Universidade Federal Rural de Pernambuco
Departamento de Matemática
Mestrado Profissional em Matemática

MÉTODOS GERADORES DE CRITÉRIOS DE DIVISIBILIDADE

Cícero Carlos Ramos de Brito

Orientador
Prof. Dr. Thiago Dias Oliveira Silva

Recife-PE

Agosto de 2017

Universidade Federal Rural de Pernambuco
Departamento de Matemática
Mestrado Profissional em Matemática

MÉTODOS GERADORES DE CRITÉRIOS DE DIVISIBILIDADE

Dissertação apresentada à Universidade Federal Rural de Pernambuco, para obtenção do título de Mestre em Matemática Profissional, Área de Concentração: Matemática Teórica.

Cícero Carlos Ramos de Brito

Recife-PE

Agosto de 2017

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Nome da Biblioteca, Recife-PE, Brasil

B862m Brito, Cícero Carlos Ramos de
Métodos geradores de critérios de divisibilidade / Cícero Carlos Ramos de Brito. – 2017.
92 f. : il.

Orientador: Thiago Dias Oliveira Silva.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Mestrado Profissional em Matemática, Recife, BR-PE, 2017.
Inclui referências e apêndice(s).

1. Divisibilidade 2. Critérios de divisibilidade 3. Métodos geradores 4. Métodos construtores 5. Teoria dos números I. Silva, Thiago Dias Oliveira, orient. II. Título

CDD 510

CÍCERO CARLOS RAMOS DE BRITO

Métodos Geradores de Critérios de Divisibilidade

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 25/08/2017

BANCA EXAMINADORA

Thiago Dias Oliveira Silva

Prof. Dr. Thiago Oliveira Dias Silva (Orientador(a))– UFRPE

Eudes Naziazeno Galvão

Prof. Dr. Eudes Naziazeno Galvão – DMAT-UFPE

Prof. Dr. Rodrigo José Gondim Neves– PROFMAT/UFRPE

As duas mulheres da minha vida, minha mãe D. Severina Ramos de Brito (in memorian) e, minha esposa Bárbara Christina Silva de Brito.

Dedico.

"É muito melhor lançar-se em busca de conquistas grandiosas, mesmo expondo-se ao fracasso, do que alinhar-se com os pobres de espírito, que nem gozam muito nem sofrem muito, porque vivem numa penumbra cinzenta, onde não conhecem nem vitória, nem derrota."

Theodore Roosevelt

Agradecimentos

Ao meu bom Deus, por estar sempre presente nos momentos de alegrias e dificuldades.

À minha família, pois, sem ela não teria conseguido vencer mais esta batalha.

À Universidade Federal Rural de Pernambuco, em especial ao Departamento de Matemática, por ter dado todas as condições necessárias para a realização do presente trabalho.

Ao Professor Doutor Thiago Dias Oliveira Silva, pela dedicação, ensinamentos, confiança, amizade e paciência sempre concedida.

À Coordenação do Programa de Pós Graduação em Matemática Profissional, por ter dado todas as condições necessárias para o desenvolvimento do curso.

A todos os Professores do Programa de Pós Graduação em Matemática Profissional que, diretamente ou indiretamente, contribuíram para o meu sucesso.

Aos professores e amigos, José de Arimatéa Rocha, Ricardo Normando e João Silva Rocha pelo apoio e incentivo a este trabalho.

Resumo

Na presente dissertação intitulada Métodos Geradores de Critérios de Divisibilidade, temos por objetivo apresentar métodos para generalizar e estender os processos da obtenção de critérios de divisibilidade. São propostos dois métodos geradores e dois métodos construtores fundamentados em teoremas aqui demonstrados. Neste trabalho compilamos algumas ideias que aparecem na literatura, com isso damos suporte ao professor do ensino básico para gerar e construir critérios de divisibilidade, diferente ou não, dos que são comumente apresentados na educação básica.
Palavras-chave: divisibilidade, critérios de divisibilidade, métodos geradores, métodos construtores, teoria dos números.

Abstract

In this dissertation entitled Generating Methods Divisibility Criteria, we aim to demonstrate methods to generate and extend the processes of acquiring divisibility criteria. We propose two generating methods and two constructor methods based on theorems demonstrated in this work. We, still, compile some ideas that exist in the mathematical literature. With that we give support to teachers of primary and high school to generate and build divisibility criteria, different or not, of those which are normally taught at those education levels.

