1 \cdot q_2 \cdot ... \cdot q_s,$$

onde p_1, p_2, ..., p_r, q_1, q_2,..., q_s são números primos.

Devido $n = u \cdot v$, segue que:

$$n = p_1 \cdot p_2 \cdot ... \cdot p_r \cdot q_1 \cdot q_2 \cdot ... \cdot q_s.$$

Assim n é escrito como produto de números primos. Daí, chegamos a uma contradição do fato de n não poder ser escrito como produto de números primos. Portanto, segue que o resultado é verdadeiro. ■

Para um inteiro a qualquer e n inteiro não negativo, podemos definir $a^0 = 1$ e a^n como o produto de a feito n vezes para todo $n > 0$. Considere a decomposição em fatores primos de n dada por $p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_m^{a_m}$ onde os números $p_1, p_2, ..., p_m$ são primos e $p_1 < p_2 < ... < p_m$.

Teremos que esta decomposição é única, pois se supormos que existem duas decomposições distintas, obtemos que existe um número primo p que dividirá um produto de primos não divisíveis por p e isso seria um absurdo devido a definição de números primos. Portanto, temos que a decomposição de um número inteiro composto em fatores primos, de acordo com o Teorema Fundamental da Aritmética, é única a menos pela ordem dos fatores no produto.

Provaremos a seguir um resultado sobre a quantidade de numeros primos existentes. Ele pode ser intitulado como Teorema dos Infinitos Números Primos e pode ser enunciado da seguinte forma:

Teorema 3.5. *Existem infinitos números primos.*

Demonstração: Suponha, por absurdo, que a quantidade de números primos é finita. Então, se $p_1, p_2, ..., p_m$ são todos esses primos existentes, teremos que que $p_1 \cdot p_2 \cdot ... \cdot p_m + 1$ é um número composto.

Sendo assim, existem naturais u e v de modo que:

$$p_1 \cdot p_2 \cdot ... \cdot p_m + 1 = u \cdot v.$$

Isolando o número 1 em um dos lados da igualdade, obtemos:

$$u \cdot v - p_1 \cdot p_2 \cdot ... \cdot p_m = 1.$$

Utilizando o Teorema Fundamental da Aritmética, obtemos que existem números primos q_1, q_2,..., q_s de modo que $u \cdot v = q_1 \cdot q_2 \cdot ... \cdot q_s$. Além disso, temos que $q_1 \mid u \cdot v$ e $q_1 \mid p_1 \cdot p_2 \cdot ... \cdot p_m$, já que $p_1, p_2, ..., p_m$ são todos os números primos existentes.

Como $u \cdot v - p_1 \cdot p_2 \cdot ... \cdot p_m = 1$, $q_1 \mid u \cdot v$ e $q_1 \mid p_1 \cdot p_2 \cdot ... \cdot p_m$, segue que $q_1 \mid 1$, que é um absurdo. Portanto, segue que a quantidade de números primos não pode ser finita. ■

Para finalização desta seção, e capítulo, provaremos o Pequeno Teorema de Fermat. Este estabelece uma relação de divisão entre um número primo e um certo número inteiro. Para que seja possível demonstrar o resultado, será necessário a utilização do lema a seguir.

Lema 3.6. *Seja p um número primo e i um inteiro onde $0 < i < p$. Então,*

$$p \mid \left[\frac{p!}{(p-i)! \cdot i!} \right]$$

.

Demonstração: Veja o livro do autor Hefez[2], p. 135. ■

Este lema será utilizado para demostrar o que é conhecido como pequeno teorema de Fermat, o qual enunciaremos e apresentaremos uma demonstração satisfatória a seguir. Este estabelece uma relação de divisão ente números primos e um inteiro qualquer e para demonstra-lo utilizaremos o princípio de indução e Binômio de Newton. A versão do Teorema apresentado aqui é similar a do livros pertencente a Ribenboim[3], p.15.

Teorema 3.7. *(Pequeno Teorema de Fermat) Sendo p um número primo e a um inteiro qualquer, temos que $p \mid (a^p - a)$. Se $mdc(p, a) = 1$ temos que $p \mid (a^{p-1} - 1)$.*

Demonstração: Provaremos primeiro que $p \mid (a^p - a)$. Tomando $p = 2$, temos que $(a^2 - a)$ é sempre um número par para todo a inteiro e portanto, $p \mid (a^p - a)$. Assim, Como todos os números primos, diferentes de 2, são ímpares, podemos admitir que p é ímpar.

Sendo p impar e considerando inicialmente que a é um inteiro positivo, vamos aplicaremos indução finita sobre a.

Para $a = 0$ temos que o resultado é verdadeiro, já que $p \mid 0$. Supondo que para certo a inteiro positivo maior ou igual a zero temos que $p \mid (a^p - a)$. Devemos mostrar que $p \mid [(a+1)^p - (a+1)]$. De fato, pelo Binômio de Newton, Teorema 2.6, temos que:

$$\begin{aligned}(a+1)^p - (a+1) &= a^p + 1 - a - 1 + \sum_{i=1}^{p-1} \frac{p!}{(p-i)! \cdot i!} \cdot a^{p-i} \\ &= a^p - a + \sum_{i=1}^{p-1} \frac{p!}{(p-i)! \cdot i!} \cdot a^{p-i}.\end{aligned}$$

Devido a Hipótese de indução, temos que:

$$p \mid (a^p - a).$$

Pelo Lema 3.6 apresentado no capítulo anterior temos que:

$$p \mid \sum_{i=1}^{p-1} \left(\frac{p!}{(p-i)! \cdot (i!)} \cdot a^{p-i} \right),$$

logo, segue que $p \mid [(a+1)^p - (a+1)]$ e concluímos, pelo princípio de indução, que $p \mid (a^p - a)$ para p impar e a inteiro positivo .

Sendo p impar e considerando agora a negativo, temos também que $p \mid (a^p - a)$, pois $a = -b$ para certo b positivo. Assim, $(a^p - a) = -(b^p - b)$ para b inteiro positivo e da demonstração feita anteriormente, temos que $p \mid (b^p - b)$. consequentemente

obtemos que $p \mid (a^p - a)$ para a negativo, já que $(a^p - a) = -(b^p - b)$ para certo b inteiro positivo.

Provaremos a segunda parte do teorema, e admitiremos que $mdc(p, a) = 1$. Devido o que já foi provado na primeira parte do resultado, temos:

$$p \quad | \quad (a^p - a),$$

daí, segue que:

$$p \quad | \quad (a^{p-1} - 1) \cdot a,$$

como $mdc(a, p) = 1$ segue que

$$p \quad | \quad (a^{p-1} - 1).$$

Portanto, concluímos a segunda parte do teorema. Finalizamos aqui a demonstração do Teorema. ■

Existem diversos resultados envolvendo números primos, no entanto, para que possamos atingir o objetivo deste trabalho, os conceitos e resultados são suficientes. Para mais informações a respeito destes números, podem ser consultado os livros dos autores Ribenboim[3] e de Santos[4].

Capítulo 4

O Teorema Divisibilidade e Aplicações

Neste capítulo, exploraremos critérios de divisibilidade em $\mathbb{Z}$. Especificamente, investigaremos as condições para que um número inteiro $\bar{x}_n$, formado por n algarismos, seja divisível por p. Esses critérios serão aplicáveis apenas quando p for um número não divisível por 2 e por 5. Para alcançar esse objetivo, analisaremos combinações lineares dos algarismos de $\bar{x}_n$.

4.1 Números do tipo 9_n

Nesta seção, mostraremos que todo inteiro p, maior que 1 e $mdc(p, 10) = 1$, divide um número com todos os seus algarismos iguais a 9. Utilizamos como base, os livros dos autores Santos [4] e Ribenboim [3] que apresentam resultados elementares, incluindo conceitos de Mínimo Múltiplo Comum e Máximo Divisor Comum. Estes conhecimentos são essenciais para o desenvolvimento do Teorema de Divisibilidade. Começamos apresentando definições iniciais e resultados que nos permitirão demonstrar tanto o Teorema do Período, quanto o Teorema de Divisibilidade.

Definição 9. *Para cada $n \in \mathbb{N}$, denotamos por π_n o conjunto de todos os inteiros positivos que são formados por n algarismos.*

Quando nos referirmos a um elemento genérico de π_n iremos representá-lo por $\bar{x}_n$, para destacar que este tem exatamente n algarismos. Tomando como exemplo π_2, os números 23, 34 e 56 são elementos desse conjunto. De forma geral, todo elemento de π_2 pode ser representado da forma $\bar{x}_2 = ab$, onde a e b são inteiros tais que $0 \leq a, b \leq 9$, com $a \neq 0$.

Definição 10. *Dado um número natural $\bar{x}_n$ formado por n algarismos, e um inteiro i, onde $0 \leq i < n$, denotamos os $n - i$ primeiros algarismos de $\bar{x}_n$ por $x_{n|i}$ e os i últimos por $x_{i|i}$. Além disso, definimos $x_{0|0} = 0$.*

Por exemplo, para o número $\bar{x}_7$= 3577585 , os 4 primeiros algarismos e os 3 últimos, são representados por:

$$x_{7|3} = 3577 \text{ e } x_{3|3} = 585.$$

Outro exemplo que vale destacar é do número $\bar{x}_8$= 10000001. Para este número, temos:

$$x_{8|5} = 100 \text{ e } x_{5|5} = 00001 = 1.$$

Note que $x_{7|7} = x_{6|6} = \cdots = x_{1|1} = 1$.

É fácil ver que a seguinte relação de igualdade é verdadeira para todo $\bar{x}_n$:

$$\bar{x}_n = 10^i \cdot x_{n|i} + x_{i|i}, \tag{4.1}$$

com $0 \leq i < n$.

A seguir, apresentamos algumas definições e resultados, voltados para compreensão e prova do Teorema 4.7. Inicialmente apresentaremos uma definição que visa facilitar a escrita de números com todos os seus algarismos iguais a 9, uma vez que a capacidade de um número $p \in \mathbb{N}$ dividir inteiros com todos os algarismos iguais será essencial para a prova do teorema do período.

Definição 11. *Para cada $n \in \mathbb{N}$, denotamos por 1_n e 9_n, respectivamente, o número formado por n algarismos, todos iguais a 1, e o número de n algarismos, todos iguais a 9 .*

De acordo com esta definição temos que:

$$9_3 = 999,\ 1_3 = 111,\ 9_6 = 999999 \text{ e } 1_1 = 1.$$

Pelo Pequeno Teorema de Fermat, veja Teorema 3.7,podemos concluir que um número primo p, com $mdc(p, 10) = 1$, sempre divide 9_{p-1}. Motivados por este resultado, iremos analisar os números inteiros p, com $mdc(p, 10) = 1$. Para isso, utilizaremos o seguinte lema:

Lema 4.1. *Para cada r e k inteiros positivos temos que:*

$$9_{r \cdot k} = 9_r \cdot \sum_{i=0}^{k-1} 10^{r \cdot i}$$

Demonstração: Fixado um inteiro positivo r, vamos provar a igualdade aplicando indução sobre k. Para $k = 1$ temos que:

$$\begin{aligned} 9_{r\cdot 1} &= 9_r \\ &= 9_r \cdot 1 \\ &= 9_r \cdot \sum_{i=0}^{1-1} 10^{r\cdot i}, \end{aligned}$$

provando a validade para $k = 1$.

Supondo que a igualdade seja válida para um certo k, inteiro maior ou igual a 1, ou seja,

$$9_{r\cdot k} = 9_r \cdot \left(\sum_{i=0}^{k-1} 10^{r\cdot i} \right).$$

Para analisar a validade do caso $k + 1$, temos que:

$$9_{r\cdot(k+1)} = 9_r \cdot 10^{r\cdot k} + 9_{r\cdot k}.$$

Usando a hipótese de indução, segue que

$$\begin{aligned} 9_{r\cdot(k+1)} &= 9_r \cdot 10^{r\cdot k} + 9_r \cdot \left(\sum_{i=0}^{k-1} 10^{r\cdot i} \right) \\ &= 9_r \cdot \left(\sum_{i=0}^{k} 10^{r\cdot i} \right). \end{aligned}$$

Assim, provamos que supondo a validade do resultado para k, ele é válido para $k+1$. Concluímos, portanto, que o resultado é verdadeiro para todo $k \in \mathbb{N}$. ■

A proposição a seguir estabelece uma relação entre os números p e n, para que p divida 9_n.

Proposição 4.2. *Seja $p \in \mathbb{N}$ ímpar maior que 1 e não divisível por 5 tal que $p \mid 9_q$ para algum $q \in \mathbb{N}$. Se r é o menor natural com $p \mid 9_r$ então, para todo $s \in \mathbb{N}$, com $s \geq r$, temos:*

$$p \mid 9_s \text{ se, e só se, } r \mid s.$$

Demonstração: Suponha inicialmente que $p \mid 9_s$. Então, existe um inteiro k tal que $p \cdot k = 9_s$. Como $s \geq r$, utilizando o Teorema da divisão Euclidiana, veja Teorema 3.3, segue que existe $u \in \mathbb{N}$ e $v \in \mathbb{Z}$ de modo que:

$$s = r \cdot u + v, \tag{4.2}$$

onde $0 \leq v < r$. Logo:

$$p \cdot k = 9_s = 9_{r \cdot u + v},$$

usando Equação (4.1) temos que:

$$p \cdot k \quad = \quad 9_{r \cdot u} \cdot 10^v + 9_v,$$

pelo Lema 4.1 segue que

$$p \cdot k \quad = \quad 9_r \cdot \left(\sum_{i=0}^{u-1} 10^{r \cdot i} \right) \cdot 10^v + 9_v,$$

isolando 9_v, em um dos lados da última igualdade, obtemos:

$$9_v = p \cdot k - 9_r \cdot \left(\sum_{i=0}^{u-1} 10^{r \cdot i} \right) \cdot 10^v.$$

Como $p \mid 9_r$ obtemos, a partir da igualdade anterior, que $p \mid 9_v$. Portanto, combinando os fatos de que $p \mid 9_v$, $0 \leq v < r$ e r ser o menor inteiro positivo tal que $p \mid 9_r$, concluímos que $v = 0$, logo, pela Equação (4.2) obtemos que $s = r \cdot u$, ou seja, $r \mid s$.

Suponhamos agora que $r \mid s$. Então, existe um inteiro k onde $r \cdot k = s$. Usando o Lema 4.1 teremos que:

$$\begin{aligned} 9_s &= 9_{r \cdot k} \\ &= 9_r \cdot \left(\sum_{i=0}^{k-1} 10^{r \cdot i} \right). \end{aligned}$$

Em virtude da definição de divisibilidade nos inteiros, obtemos a partir desta última igualdade que $9_r \mid 9_s$ e, pela hipótese inicial de $p \mid 9_r$, obtemos que $p \mid 9_s$. Portanto, finalizamos aqui a demonstração da proposição. ■

Exemplo 3. *Tomando $p = 91$, note que $91 \mid 9_{12}$ pois $7 \mid 9_{12}$, $13 \mid 9_{12}$ e $91 = 7 \cdot 13$. Assim, segue da Proposição 4.2 que o menor número divisível por 91, com todos os seus algarismos iguais a 9, pertence ao conjunto $A = \{9_1, 9_2, 9_3, 9_4, 9_6, 9_{12}\}$. Fazendo a verificação direta, obtemos que 9_6 é o menor elemento de A em que 91 divide. Utilizando a Proposição 4.2 obtemos que: $91 \mid 9_s$ se, e só se, $6 \mid s$.*

A partir da demonstração da Proposição 4.2 obtemos o seguinte lema:

Lema 4.3. *Seja $p \in \mathbb{N}$ ímpar maior que 1 e não divisível por 5 tal que $p \mid 9_r$ para algum $r \in \mathbb{N}$. Se $s \in \mathbb{N}$ e $r \mid s$, então $p \mid 9_s$.*

Usando as hipóteses da Proposição 4.2, um questionamento natural é: Dado $p \in \mathbb{N}$ onde p é ímpar maior que 1 e não divisível por 5, sempre existe $r \in \mathbb{N}$, $r < p$, de modo que $p \mid 9_r$? Este questionamento tem sua solução obtida no Teorema 4.7. Por enquanto, vamos estabelecer a existência de um r tal que $p \mid 9_r$, sem a exigência $r < p$.