Keywords: Divisibility. Divisibility criteria. Generating Methods. Constructors methods. Number theory.

Sumário

Capítulo 1

INTRODUÇÃO

A matemática é de uma enorme importância para a sociedade, pela utilidade e oportunidades que oferece para a criação e a descoberta assim como pelo seu uso na vida pessoal, social e econômica. Seu crescimento é bastante rápido e contínuo, satisfazendo tanto a curiosidade quanto às necessidades de aplicação (engenharia, economia, estatística, física, química, entre outros). A mesma proporciona aos estudantes desenvolverem processos sistemáticos para tratar problemas, sejam ou não, de rotina ou de soluções imediatamente determináveis.

Contudo, muito do desenvolvimento matemático é determinado pela pesquisa com foco em sua própria internalização, isto é, em busca de autorregulação do seu status de ciência. Assim é que, por exemplo, na teoria dos números muitos resultados surgiram a partir de problemas internos. É o caso da busca por critérios que indiquem a divisibilidade de um número dado por outro fixado. Nossa preocupação inicial se deveu a análise de tais critérios.

Assim, nossa motivação foi dada pela necessidade e curiosidade de entendermos de forma mais profunda os critérios de divisibilidades, justamente para compilar o existente na literatura buscando apontar seu amplo desenvolvimento nos livros do ensino fundamental, médio ou superior.

Deste modo, o objetivo geral deste trabalho é deduzir métodos geradores de critérios de divisibilidade, e os objetivos específicos são:

- Servir como material de pesquisa para estudantes e professores interessados em desvendar um pouco da teoria dos números;

- Deduzir métodos construtores de critérios de divisibilidade, para números com dois dígitos ou mais que são simples de aplicar;

- Construir métodos tanto geradores como construtores de critérios de divisibilidades especiais (casos especiais ou específicos);

O capítulo 2 uma revisão de literatura em que, a partir de elementos históricos da teoria dos números apresentaremos dados básicos para o corpo da dissertação.

O capítulo 3 trará, por ordem de compreensão, os resultados centrais obtidos, cercados de exemplos significativos para seu completo entendimento. Entre tais resultados, queremos salientar o corolário 2 do Teorema 3.1 (Método Gerador de Critérios de Divisibilidade do tipo Alfa) qual nos conduz a um método iterativo de divisibilidade suficientemente geral e de convergência relativamente rápida, como será visto.

Avançando nesta ideia, obtemos um método gerador de critérios de divisibilidade (Teorema 3.2) o qual produz diversos corolários indicativos de tais construções, a partir do algarismo das unidades dos números a serem analisados, no caso, números terminados em 1, 3, 7 ou 9.

No capítulo 4, faremos nossas conclusões, absorvendo as contribuições obtidas e indicando possibilidades para futuros trabalhos.

Assim, esperamos apresentar um texto que servirá de consulta, especialmente sob o aspecto didático, para professores e estudantes de matemática. Aliás, a preocupação maior foi buscar explicar o porquê de certos procedimentos e algoritmos usados desde muito cedo no ensino de matemática e, em determinadas vezes, de maneira puramente mecânica.

Quando pensamos em critérios de divisibilidade, em geral vem a nossa cabeça os clássicos critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11. Isso porque em geral, livros de álgebra abstrata introdutórios, ou livros didáticos do ensino médio trazem os critérios de divisibilidade de números inteiros e apresentam técnicas para determinar quando um número é divisível por outro, sempre no sistema numérico decimal.

No apêndice à página 75 o leitor poderá encontrar uma série de questões propostas para exercitar os métodos desenvolvidos ao longo do texto.

Por outro lado, a aritmética modular permite fazer essa análise para qualquer par de números inteiros e a facilidade ou dificuldade de um critério de divisibilidade de um número por outro está intimamente ligada a base numérica na qual esses números estão representados.

Percebamos ainda que ao trabalhar com o sistema de numeração decimal, sabemos que o resto da divisão de número inteiro n por 9, é o mesmo resto da soma dos seus dígitos, em outras palavras, o número será divisível por 9 se e somente se a soma de seus dígitos for divisível por 9. A pergunta que fazemos é a seguinte: se mudarmos a base de representação de um número, o que podemos dizer sobre os critérios de divisibilidade nessa nova base? Para quais números temos critérios de divisibilidade mais fáceis de serem verificados? Nossa intenção é estender o raciocínio para uma base numérica k genérica e verificar o que é de fato geral e o que é intrínseco da base numérica escolhida.