Proposição 4.4. *Seja $p \in \mathbb{N}$, com p ímpar maior que 1 e não divisível por 5. Então, existe $r \in \mathbb{N}$ tal que:*

$$p \mid 9_r$$

Demonstração: Se p é um número primo, pelo Pequeno Teorema de Fermat, (veja Teorema 3.7), $p \mid 9_{p-1}$ pois $mdc(p, 10) = 1$. Assim, tomando $r = p - 1$, obtemos o resultado desejado. Vamos supor que p é composto e provar, por absurdo, que o resultado também é válido. De fato, suponha, por absurdo, que o resultado seja falso, ou seja, existe um $p \in \mathbb{N}$ composto, p ímpar maior que 1 e não divisível por 5, com $p \nmid 9_r$ para todo $r \in \mathbb{N}$. Pelo Princípio da Boa Ordenação podemos supor que p é o menor número natural composto com tal propriedade e como p é composto podemos escrevê-lo da forma $p = u \cdot v$, onde $u, v \in \mathbb{N}$, com $u \leq v$ e ambos maiores que 1, menores que p e não são divisíveis por 2 e nem por 5.

Segue do fato de que p é o menor natural, não divisível por 2 e por 5 que não divide 9_r, que existem x e y naturais de modo que $u \mid 9_x$ e $v \mid 9_y$. Sejam $a, b \in \mathbb{N}$ tais que: $n = a \cdot x$, $n = b \cdot y$ e $mmc(x, y) = n$. Denotando $mdc(u, v) = m$, vamos analisar os casos em que $m = 1$ e $m \neq 1$:

Se $m = 1$, então usando a igualdade:

$$\begin{aligned} 9_n &= 9_{x \cdot a} \\ &= 9_x \cdot \sum_{i=0}^{a-1} 10^{x \cdot i}, \end{aligned}$$

juntamente com a hipótese de $u \mid 9_x$, segue que $u \mid 9_n$. Por outro lado, temos que:

$$\begin{aligned} 9_n &= 9_{y \cdot b} \\ &= 9_y \cdot \sum_{i=0}^{b-1} 10^{y \cdot i}, \end{aligned}$$

e como $v \mid 9_y$, segue que $v \mid 9_n$.

Como por hipótese, $mdc(u, v) = 1$, segue que $u \cdot v \mid 9_n$, ou seja, $p \mid 9_n$, chegando a uma contradição. Provaremos agora o caso em que $m \neq 1$. Para isso, temos:

$$\begin{aligned} 9_{n\cdot u} &= 9_n \cdot \sum_{i=0}^{u-1} 10^{n\cdot i} \\ &= 9_n \cdot \left(\sum_{i=0}^{u-1} (10^{n\cdot i} - 1) + u \right) \\ &= 9_n \cdot \left(\sum_{i=0}^{u-1} 9_{n\cdot i} + u \right). \end{aligned}$$

Como $u \mid 9_x$, $v \mid 9_y$, $x \mid n$ e $y \mid n$, segue pelo Lema 4.3, que $v \mid 9_n$ e $u \mid \left(\sum_{i=1}^{u-1} 9_{n\cdot i} + u \right)$, e assim segue que $p \mid 9_{n\cdot u}$.

Portanto, concluímos que não pode existir um $p \in \mathbb{N}$ composto, p ímpar maior que 1 e não divisível por 5, com $p \nmid 9_r$ para todo $r \in \mathbb{N}$. Assim, segue que o resultado é verdadeiro. ■

Como observado na demonstração da Proposição 4.4, e pelo Pequeno Teorema de Fermat, temos que o Corolário 4.5 descrito a seguir é verdadeiro.

Corolário 4.5. *Sejam u, v, $p \in \mathbb{N}$, tais que $p = u \cdot v$, p é impar maior que 1 e não divisível por 5 com $u \leq v$. Sendo $mmc(x, y) = n$ onde x e y são inteiros tais que $u \mid 9_x$ e $v \mid 9_y$ temos:*

(I) Se p é primo então $p \mid 9_{p-1}$.

(II) Se p é composto e $mdc(u, v) = 1$ então $p \mid 9_n$.

(III) Se p é composto e $mdc(u, v) \neq 1$ então $p \mid 9_{n\cdot u}$.

Como aplicação deste corolário, mostraremos que $p^\alpha \mid 9_{x\cdot p^{\alpha-1}}$ para p primo e $x \in \mathbb{N}$, $x \leq p$, tal que $p \mid 9_x$.

Corolário 4.6. *Sejam $p, \alpha, x \in \mathbb{N}$, tais que $x < p$, $mdc(p, 10) = 1$, p é um número primo e $p \mid 9_x$. Então, $p^\alpha \mid 9_{x\cdot p^{\alpha-1}}$.*

Demonstração: Fixado p primo, diferente de 2 e 5, vamos aplicar indução finita sobre α.

Para $\alpha = 1$ temos:

$$p^\alpha = p$$

e

$$\begin{aligned} 9_{x\cdot p^{\alpha-1}} &= 9_{x\cdot p^{1-1}} \\ &= 9_x. \end{aligned}$$

Assim, como por hipótese temos que $p \mid 9_x$, segue que no caso $\alpha = 1$ temos que $p^\alpha \mid 9_{x\cdot p^{\alpha-1}}$.

Suponha que o resultado é válido para certo valor de α maior ou igual a 1:

$$p^\alpha \mid 9_{x\cdot p^{\alpha-1}}.$$

Para $\alpha+1$ temos que $p^{\alpha+1} = p^\alpha \cdot p$. Seja $p^{\alpha+1} = u \cdot v$ para $u = p$ e $v = p^\alpha$. Como $mmc(x, x\cdot p^{\alpha-1}) = x\cdot p^{\alpha-1}$, $u \mid 9_x$, por hipótese de indução $v \mid 9_{x\cdot p^{\alpha-1}}$ e $mdc(u,v) \neq 1$ podemos aplicar o item (III) do Corolário 4.5 e obtemos:

$$(p^\alpha \cdot p) \mid 9_{x\cdot p^{\alpha-1}\cdot p} \quad \Rightarrow \quad p^{\alpha+1} \mid 9_{x\cdot p^\alpha}.$$

Assim, supondo a validade do resultado para α, obtemos que ele também será verdadeiro para $\alpha+1$. Portanto, pelo princípio de indução finita, concluímos a demonstração do resultado. ■

Note que até o momento obtivemos que todo número inteiro ímpar, maior que 1 e não divisível por 5 sempre divide um número do tipo 9_r, no entanto, não temos ainda uma estimativa precisa sobre o valor limite de r para cada valor de p. Faremos isso no teorema a seguir. Seja $p \in \mathbb{N}$, $p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$ para $p_1, p_2, ..., p_m$ números primos todos distintos entre si. Esta decomposição é obtida quando levamos em consideração o Teorema Fundamental da Aritmética. a seguir, definiremos $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_m^{\alpha_m}$ obtidos a partir da decomposição de p.

Definição 12. *Seja $p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$ com $p_1, p_2, ..., p_m$ números primos distintos entre si. Definimos $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_m^{\alpha_m}$ como potências de primos de p.*

Como exemplo considere o número 1323. Observando que $1323 = 3^3 \cdot 7^2$, onde $3, 7$ são fatores primos distintos entre si. Assim segue que 1323 tem duas potências de primos, que são 3^3 e 7^2.

Teorema 4.7. *Sejam $p \in \mathbb{N}$, p ímpar maior que 1 e não divisível por 5 e o conjunto $\Omega_p = \{r \in \mathbb{N};\ r < p \quad e \quad p \mid 9_r\}$. Então $\Omega_p \neq \varnothing$.*

Demonstração: Se p é primo, como por hipótese p é impar e diferente de 5 então $mdc(p, 10) = 1$, assim pelo Pequeno Teorema de Fermat temos que $p \mid 9_{p-1}$ e portanto $p - 1 \in \Omega_p$. Temos neste caso que Ω_p é não vazio, mostrando a validade para p primo.

Se p é composto, das hipóteses temos que $mdc(p, 10) = 1$, então vamos provar a validade do teorema via indução sobre a quantidade de potências de primos de p.

Suponha que p possua exatamente uma potência de primo na sua decomposição, ou seja, $p = p_1^{\alpha_1}$ onde p_1 é um número primo e $\alpha_1 \in \mathbb{N}$. Como p é ímpar maior que 1 e $mdc(p, 10) = 1$, segue que p_1 também satisfaz essas mesmas hipóteses. Assim, pelo Pequeno Teorema de Fermat $p_1 \mid 9_{p_1-1}$. Daí, podemos aplicar o Corolário 4.6: Como p_1 é primo, temos que $p_1 \mid 9_{p_1-1}$. Daí, segue que

$$p_1^{\alpha_1} \mid 9_{(p_1-1)\cdot p_1^{\alpha_1-1}},$$

como $0 < p_1 - 1 < p_1$ temos que $(p_1 - 1) \cdot (p_1)^{\alpha_1-1} < p_1^{\alpha_1} = p$. Assim, Ω_p é não vazio, pois $(p_1 - 1) \cdot p_1^{\alpha_1-1} \in \Omega_p$, concluímos a base da indução.