Capítulo 2

REVISÃO DE LITERATURA

Atualmente já que existem as calculadoras, os computadores e os celulares, desta forma, este trabalho aparentemente não traz nenhuma contribuição prática para os leitores (ou alunos). Por outro lado, caso este trabalho tivesse sido escrito numa época em que não existiam essas máquinas, provavelmente, a contribuição ao ensino da matemática seria muito maior que a apresentada hoje.

Vale salientar que, apesar do exposto anteriormente, o forte deste trabalho é a contribuição teórica para a matemática, sendo possível implementar algoritmos computacionais para resolver problemas de teoria dos números, relacionados com congruência modular, que vai apontando, também, sua aplicabilidade para o ensino da matemática no ensino básico e também no ensino superior.

2.1 Histórico

O escopo deste trabalho encontra sua base na chamada teoria dos números. Esta, juntamente com a geometria, tem sua organização inicial a partir dos elementos de Euclides, por volta do século III A.C. Nota-se que à época, a matemática grega não contava com uma representação numérica que permitisse grandes avanços na compreensão dos sistemas numéricos, sendo a aritmética tratada a partir de dados geométricos, como ocorre com a teoria das proporções e o estudo dos incomensuráveis em Euclides, em que pese o fato de a demonstração encontrada no livro IX de Euclides de que o conjunto dos números primos é infinito ser "considerada universalmente como um modelo de elegância matemática" (EVES, P. 175).

O desenvolvimento histórico da matemática a partir de Euclides, segue uma rota muito delineada pela centralidade da Grécia no plano cultural, mas que vai sofrendo influência de outras culturas como a Hindu, por exemplo, convergindo para a Europa Ocidental, berço da modernidade matemática. Ali, na chamada idade média, o gênio de Fibonacci (1175 - 1250) que tivera passagem pelo norte da África, faz surgir outro texto singular da matemática: O Liber Abaci, obra com muita influência da matemática árabe e que traz, entre outras contribuições, a escrita e a leitura dos novos numerais, fato que vai propiciar um desenvolvimento ímpar para a aritmética.

De fato, o renascimento europeu após a queda de Constantinopla em 1453, traz em si, um revigoramento intelectual que se faz sentir na matemática (EVES, 2008). De modo que "como consequência do interesse pela educação e do crescimento enorme da atividade comercial no renascimento, começaram a surgir muitos textos populares de aritmética" (EVES, p. 299).

Entre estas aritméticas, conta-se a "Aritmética de Treviso" (1478), primeiro livro de matemática impresso no ocidente, a qual lançava mão da nova escrita matemática para explicar problemas matemáticos sugeridos com as trocas comerciais e outros problemas práticos. De fato, esse crescimento proporcionado pela "nova escrita" implicou em amplo desenvolvimento do ensino da matemática e dela própria enquanto ciência.

2.2 Números e Representações

Em suma, está na nova representação numérica os primórdios da democratização do conhecimento matemático. Esta, juntamente com o simbolismo algébrico, que também se inicia, propicia o que os teóricos da história da matemática chama de "Alvorada da matemática moderna". (EVES, p. 340).

De modo sintomático, a evolução de um conhecimento é, em si, um problema de semiologia ou de representação. No que diz respeito a teoria dos números, o coroamento deste processo dá-se com o chamado sistema de numeração decimal que se baseia em fatos, hoje simples, que levaram milênios para serem estabelecidos.

O primeiro e mais elementar é a criação de um número finito de símbolos para estabelecer a representação dos infinitos números. Daí a chegada dos chamados algarismo indo arábicos: 0,1,2,3,4,5,6,7,8 e 9.

O segundo fato, e mais decisivo, é a descoberta do chamado princípio da posição, regra que supõe que o valor de um algarismo varia com a posição que ele ocupa na representação. No dizer de um teórico dos mais importantes na história da matemática.

"Esse princípio parece-nos hoje de uma tal simplicidade que a humanidade tateou e hesitou durante milênios antes de descobri-lo, e que culturas tão avançadas quanto as civilizações grega e egípcia ignoraram-no completamente". (IPHRAH, p. 678).