Suponha agora que o teorema é válido para p possuindo exatamente m potências de primos na sua decomposição, com $1 \leq m$, ou seja:

$$p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m},$$

com $\alpha_i \in \mathbb{N}$, para todo $i = 1, 2, ..., m$, de modo que $\Omega_p \neq \varnothing$.

Para p possuindo exatamente $m + 1$ potências de primos na sua decomposição temos que:

$$p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m} \cdot p_{m+1}^{\alpha_{m+1}},$$

com $\alpha_i \in \mathbb{N}$ e $\alpha_i > 1$, $\forall i = 1, 2, ..., m, m + 1$. Como p_{m+1} é primo, existe um inteiro s, de modo que $p_{m+1} \mid 9_s$ para $1 \leq s \leq p_{m+1} - 1$. Assim, aplicando o Corolário 4.6 segue que: p_{m+1} é primo e $p_{m+1} \mid 9_s$ então $p_{m+1}^{\alpha_{m+1}} \mid 9_{s\cdot(p_{m+1})^{\alpha_{m+1}-1}}$.

Por hipótese de indução, $\Omega_{p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ...\cdot p_m^{\alpha_m}} \neq \varnothing$. Assim existe $n \in \Omega_{p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ...\cdot p_m^{\alpha_m}}$ de modo que $[p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m}] \mid 9_n$ com $1 < n < [p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m}]$. Temos também que $p_{m+1}^{\alpha_{m+1}} \mid 9_{s\cdot p_{m+1}^{\alpha_{m+1}-1}}$.

Sendo $p = u \cdot v$ com u e v iguais respectivamente ao menor número e ao maior número dentre $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m}$ e $p_{m+1}^{\alpha_{m+1}}$, temos que existem $x, y \in \{n, s \cdot p_{m+1}^{\alpha_{m+1}-1}\}$, $x \neq y$, de modo que $u \mid 9_x$ e $v \mid 9_y$.

Como, por hipótese, p é ímpar maior que 1 e não divisível por 5 e $u, v, x, y \in \mathbb{N}$ satisfazem:

$$p = u \cdot v,\ u \leq v,\ u \mid 9_x,\ v \mid 9_y \text{ e } mdc(u, v) = 1,$$

segue pelo Corolário 4.6, item (II), que:

$$p \mid 9_z,$$

com $z = mmc(x, y) = mmc(n, s \cdot p_{m+1}^{\alpha_{m+1}-1})$.

Resta mostrar somente que $z \in \Omega_p$, ou seja:

$$z < p.$$

De fato, como:

$$n < [p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m}] \text{ e } s \cdot p_{m+1}^{\alpha_{m+1}-1} < p_{m+1}^{\alpha_{m+1}},$$

segue que $z \leq n \cdot s \cdot p_{m+1}^{\alpha_{m+1}-1} < p$. Portanto, $z \in \Omega_p$ e $\Omega_p \neq \varnothing$.

Segue pelo princípio de indução finita que $\Omega_p \neq \varnothing$ para p formado por qualquer quantidade de números primos em sua decomposição. Como, pelo Teorema Fundamental da Aritmética todo número natural maior que 1 se escreve da forma

$$p = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m},$$

com $\alpha_i, p_i \in \mathbb{N}$, $\alpha_i > 1$, p_i primo e $p_i \neq p_j$ para todo $i \neq j$. Portanto, concluímos a demonstração do resultado. ■

Note que nem sempre $p-1$ é o menor valor para que $p \mid 9_{p-1}$ para p primo diferente de 2 e 5. Por exemplo, $13 \mid 9_6$ e neste caso o menor valor numérico para b, de modo que $13 \mid 9_b$, será 6 e não 12. Sendo 9_r um número natural que é divisível por p, existe um único inteiro k_r, de modo que:

$$9_r = p \cdot k_r.$$

Este fato será de fundamental importância para o desenvolvimento dos resultados da seção seguinte.

4.2 Teorema do Período

Buscaremos apresentar e provar o Teorema do Período, para isso iniciaremos provando o seguinte resultado:

Proposição 4.8. *Sejam $r, p \in \mathbb{N}$, com $r < p$ tais que $mdc(p, 10) = 1$ e $p \mid 9_r$. Então, para cada $0 \leq i \leq r$ existem únicos $k_i \in \mathbb{Z}^+$, e $\Gamma_i \in \mathbb{N}$, com $0 < \Gamma_i < p$, tal que:*

$$10^i \cdot \Gamma_i = p \cdot k_i + 1$$

Demonstração: Se $i = 0$, basta tomar $k_0 = 0$ e $\Gamma_0 = 1$ e obtemos:

$$10^0 \cdot \Gamma_0 = p \cdot k_0 + 1,$$

assim, no caso $i = 0$ obtemos a proposição.

Suponha agora $i = r$. Como $p \mid 9_r$, então, por definição de divisão, existe um único $k_r \in \mathbb{N}$ tal que:

$$9_r = p \cdot k_r,$$

como $9_r = 10^r - 1$, obtemos:

$$10^r = p \cdot k_r + 1.$$

Portanto, para $i = r$, obtemos $\Gamma_r = 1$ e a proposição é satisfeita.

Sendo assim, podemos supor que $1 < i < r$. Como, por hipótese, $p \mid 9_r$ segue que existe $k_r \in \mathbb{N}$ tal que:

$$9_r = p \cdot k_r.$$

Como $9_r = 10^r - 1$, obtemos:

$$10^r = p \cdot k_r + 1,$$

utilizando a Equação (4.1), temos que:

$$9_{r-i} \cdot 10^i + 9_i = p \cdot k_r. \tag{4.3}$$

Como 9_{r-i} é positivo, em virtude do Teorema da Divisão Euclidiana, Teorema 3.3, temos que existem únicos inteiros não negativos, u e v, de modo que:

$$9_{r-i} = p \cdot u + v;\ 0 \leq v \leq p - 1. \tag{4.4}$$

Note que, se $v = p - 1$ substituindo $9_r = 10^r - 1$ na Equação (4.4) obtemos que $p \mid 10^{r-i}$ e isso não pode ocorrer devido p ser um numero não divisível por 2 e por 5. Assim, temos que $0 \leq v < p - 1$.

Substituindo a Equação 4.3 na Equação 4.4 e somando e subtraindo o número 1 obtemos:

$$(p \cdot u + v) \cdot 10^i + 9_i + 1 - 1 \quad = \quad p \cdot k_r,$$

usando que $9_i + 1 = 10^i$, temos

$$(p \cdot u) \cdot 10^i + (v) \cdot 10^i + 10^i \quad = \quad p \cdot k_r + 1$$

e, portanto,

$$10^i \cdot (1 + v) \quad = \quad p \cdot (k_r - u \cdot 10^i) + 1.$$

Assim, podemos tomar $k_i = k_r - u \cdot 10^i$ e $\Gamma_i = 1 + v$ onde $0 < \Gamma_i < p$, os quais são únicos devido a unicidade do u e do v. Assim, garantimos que a proposição também ocorre para $1 < i < r$. Portanto, concluímos que a proposição é verdadeira para todo i inteiro, $0 \leq i \leq r$. ■

A Proposição 4.8 nos dá suporte para introduzir a seguinte definição:

Definição 13. *Sejam $r, p \in \mathbb{N}$, com $r < p$ e $mdc(p, 10) = 1$ e $p \mid 9_r$. Denotamos $\Gamma_0 = 1$, $k_0 = 0$ e definimos $\Gamma^{(p,r)} = (\Gamma_1, \Gamma_2, ..., \Gamma_r)$ e $K^{(p,r)} = (k_1, k_2, ..., k_r)$, cujas coordenadas satisfazem:*

$$0 < \Gamma_i < p \text{ e } 10^i \cdot \Gamma_i = p \cdot k_i + 1, \ \forall i = 1, 2, ..., r$$

Exemplo 4. *Podemos supor $p = 7$ e devido ao pequeno teorema de Fermat, $7 \mid 9_6$. Vamos determinar $\Gamma^{(7,6)}$ e $K^{(7,6)}$.*

Solução 1: Devemos ter que:

$$\Gamma^{(7,6)} = (\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Gamma_5, \Gamma_6) \text{ e } K^{(7,6)} = (k_1, k_2, k_3, k_4, k_5, k_6)$$

com

$$10^i \cdot \Gamma_i = 7 \cdot k_i + 1, \forall i = 1, 2, ..., 6. \tag{4.5}$$

Para $i = 6$, conforme Proposição 4.8, $k_6 = \dfrac{999999}{7} = 142857$ e $\Gamma_6 = 1$. Já no caso $1 \leq i \leq 5$, Sendo $9_{6-i} = 7 \cdot u + v$ com $0 \leq v \leq p - 1$, teremos que $k_i = k_6 - u \cdot 10^i$ e $\Gamma_i = 1 + v$. Dai, segue que:

(a) Para $i = 5$ obtemos $9_{6-5} = 9 = 7 \cdot 1 + 2$ e dai segue que $u = 1$ e $v = 2$. Logo, $k_5 = 142857 - 1 \cdot 10^5 = 42857$ e $\Gamma_5 = 3$.

(b) Para $i = 4$ obtemos $9_{6-4} = 99 = 7 \cdot 14 + 1$ e dai segue que $u = 14$ e $v = 1$. Logo, $k_4 = 142857 - 14 \cdot 10^4 = 2857$ e $\Gamma_4 = 2$.

(c) Para $i = 3$ obtemos $9_{6-3} = 999 = 7 \cdot 1 + 5$ e dai segue que $u = 142$ e $v = 5$. Logo, $k_3 = 142857 - 142 \cdot 10^3 = 857$ e $\Gamma_3 = 6$.

(d) Para $i = 2$ obtemos $9_{6-2} = 9999 = 7 \cdot 1428 + 3$ e dai segue que $u = 1428$ e $v = 3$. Logo, $k_2 = 142857 - 1428 \cdot 10^2 = 57$ e $\Gamma_2 = 4$.

(e) Para $i = 1$ obtemos $9_{6-1} = 99999 = 7 \cdot 14285 + 4$ e dai segue que $u = 14285$ e $v = 4$. Logo, $k_1 = 142857 - 1 \cdot 10^5 = 42857$ e $\Gamma_1 = 5$.

Assim, segue que $\Gamma^{(7,6)} = (5, 4, 6, 2, 3, 1)$ e $K^{(7,6)} = (7, 57, 857, 2857, 42857, 742857)$. ■

A Definição 13 será de grande utilidade para formação do Teorema do Período e no Teorema de Divisibilidade. Vale ressaltar que no Exemplo 4 podemos perceber que existiu uma relação entre k_i e k_{i-1} para todo i=1,2,...,6.

Note que para $p \in \mathbb{N}$, maior que 1 e $mdc(p, 10) = 1$, temos que $p \mid 9_r$ para $r \in \mathbb{N}$ menor que p e neste caso, definimos Γ_i e k_i para cada $i \leq r$, $i \in \mathbb{N}$. Com base na próxima definição, e Teorema do período, será definido Γ_i e k_i para $i \in \mathbb{Z}^+$.

Definição 14. *Sendo* $r, p \in \mathbb{N}$, $r < p$, $mdc(p, 10) = 1$, $p \mid 9_r$ *e* $k_r = \dfrac{9_r}{p}$. *Para todo* $m \in \mathbb{N}$ *definimos* $k_{r\cdot m} = k_r \cdot 10^{(m-1)\cdot r} + k_{r\cdot(m-1)}$.

O Teorema 4.9 foi chamado de Teorema do Período em virtude de apresentar a capacidade de Γ_i ter comportamento periódica, quando tomamos k_i com determinadas características na equação $10^i \cdot \Gamma_i = p \cdot k_i + 1$.

Teorema 4.9. *(Teorema do Período) Sejam* $r, p \in \mathbb{N}$, *tais que* $r < p$, $mdc(p, 10) = 1$ *e* $p \mid 9_r$. *Sejam,* $K^{(p,r)} = (k_1, k_2, ..., k_r)$ *e* $\Gamma^{(p,r)} = (\Gamma_1, \Gamma_2, ..., \Gamma_r)$. *Então, para todo* $m \in \mathbb{Z}^+$ *e cada inteiro* s, $1 \leq s \leq r$, *tomando* $k_{r\cdot m+s} = k_s \cdot 10^{m\cdot r} + k_{r\cdot m}$ *e* $\Gamma_{r\cdot m+s}$ *satisfazendo a equação* $10^{r\cdot m+s}\Gamma_{r\cdot m+s} = p \cdot k_{r\cdot m+s} + 1$ *teremos que* $\Gamma_{r\cdot m+s} = \Gamma_s$ *e* $p \cdot k_{r\cdot m} + 1 = 10^{r\cdot m}$.

Demonstração: Provaremos o Teorema, aplicando indução finita sobre m. Para $m = 0$ e Para todo $s = 1, 2, ..., r$ temos que:

$$k_{r\cdot m+s} = k_{r\cdot 0+s} = k_s \cdot 10^{0\cdot r} + k_{r\cdot 0} = k_s.$$

Substituindo $m = 0$ e $k_{r\cdot 0+s} = k_s$ na equação $10^{r\cdot m+s} \cdot \Gamma_{r\cdot m+s} = p \cdot k_{r\cdot m+s} + 1$ obtemos:

$$\begin{aligned} 10^s \cdot \Gamma_{r\cdot 0+s} &= p \cdot (k_s \cdot 10^0 + k_0) + 1 \\ &= p \cdot k_s + 1, \end{aligned}$$

como $K^{(p,r)} = (k_1, k_2, ..., k_r)$, $\Gamma^{(p,r)} = (\Gamma_1, \Gamma_2, ..., \Gamma_r)$ e $10^s\Gamma_s = p \cdot k_s + 1$, segue que:

$$\begin{aligned} 10^s \cdot \Gamma_{r\cdot 0+s} &= p \cdot k_s + 1 \\ &= 10^s \cdot \Gamma_s. \end{aligned}$$

Assim, segue para $m = 0$ que:

$$\Gamma_{r\cdot m+s} = \Gamma_s \text{ e } p \cdot (k_{r\cdot 0}) + 1 = 10^{r\cdot 0}.$$

Suponha, por hipótese de indução, que o resultado é válido para certo m inteiro não negativo, $m \geq 0$, ou seja, para cada $k_{r\cdot m+s} = k_s \cdot 10^{m\cdot r} + k_{r\cdot m}$ e $\Gamma_{r\cdot m+s}$ satisfazendo a equação $10^{r\cdot m+s}\Gamma_{r\cdot m+s} = p \cdot k_{r\cdot m+s} + 1$ obtemos que $\Gamma_{r\cdot m+s} = \Gamma_s$ e $p \cdot k_{r\cdot m} + 1 = 10^{r\cdot m}$, para todo $s = 1, 2, ..., r$.

Para $m+1$, mostraremos que dados $K^{(p,r)} = (k_1, k_2, ..., k_r)$, $\Gamma^{(p,r)} = (\Gamma_1, \Gamma_2, ..., \Gamma_r)$, para cada $k_{r\cdot(m+1)+s} = k_s \cdot 10^{(m+1)\cdot r} + k_{r\cdot(m+1)}$ e $\Gamma_{r\cdot(m+1)+s}$ que satisfazendo $10^{r\cdot(m+1)+s}$. $\Gamma_{r\cdot(m+1)+s} = p \cdot k_{r\cdot(m+1)+s} + 1$ obtemos que $\Gamma_{r\cdot(m+1)+s} = \Gamma_s$ e $p \cdot k_{r\cdot(m+1)} + 1 = 10^{r\cdot(m+1)}$, para todo $s = 1, 2, ..., r$.