Um terceiro fato é a ideia de uma notação somativa. Por exemplo, ao escrevermos 3475 queremos dizer 3000+400+70+5 que resulta na chamada expansão decimal.

$$3475 = 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$$

Tem-se, pois o conceito chave de base do sistema. No caso, o sistema decimal ou de base 10, que é o usado para a representação numérica tradicionalmente, a partir do século XIII, carrega neste conceito a essência de sua simplicidade: com apenas dez símbolos e a ideia de que a posição do mesmo na representação varia seu valor, da direita para a esquerda, por uma potência de 10, representam todos os números. É claro, para cingirmos nossa preocupação ao proposito desta dissertação, estamos tratando dos chamados números naturais. Para IPHRAH 1997:

> Com o panorama de que dispomos agora o nascimento de nossa numeração atual parece-nos, por conseguinte um acontecimento colossal na história da humanidade um acontecimento tão revolucionário quanto o domínio do fogo, o desenvolvimento da agricultura, ou a invenção escrita, da roda ou da máquina a vapor (IPHRAH 1997, p. 692).

Percebe-se com isso que o próprio sistema de numeração decimal, além de representar uma tecnologia que permite realizar operações numéricas de forma simples e rapidamente, traz em sua estrutura possibilidades de desenvolvimento para a própria matemática. É nesta ordem de ideia que colocamos nosso trabalho atual cujo, objetivo é o de desenvolver métodos para gerar critérios de divisibilidade no âmbito da teoria dos números.

2.2.1 Bases de sistemas de numeração

Claro que, com tais princípios assumidos, podemos trabalhar com sistemas de numeração em outras bases. Na Babilônia antiga, sem os símbolos arábicos dos quais os símbolos decorrem, a ideia da base 60 (hexadecimal) era usada. Daí decorreu os modos ainda utilizados de medida de tempo (1 hora = 60 minutos, 1 minuto = 60 segundos) e de ângulo (1^o = 60', 1' = 60"), por exemplo. O sistema binário é usado para fazer face aos usos computacionais. Neste, cada número natural N é dado por uma expressão de tipo

$$N = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + \ldots + 2^na_n,$$

em que $a_0, a_1, a_2, \ldots, a_n$ são símbolos escolhidos entre **0** e **1**.

De um modo geral, para uma base b qualquer temos:

$$N = \sum_{j=0}^{n} a_j b^j,$$

em que $a_j \in \{0, 1, 2, 3, \ldots, b-1\}$.

2.3 Indução e somatórios

Coube ao matemático italiano G. Peano (1858-1932) o desenvolvimento de uma axiomática completa para o sistema dos números naturais. Nela, aliado aos conceitos de um primeiro número natural (no nosso caso, o zero) e de sucessor de um numero natural, ele formulou um conjunto de quatro axiomas. Com tão pouco o "edifício" dos números naturais é, então, construído, fato que não é nosso objetivo, mas, que pode ser encontrados em livros de Análise Real. (Ver Lima, 1998)

No nosso caso estamos interessados no quarto axioma de Peano que pode receber o seguinte enunciado:

Se S é um subconjunto de $\mathbb{N}$ tal que:

(i) $0 \in S$;

(ii) o sucessor de cada elemento de S também pertence a S, então S=$\mathbb{N}$.

Uma reformulação deste axioma, conhecido como princípio da indução finita pode ser justa como segue, sendo tida como uma metodologia poderosa para demonstração de fatos sobre números naturais.

Se $P(n)$ é uma afirmativa acerca de um natural genérico n tal que

(i) $P(0)$ é verdadeira; e

(ii) $P(k)$ ser verdadeira para um certo natural k implica $P(k+1)$ verdadeira,

e então $P(n)$ é verdadeira para todo n natural.

O desenvolvimento completo do sistema dos números naturais não é objetivo desta dissertação.

2.4 Divisibilidade e Primalidade

2.4.1 O Algoritmo da Divisão

É historicamente curioso que uma civilização com um modo de representação numérica frágil como a Civilização Grega antiga, tenha produzido resultados matemáticos altamente relevantes como são os resultados conseguidos por ela na Teoria dos Números.

Nesse sentido, o Algoritmo da Divisão ou Algoitmo Euclideano é um desses resultados que marcam o percurso por ser a gene de toda uma teia de relações matemáticas enriquecedoras da ideia de divisibilidade. Um de seus enunciados diz que dados dois naturais a e b, este não nulo, existem únicos naturais q e r tais que

1) $a = b \cdot q + r$, e

2) $0 < r < b$, se r não for nulo.