Provaremos primeiro que para $m + 1$ temos que $p \cdot k_{r\cdot(m+1)} + 1 = 10^{r\cdot(m+1)}$. Note que por definição, $k_{r\cdot m+r} = k_{r\cdot(m+1)} = k_r \cdot 10^{r\cdot m} + k_{r\cdot m}$. Podemos multiplicar por

p cada membro desta ultima igualdade, somar o número 1 em cada um dos lados desta igualdade para obter:

$$p \cdot k_{r\cdot(m+1)} + 1 \quad = \quad p \cdot k_r \cdot 10^{r\cdot m} + p \cdot k_{r\cdot m} + 1, \tag{4.6}$$

Por hipótese de indução temos que $p \cdot k_{r\cdot m} + 1 = 10^{r\cdot m}$, assim a Equação (4.6) é equivalente a:

$$\begin{aligned} p \cdot k_{r\cdot(m+1)} + 1 &= p \cdot k_r \cdot 10^{r\cdot m} + 10^{r\cdot m} \\ &= 10^{r\cdot m} \cdot (p \cdot k_r + 1), \end{aligned}$$

usando a Definição 13, temos que $p \cdot k_r + 1 = 10^r \cdot \Gamma_r$ e combinando este fato com a hipótese de $p \mid 9_r$, teremos que $\Gamma_r = 1$. Assim, segue que $p \cdot k_r + 1 = 10^r$ e obtemos nesta última igualdade que:

$$p \cdot k_{r\cdot(m+1)} + 1 \quad = \quad 10^{r\cdot m} \cdot 10^r$$

logo,

$$p \cdot k_{r\cdot(m+1)} + 1 \quad = \quad 10^{r\cdot(m+1)}. \tag{4.7}$$

Assim, falta mostrar somente que para cada $k_{r\cdot(m+1)+s} = k_s \cdot 10^{(m+1)\cdot r} + k_{r\cdot(m+1)}$ e $\Gamma_{r\cdot(m+1)+s}$ que satisfaz a equação

$$10^{r\cdot(m+1)+s} \cdot \Gamma_{r\cdot(m+1)+s} = p \cdot (k_s \cdot 10^{r\cdot(m+1)} + k_{r\cdot(m+1)}) + 1,$$

obtemos $\Gamma_{r\cdot(m+1)+s} = \Gamma_s$.

De fato:

$$\begin{aligned} 10^{r\cdot(m+1)+s}\Gamma_{r\cdot(m+1)+s} &= p \cdot (k_s \cdot 10^{r\cdot(m+1)} + k_{r\cdot(m+1)}) + 1 \\ &= p \cdot k_s \cdot 10^{r\cdot(m+1)} + p \cdot k_{r\cdot(m+1)} + 1. \end{aligned}$$

Utilizando a Equação (4.7) temos que $p \cdot k_{r\cdot(m+1)} + 1 = 10^{r\cdot(m+1)}$, assim obtemos:

$$10^{r\cdot(m+1)+s}\Gamma_{r\cdot(m+1)+s} = p \cdot k_s \cdot 10^{r\cdot(m+1)} + 10^{r\cdot(m+1)}.$$

Dividindo ambos os lados desta última igualdade por $10^{r\cdot(m+1)}$ obtemos:

$$10^s \cdot \Gamma_{r\cdot(m+1)+s} \quad = \quad p \cdot k_s + 1.$$

Como $0 < s < r$, temos que $p \cdot k_s + 1 = 10^s \cdot \Gamma_s$, obtemos:

$$10^s \cdot \Gamma_{r\cdot(m+1)+s} \quad = \quad 10^s \cdot \Gamma_s.$$

Assim, para $m+1$ e para todo $s = 1, 2, ..., r$ temos que:

$$\Gamma_{r\cdot(m+1)+s} = \Gamma_s \text{ e } p \cdot k_{r\cdot(m+1)} + 1 = 10^{r\cdot(m+1)}.$$

Provando a validade para o caso $m+1$, segue pelo princípio da indução finita que o resultado vale para todo m não negativo e cada $1 < s < r$. ■

A partir do Teorema do Período, podemos generalizar os valores numéricos de Γ_i e k_i, apresentados na Definição 13, para $i \in \mathbb{Z}^+$.

Definição 15. *Sejam $p, r, \in \mathbb{N}$, tais que $r < p$, $mdc(p, 10) = 1$ e $p \mid 9_r$. Sejam $\Gamma^{(p,r)} = (\Gamma_1, \Gamma_2, ..., \Gamma_r)$ e $K^{(p,r)} = (k_1, k_2, ..., k_r)$, cujas coordenadas satisfazem:*

$$0 < \Gamma_j < p \text{ e } 10^j \cdot \Gamma_j = p \cdot k_j + 1, \forall j = 1, 2, ..., r.$$

Para $m, s, i \in \mathbb{Z}^+$ com $1 \leq s \leq r$ e $i = r \cdot m + s$ definimos $k_0 = 0$, $\Gamma_0 = 1$, $k_i = k_s \cdot 10^{m\cdot r} + k_{r\cdot m}$ e Γ_i que satisfazem $10^i \cdot \Gamma_i = p \cdot k_i + 1$.

Se $p \mid 9_r$, para algum r, tal que $1 \leq r \leq p-1$, temos que $k_r = \dfrac{9_r}{p}$ e $\Gamma_r = 1$. Assim, o resultado a seguir é verdadeiro:

Proposição 4.10. *Sejam $p, r \in \mathbb{N}$, tais que $r < p$, $mdc(p, 10) = 1$, $p \mid 9_r$ e k_i e Γ_i conforme Definição 15. Se r é par e $s = \dfrac{r}{2}$ com $mdc(p, 9_s) = 1$, então $\Gamma_s = p - 1$.*

Demonstração: De fato,

$$10^r \cdot 1 = p \cdot k_r + 1 \tag{4.8}$$

e

$$10^s \cdot \Gamma_s = p \cdot k_s + 1, \text{ com } 0 < \Gamma_s < p. \tag{4.9}$$

multiplicando ambos os lados da Equação (4.9) por 10^s e combinando isto com a Equação (4.8) obtemos:

$$10^r \cdot 1 + (10^s \cdot 10^s \cdot \Gamma_s) = p \cdot k_r + 1 + (10^s \cdot p \cdot k_s + 10^s),$$

como $10^s \cdot 10^s = 10^r$, já que $s = \dfrac{r}{2}$, obtemos a partir desta última igualdade que:

$$10^r \cdot (1 + \Gamma_s) = p \cdot (k_r + 10^s \cdot k_s) + 10^s + 1, \tag{4.10}$$

multiplicando cada lado da Equação (4.10) por 9_s obtemos:

$$\begin{aligned} 9_s \cdot 10^r \cdot (1 + \Gamma_s) &= 9_s \cdot p \cdot (k_r + 10^s \cdot k_s) + 9_s \cdot 10^s + 9_s \\ &= p \cdot (9_s \cdot k_r + 9_s \cdot 10^s \cdot k_s) + 9_r, \end{aligned}$$

Da Equação (4.8) temos que $9_r = p \cdot k_r$, logo:

$$\begin{aligned} 9_s \cdot 10^r \cdot (1 + \Gamma_s) &= 9_s \cdot p \cdot (k_r + 10^s \cdot k_s) + p \cdot k_r \\ &= p \cdot (9_s \cdot k_r + 9_s \cdot 10^s \cdot k_s + k_r). \end{aligned}$$

Dai, segue que $p \mid (9_s \cdot 10^r \cdot (1+\Gamma_s))$. Como $mdc(p, 9_s \cdot 10^r) = 1$ segue que $p \mid (1+\Gamma_s)$. Devido $0 < \Gamma_s < p$ e $p \mid (1 + \Gamma_s)$, teremos que:

$$\Gamma_s + 1 = p.$$

Portanto, segue que $\Gamma_s = p - 1$. ■

Na seção seguinte, utilizaremos o teorema do período provado anteriormente para construir, e demonstrar, o Teorema de divisibilidade.

4.3 Teorema de Divisibilidade

Nesta seção, provaremos o resultado principal deste capítulo, que é um Teorema de Divisibilidade. Este resultado proporciona decidir se números dividem, ou não, um $\bar{x}_n$ a partir da combinação linear dos seus algarismos. O resultado possui o seguinte enunciado:

Teorema 4.11. *(Teorema de Divisibilidade) Seja $\bar{x}_n$ um inteiro positivo de n algarismos e $p, r \in \mathbb{N}$, tais que $r < p$, $mdc(p, 10) = 1$ e $p \mid 9_r$. Seja $i \in \mathbb{N}$ com $0 < i < n$, $x_{n|i}$ os $n - i$ primeiros algarismos de $\bar{x}_n$ e $x_{i|i}$ os i últimos algarismos de $\bar{x}_n$. Então:*

$$p \mid \bar{x}_n \text{ se, e somente se, } p \mid (x_{n|i} + \Gamma_i \cdot x_{i|i}).$$

Demonstração: Suponha inicialmente que $p \mid \bar{x}_n$:
Podemos escrever $\bar{x}_n$ como:

$$\bar{x}_n = 10^i \cdot x_{n|i} + x_{i|i}, \text{ onde } 0 < i < n.$$

Como p divide $\bar{x}_n$, temos que, existe $u \in \mathbb{N}$ de modo que $\bar{x}_n = p \cdot u$, logo:

$$p \cdot u = 10^i \cdot x_{n|i} + x_{i|i}.$$

Isolando $x_{n|i}$ em um dos lados da igualdades teremos que:

$$x_{n|i} = \frac{p \cdot u - x_{i|i}}{10^i}. \tag{4.11}$$

Como $10^i \cdot \Gamma_i = p \cdot k_i + 1$, vamos somar $\Gamma_i \cdot x_{i|i}$ em ambos os membros da Equação (4.11) e obtemos:

$$x_{n|i} + \Gamma_i \cdot x_{i|i} = \frac{p \cdot u - x_{i|i}}{10^i} + \Gamma_i \cdot x_{i|i}.$$

Multiplicando os dois lados da última igualdade por 10^i e colocando em evidência o $x_{i|i}$ no segundo lado da última igualdade, obtemos:

$$(x_{n|i} + \Gamma_i \cdot x_{i|i}) \cdot 10^i = p \cdot u + x_{i|i} \cdot (10^i \cdot \Gamma_i - 1).$$

Como $10^i \cdot \Gamma_i - 1 = p \cdot k_i$, segue que:

$$\begin{aligned}(x_{n|i} + \Gamma \cdot x_{i|i}) \cdot 10^i &= p \cdot u + x_{i|i} \cdot (p \cdot k_i) \\ &= p \cdot (u + x_{i|i} \cdot k_i).\end{aligned}$$

Dessa forma, temos que p divide o produto $(x_{n|i} + \Gamma \cdot x_{i|i}) \cdot 10^i$ e como $p \nmid 10^i$, pois $mdc(p, 10) = 1$, segue que $p \mid (x_{n|i} + \Gamma_i \cdot x_{i|i})$.
Reciprocamente, se $p \mid (x_{n|i} + \Gamma \cdot x_{i|i})$ para $0 < i < n$, teremos pela definição de divisibilidade, que existe um inteiro u onde $p \cdot u = (x_{n|i} + \Gamma \cdot x_{i|i})$ e sendo $10^i \cdot \Gamma_i = p \cdot k_i + 1$, segue que,

$$\begin{aligned}p \cdot u \cdot 10^i &= 10^i \cdot x_{n|i} + 10^i \cdot \Gamma \cdot x_{i|i} \\ &= 10^i \cdot x_{n|i} + (p \cdot k_i + 1) \cdot x_{i|i}.\end{aligned}$$

Daí, segue que,

$$\begin{aligned}p \cdot u \cdot 10^i - p \cdot k_i \cdot x_{i|i} &= 10^i \cdot x_{n|i} + x_{i|i} \\ &= \bar{x}_n\ .\end{aligned}$$

Assim, obtemos que $p \mid \bar{x}_n$. ■

Note que analisando o Teorema do Período para certo $p \in \mathbb{N}$ que atende as condições do Teorema 4.9, temos que o Teorema de Divisibilidade terá sua aplicação com maior eficiência quando $r \in \mathbb{N}$ é o menor número possível de modo que $p \mid 9_r$. Esse fato é verdadeiro em virtude de quanto menor for r, menor será a quantidade

de r-uplas de $\Gamma^{(p,r)}$ e consequentemente será menor o período de Γ_i para $i \in \mathbb{N}$. Encerraremos o capítulo apresentando uma aplicação do Teorema de divisibilidade.

Exemplo 5. *: O número $\bar{x}_n$ que tem todos os seus algarismos iguais a 8, onde $n = 6 \cdot 23571113171923293137417535961677181 7$, é um número divisível por 91?*

Solução: Note que $91 = 7 \cdot 13$, $7 \mid 9_6$, $13 \mid 9_6$ e assim $91 \mid 9_6$. como 9_6 é o menor número com todos os algarismos iguais a 9 que é divisível tanto por 7 quanto por 13, segue que ele também será o menor em que 91 divide. Sendo assim, temos que Γ_i terá período igual a 6 com $\Gamma^{(91,6)} = (\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Gamma_5, 1)$.

Temos que $mdc(91, 9_3) = 1$, pois 9_6 é o menor número de todos os algarismos iguais a 9 onde $91 \mid 9_6$, e assim usando a Proposição 4.10 obtemos que $\Gamma_3 = 91 - 1$. Tomando $i = \dfrac{n}{2}$ segue que ($x_{n|i} = x_{i|i}$, i é um número do tipo $6 \cdot m + 3$ e aplicando o Teorema da divisibilidade, Teorema 4.11, teremos que:

$$91 \mid \bar{x}_n \text{ se, e somente se, } 91 \mid (x_{n|i} + 90 \cdot x_{i|i}).$$

Da Proposição 3.2, $91 \mid (x_{n|i} + 90 \cdot x_{i|i})$ se, e somente se, $91 \mid (x_{n|i} - (91 - 90) \cdot x_{i|i})$. Logo:

$$91 \mid \bar{x}_n \text{ se, e somente se, } 91 \mid (x_{n|i} - x_{i|i}).$$

Como $x_{n|i} = x_{i|i}$ segue que:

$$91 \mid \bar{x}_n \text{ se, e somente se, } 91 \mid 0.$$

Como 91 divide 0, segue que $91 \mid \bar{x}_n$. ■

No capítulo seguinte faremos mais aplicações do teorema de divisibilidade em critérios de divisibilidade.

Capítulo 5

Critérios de Divisibilidade

Nesse Capítulo faremos aplicações do Teorema de Divisibilidade afim de estabelecer Critérios de Divisibilidade. Além disso, provaremos o Teorema da Infinitude dos Números Primos como aplicação dos resultados apresentados anteriormente.

Com base no livro do autor [4], p. 22, temos que:

Proposição 5.1. *Um número inteiro positivo n será divisível por 7 se, e somente se, a diferença entre o dobro do primeiro algarismo com o número formado pelos demais algarismos de n é divisível por 7*

Para números grandes, assim como 671.050.273.981.553.126.377.328.955, esse critério deverá ser aplicado muitas vezes para sabermos se 7 o divide. Assim, a seguir apresentaremos critérios de divisibilidade para 7 e para 13, utilizando como fundamento o teorema de divisibilidade, Teorema 4.11.

Proposição 5.2 (Critério de divisibilidade por 7)**.** *Sejam $n, i \in \mathbb{N}$ com $i < n$. Um número inteiro positivo de n algarismos será divisível por 7 se, e somente se, $x_{n|i} + l_i \cdot x_{i|i}$ é divisível por 7 com:*

(a) $l_i = -2$, *se* $i = 6 \cdot m + 1$ *para certo* $m \in \mathbf{Z}^+$.

(b) $l_i = -3$, *se* $i = 6 \cdot m + 2$ *para certo* $m \in \mathbf{Z}^+$.

(c) $l_i = -1$, *se* $i = 6 \cdot m + 3$ *para certo* $m \in \mathbf{Z}^+$.

(d) $l_i = 2$, *se* $i = 6 \cdot m + 4$ *para certo* $m \in \mathbf{Z}^+$.

(e) $l_i = 3$, *se* $i = 6 \cdot m + 5$ *para certo* $m \in \mathbf{Z}^+$.

(f) $l_i = 1$, *se* $i = 6 \cdot m + 6$ *para certo* $m \in \mathbf{Z}^+$.

Demonstração: Fazendo $p = 7$ no Teorema de Divisibilidade, Teorema 4.11, segue que:

$$7 \mid \bar{x}_n \text{ se, e somente se, } 7 \mid (x_{n|i} + \Gamma_i \cdot x_{i|i}).$$

Devido $7 \mid 9_6$ e $\Gamma^{(7,6)} = (5, 4, 6, 2, 3, 1)$ temos que:

(I) $\Gamma_i = 5$, se $i = 6 \cdot m + 1$ para certo $m \in \mathbf{Z}^+$.

(II) $\Gamma_i = 4$, se $i = 6 \cdot m + 2$ para certo $m \in \mathbf{Z}^+$.

(III) $\Gamma_i = 6$, se $i = 6 \cdot m + 3$ para certo $m \in \mathbf{Z}^+$.

(IV) $\Gamma_i = 2$, se $i = 6 \cdot m + 4$ para certo $m \in \mathbf{Z}^+$.

(V) $\Gamma_i = 3$, se $i = 6 \cdot m + 5$ para certo $m \in \mathbf{Z}^+$.

(VI) $\Gamma_i = 1$, se $i = 6 \cdot m + 6$ para certo $m \in \mathbf{Z}^+$.