No caso de r ser nulo diz-se que b é divisor de a ou que a é múltiplo de b. Estas noções - de divisor e de múltiplo – podem ser estendidas no caso de $b = 0$, mas nesse caso, a só poderia ser 0. Isto é, 0 é considerado como um múltiplo universal e como divisor apenas de si mesmo.

2.4.2 Teorema Fundamental da Aritmética

O conceito de número primo é um dos mais importantes na Matemática. Estes números desempenham papel fundamental na Teoria dos Números e estão associados a muitos problemas famosos que permanecem sem soluções apesar dos esforços de vários matemáticos ao longo dos anos.

Um número natural maior do que 1 que só possui como divisores 1 e ele próprio é chamado de número primo. O Teorema Fundamental da Aritmética garante que todo número natural maior do que um, ou é primo, ou pode ser decomposto de maneira única num produto de números primos, a menos de permutações dos fatores (Alencar Filho, 1988). A partir disso, Carvalho et al (2015) afirma que:

> os conceitos que se associam favorecendo a sua compreensão são as relações de múltiplos e fatores que podem se estabelecer entre um par de números naturais e as propriedades que derivam destas relações, os critérios de divisibilidade, a diferenciação entre primos e compostos e decomposição de um número em fatores primos (p. 4).

Uma aplicação muito recorrente do Teorema Fundamental da Aritmética no Ensino Básico é o uso deste teorema para determinar a quantidade de divisores de um número natural qualquer.

Deste modo, os conceitos que se associam para favorecer a sua compreensão são as relações de múltiplos e fatores que se estabelecem entre um par de números naturais e as propriedades que derivam das mesmas, os critérios de divisibilidade, a diferenciação entre primos e compostos e decomposição de um número em fatores primos (CARVALHO et al, 2015).

Destacamos ainda, a relevância desses conceitos dentro do corpo de conhecimentos matemáticos a serem estudados na Educação Básica. Conhecendo alguns critérios de divisibilidade, o estudante poderá efetuar tanto cálculos mentais e estimativas. Ao observar a decomposição de números naturais em fatores primos, pode-se obter rapidamente tanto o MMC quanto o MDC dos números em questão, podendo ainda calcular o número de divisores de cada um ou encontrar cada um desses divisores (CARVALHO et al, 2015).

Em 1998, foi publicado os Parâmetros Curriculares Nacionais (PCNs), documento que aponta diretrizes para a construção dos currículos escolares. Foram apontadas críticas relacionadas à linguagem, como sendo elemento que dificulta a compreensão da proposta, e à sua presença num contexto democrático. No que se refere à Matemática, Angelo e Silva (2008) in Carvalho et al (2015) apontam que "(...) os documentos são relevantes, uma vez que estes refletem as recomendações dos educadores matemáticos desde os anos 80 e sistematizam questões de primeira ordem sobre o ensino e a aprendizagem dessa área do conhecimento" (p.33). Nos PCNs de Matemática do Ensino Fundamental os conteúdos estão distribuídos em quatro blocos: números e operações, espaço e forma, grandezas e medidas e tratamento da informação. O Teorema Fundamental da Aritmética e os demais conceitos associados a ele estão contidos no bloco números e operações e, deste modo, grande parte das escolas brasileiras e livros didáticos, são apresentados desde o 4º ano do Ensino Fundamental, sendo retomado posteriormente nos anos subsequentes com aumento gradual dos números, cuja decomposição é solicitada aos estudantes (CARVALHO et al, 2015).

Os PCN elencam os conteúdos a serem estudado e apontam uma reflexão no ensino. No caso do ensino da Aritmética é sugerida uma abordagem mais reflexiva dos números considerando que deve ser percebido por parte dos estudantes a existência de diversos tipos de números, tais como os naturais, os negativos, os racionais e os irracionais, bem como os seus diferentes significados. (BRASIL, 1998: 50).

Sobre o Teorema Fundamental da Aritmética, Coelho et al. (2005) investigaram sua compreensão por professores de Matemática em curso de formação continuada e por estudantes de 8ª série do Ensino Fundamental de São Paulo. Elas concluíram que existem diferenças entre os dois grupos. Grande parte das vezes, os estudantes reproduzem algoritmos sem interpretar cada etapa de suas ações e seus resultados. Já com os professores foi percebida uma compreensão conceitual mais aprofundada, decorrente do estudo recente da Teoria dos Números no curso de formação continuada já citado. Com este estudo conclui-se que é possível criar cursos voltados para estudantes de qualquer nível de ensino em que a compreensão conceitual seja enfatizada, por outro lado, o professor deve estar atento para que a abordagem não seja voltada para um ensino com muitos algoritmos.

Carvalho et al (2015) corrobora conosco quando reforça que se faz necessário uma "abordagem que priorize a formação de conceitos e não simplesmente a memorização de algoritmos, desde os anos iniciais do Ensino Fundamental." Nota-se assim que se não houver favorecimento da construção de conceitos, o estudante encontrará dificuldades durante sua vida escolar, muito mais quando confrontado com situações que exijam tomar decisões e estabelecer estratégias de resolução de problemas.

Nota-se assim que não cabe ao educador apenas a apropriação dos conceitos que deseja ensinar, faz-se necessário que sua esfera de conhecimento seja mais abrangente. É possível elaborar uma metodologia de ensino com estratégias que estimulem a capacidade de dedução, a memorização e a habilidade de generalizar quando o professor se envolve de forma mais aprofundada com os teoremas e propriedades que embasam suas aulas. Acredita-se que os tópicos a seguir são essenciais para que o professor conceba uma forma própria de trabalhar, em nível adequado às turmas do Ensino Fundamental - sexto ano, com as ideias de divisibilidade, múltiplos, divisores, divisão euclidiana, números primos e o Teorema Fundamental da Aritmética. Para chegar à abstração os mesmos precisarão construir definições, refletir e argumentar sobre conceitos e processos matemáticos, orientados pelo professor que deve dominar o assunto com profundidade (CARVALHO et al, 2015).

2.5 Múltiplos e divisores

2.5.1 Mínimo múltiplo comum

Dados a e b inteiros não nulos, o mínimo múltiplo comum de a e b é o menor dentre os múltiplos positivos comuns de a e b.

Mais precisamente, o mínimo múltiplo comum de a e b é o natural m com as seguintes propriedades:

(i) $m > 0$;

(ii) m é um múltiplo comum de a e b;

(iii) se c é um múltiplo comum de a e b, então m | c.

2.5.2 Máximo divisor comum

Toda a estrutura multiplicativa de um número inteiro é mostrada pela sua fatoração em primos. Permitindo, por exemplo, determinar de modo mais rápido o mdc e o mmc de dois números inteiros não nulos (FARIA, 2015).

No ensino fundamental, um dos métodos ensinados para encontrar o mdc de dois inteiros positivos a e b é o número obtido ao se tomar o produto de todos os fatores primos comuns de a e b, com cada um desses fatores sendo escolhido com o menor dos expoentes que aparece nas fatorações de a e b.

Apresentamos a seguir a definição de MDC:

Dados dois números inteiros a e b (a ou b não nulos), a cada um deles pode-se associar seu conjunto de divisores, D_a e D_b, respectivamente. A interseção $D_a \cap D_b$ é não vazia, visto que o 1 pertence à interseção. Por ser finito, $D_a \cap D_b$ possui elemento máximo.

Euclides no livro Os Elementos, Livro VII, apresenta a constatação da existência do MDC. Podemos perceber que o algoritmo de Euclides é um método prático para obtenção do MDC, uma vez que ele é o maior inteiro que divide os dois valores sem deixar resto (resto zero, na divisão). Inicialmente o algoritmo foi descrito apenas para números naturais e comprimentos geométricos, mas, posteriormente, foi estendido para outras classes de números. Pode-se encontrar a demonstração deste método em Hefez (2005).

Associado ao conceito de MDC está o resultado conhecido como Lema de Bezout, que enunciaremos a seguir:

2.5.3 Lema 2.1: Lema de Bezout

Se a e b são inteiros e d é o mdc de a e b, então existem inteiros q e r tais que $d = a \cdot q + b \cdot r$. Um resultado que decorre deste Lema, permite-nos concluir que, c, d, p $>$ 1 inteiros pelo lema 2.1 existe s e $t \in \mathbb{Z}$ tal que $p \cdot s + c \cdot t = 1$.

2.6 Congruência ou aritmética modular

No século III d.C., o matemática Diofanto, em seu livro Aritmética, procurou pela primeira vez estudar sistematicamente as soluções inteiras de certos tipos de equações polinomiais, as quais passaram a ser conhecidas como ***diofantinas***.