Da Proposição 3.2, $7 \mid (x_{n|i} + \Gamma_i \cdot x_{i|i})$ se, e somente se, $7 \mid (x_{n|i} - (7 - \Gamma_i) \cdot x_{i|i})$.

Assim, temos que $7 \mid \bar{x}_n$ se, e somente se $7 \mid (x_{n|i} + (\Gamma_i) \cdot x_{i|i})$ e $7 \mid \bar{x}_n$ se, e somente se $7 \mid (x_{n|i} - (7 - \Gamma_i) \cdot x_{i|i})$. Portanto, para $0 < \Gamma_i < 4$ tome $l_i = \Gamma_i$ e para $3 < \Gamma_i < 7$ tome $l_i = \Gamma_i - 7$ e obtemos:

(a) $l_i = -2$, se $i = 6 \cdot m + 1$ para certo $m \in \mathbf{Z}^+$.

(b) $l_i = -3$, se $i = 6 \cdot m + 2$ para certo $m \in \mathbf{Z}^+$.

(c) $l_i = -1$, se $i = 6 \cdot m + 3$ para certo $m \in \mathbf{Z}^+$.

(d) $l_i = 2$, se $i = 6 \cdot m + 4$ para certo $m \in \mathbf{Z}^+$.

(e) $l_i = 3$, se $i = 6 \cdot m + 5$ para certo $m \in \mathbf{Z}^+$.

(f) $l_i = 1$, se $i = 6 \cdot m + 6$ para certo $m \in \mathbf{Z}^+$.

■

Vamos verificar como exemplo que o número 671.050.273.981.553.126.377.328.955 é divisível por 7. Como $7 \mid 9_6$, temos que $\Gamma^{(7,6)} = (5, 4, 6, 2, 3, 1)$ e devido este número ter 27 algarismos, ele é um $\bar{x}_{27}$ então:
Para $i = 12$, temos que $671050273981553 + 126377328955 = 671176651310508 = \bar{x}_{15}$
Para $i = 6$, temos que $671176651 + 310508 = 671487159 = \bar{x}_9$
Para $i = 3$, temos que $671487 - 159 = 671328 = \bar{x}_6$
Para $i = 3$, temos que $671 - 328 = 343 = \bar{x}_3$
Para $i = 1$, temos que $34 - 2 \cdot 3 = 28 = \bar{x}_2$
Como 7 divide 28 segue que 7 divide 671050273981553126377328955.

Proposição 5.3 (Critério de divisibilidade por 13)**.** *Sejam $n, i \in \mathbb{N}$ com $i < n$. Um número inteiro positivo de n algarismos será divisível por 13 se, e somente se, $x_{n|i} + l_i \cdot x_{i|i}$ é divisível por 13 com:*

(a) $l_i = 4$, *se* $i = 6 \cdot m + 1$ *para certo* $m \in \mathbb{Z}^+$.

(b) $l_i = 3$, *se* $i = 6 \cdot m + 2$ *para certo* $m \in \mathbb{Z}^+$.

(c) $l_i = -1$, *se* $i = 6 \cdot m + 3$ *para certo* $m \in \mathbb{Z}^+$.

(d) $l_i = -4$, *se* $i = 6 \cdot m + 4$ *para certo* $m \in \mathbb{Z}^+$.

(e) $l_i = 10$, *se* $i = 6 \cdot m + 5$ *para certo* $m \in \mathbb{Z}^+$.

(f) $l_i = 1$, *se* $i = 6 \cdot m + 6$ *para certo* $m \in \mathbb{Z}^+$.

Demonstração: Análoga a demonstração do critério de divisibilidade por 7, levando em consideração que $13 \mid 9_6$. ■

Vamos verificar que o número 671050273981553126377328955 não é divisível por 13:
Para $i = 12$, temos que $671050273981553 + 126377328955 = 671176651310508$
Para $i = 6$, temos que $671176651 + 310508 = 671487159$
Para $i = 3$, temos que $671487 - 159 = 671328$
Para $i = 3$, temos que $671 - 328 = 343$
Para $i = 1$, temos que $34 + 4 \cdot 3 = 46$
Como 13 não divide 46 segue que 13 não divide 671050273981553126377328955. ■

Vamos verificar que o número 671.050.273.981.553.126.377.328.955 não é divisível por 19. Temos certamente que $19 \mid 9_{18}$, pelo Pequeno Teorema de Fermat. Vamos fazer os cálculos para determinar alguns valores de Γ_i e aplicar o Teorema da Divisibilidade, Teorema 4.11:
Para $i = 1$, temos que $k_1 = 1$ e obtemos $\Gamma_1 = 2$.
Para $i = 2$, temos que $k_2 = 21$ e obtemos $\Gamma_2 = 4$.
Para $i = 3$, temos que $k_3 = 421$ e obtemos $\Gamma_3 = 8$.
Para $i = 4$, temos que $k_4 = 8421$ e obtemos $\Gamma_4 = 16$.
Para $i = 5$, temos que $k_5 = 68421$ e obtemos $\Gamma_5 = 13$.
Para $i = 10$, temos que $k_{10} = 8947368421$ e obtemos $\Gamma_{10} = 17$.
Olhando para estes valores teremos que 19 irá dividir este número $\bar{x}_{27}$ se, e somente se, 19 divide $x_{27|10} + 17 \cdot x_{10|10}$ ou de maneira equivalente, utilizando a Proposição 3.2 segue que 19 divide $x_{27|10} + 2 \cdot x_{10|10}$. Dai, temos que:
Para $i = 10$, temos que $67105027398155312 - 2 \cdot 6377328955) = 67105014643497402$
Para $i = 10$, temos que $6710501 - 2 \cdot 4643497402 = -9280284303$
Para $i = 5$, temos que $92802 - 6 \cdot 84303 = -413016$
Para $i = 3$, temos que $413 + 8 \cdot (016) = 541$
Para $i = 1$, temos que $54 - 17 \cdot 1 = 37$
Como 19 não divide 37 segue que 19 não divide 671.050.273.981.553.126.377.328.955.

Teorema 5.4. *(Infinitude dos Números Primos) Existem infinitos números Primos*

Demonstração: Suponha, por absurdo, que a quantidade de números primos é finita. Cada número primo p, diferente de 2 e de 5, divide 9_{p-1}. Como a quantidade de primos maiores que 5 é finita, suponha que esta quantidade é n e que p_n é o maior de todos. Sendo $s = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_n - 1)$ teremos que $9_s + 2 = u \cdot v$ para um u primo ímpar e v inteiro diferente de 1. Como $u \mid 9_{u-1}$, segue que $u \mid 9_s$ o que acarreta $u \mid 2$. Como chegamos a um absurdo, segue que existem infinitos números primos. ■

Finalizamos aqui as aplicações do Teorema de divisibilidade. Podemos perceber que ele é uma ferramenta que permite demonstrar alguns resultados de aritmética, principalmente na parte de critérios de divisibilidade.

Capítulo 6

Considerações Finais

Diante do que foi apresentado, comprovamos que é possível obter um Teorema de divisibilidade nos inteiros que permite determinar a partir da combinação dos algarismos de um número $\bar{x}_m$, de m algarismos, a divisibilidade deste por um inteiro n. Vale ressaltar que uma das principais dificuldades para encontrar uma combinação eficiente e prática, foi a obtenção do Teorema do Período, já que este resultado viabiliza e dá sentido ao Teorema de Divisibilidade.

Podemos destacar como principal aplicação deste resultado, a obtenção de critérios de divisibilidade. Além disso, observamos na aplicação do resultado que escolhendo adequadamente a quantidade de algarismos, podemos diminuir rapidamente a quantidade dos algarismos da combinação, fazendo apenas cálculos de soma ou subtração.

Vale ressaltar que os resultados no Capítulo 4 podem ser aplicados à Aritmética, como mostrado, apresentamos uma demonstração do Teorema da infinitude dos Números Primos.

Referências Bibliográficas

1 LIMA, E. L. *Curso de Análise Volume 1*. 14. ed. Rio de Janeiro, RJ: IMPA, 2017.

2 HEFEZ, A. *Aritmética, Coleção PROFMAT*. 2. ed. Rio de Janeiro, RJ: SBM, 2017.

3 RIBENBOIM, P. *Números Primos. Velhos Mistérios e Novos Recordes*. 1. ed. Rio de Janeiro, RJ: IMPA, 2014.

4 SANTOS, J. P. de O. *Introdução à Teoria dos Números*. 3. ed. Rio de Janeiro, RJ: IMPA, 2010.