Há de se notar, conforme aponta Rocha (2012), que um dos fatores que contribuíram fundamentalmente para o desenvolvimento da álgebra é a necessidade de se introduzir novos conjuntos de números, com o consequente esforço para compreender sua natureza e, também a sua formalização adequada.

Nota-se que após Euclides, a Teoria dos Números havia se estagnada por cerca de 500 anos, ressuscitando com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 a.C. Dentre os 13 volumes de sua obra, apenas 7 chegaram até nós. Esta obra tida como o primeiro tratado de álgebra conhecido até hoje. Diferentemente de seus precursores, Diofanto utiliza uma abordagem totalmente algébrica, não sendo revestida de interpretação ou linguagem geométrica. Muitas vezes se limitou a encontrar soluções inteiras de determinadas equações algébricas com uma ou várias incógnitas, abstendo-se de aspectos conceituais e teóricos os quais Platão preconizava acerca da abordagem aritmética (HEFEZ, 2013; EVES, 2008).

Nota-se ainda que as equações diofantinas são equações em números inteiros com mais de uma variável. Para Neto (2012), a análise dessas equações, de uma forma geral, é uma tarefa não muito trivial, exigindo argumentos sofisticados.

Sendo a, b e m inteiro com $m > 0$, diz-se que a é congruente a b módulo m, se existir um inteiro k tal que $a - b = k \cdot m$.
Escreve-se:

$$a \equiv b \ mod \ (m)$$

Algumas propriedades da congruência módulo m serão usadas neste texto. As principais delas são:

- Se a, b, c, d e m inteiros tais que $a \equiv b \ mod \ (m)$ e $c \equiv d \ mod \ (m)$, então
  - (i) $a + c \equiv b + d \ mod \ (m)$;
  - (ii) $a - c \equiv b - d \ mod \ (m)$;
  - (iii) $a \cdot c \equiv b \cdot d \ mod \ (m)$;
- Se a, b, k e m inteiros tal que $a \equiv b \ mod \ (m)$ com $k > 0$, então $a \cdot k \equiv b \cdot k \ mod \ (m)$.

Não é nosso objetivo demonstrá-las aqui, mas estes resultados podem ser encontrados em Landau (2002) e Santos (1998).

2.7 Critérios ou caracteres de divisibilidade

Primeiro vamos definir a relação divide entre dois números inteiros, conhecida também como relação de divisibilidade: Dados dois números $a, b \in \mathbb{Z}$, dizemos que b

"*divide*" a, se existir um $c \in \mathbb{Z}$ tal que $a = bc$. Se b dividir a, dizemos que b é um divisor de a, que a é divisível por b ou ainda que a é um múltiplo de b.

Em Carvalho (2013) é apontada a definição de divisibilidade de uma forma diferente, em que este autor argumenta que "ao partir dessa premissa, podemos levar os alunos a pensar que a divisão somente pode ser realizada quando um número é divisível por outro, criando um obstáculo para a aprendizagem de posteriores divisões que deixam restos não nulos" (p. 19). O mesmo argumenta que, diferente dos livros didático tradicionais, a ideia de um número ser dividido por outro é quando este for múltiplo do outro.

Nota-se que na educação básica, definimos critérios ou caracteres de divisibilidade como sendo regras que permitem dizer se um número é ou não divisível por outro sem efetuar a divisão, dependendo dos critérios ou caracteres de divisibilidade utilizados sabemos o resto da divisão ou não.

De forma mais rigorosa dizemos que critérios ou caracteres de divisibilidade são teoremas, ou seja, são afirmações demonstradas que permitem dizer se um número é ou não divisível por outro sem efetuar a divisão dando até o resto da divisão dependendo do critério utilizado.

2.8 Generalização dos Critérios de divisibilidade

Em Rodrigues (2013) encontramos o seguinte resultado apresentando uma generalização dos critérios de divisibilidades.

2.8.1 Teorema 2.1: Generalização dos Critérios de divisibilidade.

Dados dois números positivos N e p, com $p > 1$ existe uma única sequência finita $a_0, a_1, \ldots, a_m$ de números menores do que p, com $a_m \neq 0$, tal que $N = \sum_{i=0}^{m} a_i \cdot p^i$.

Note que o TEOREMA 2.1 não faz referência ao número zero, mas este caso é trivial, assim como o do número um, já que esses números serão sempre representados como 0 e 1 independentemente da base do sistema de numeração posicional.

A seguinte proposição também é encontrado naquela dissertação.

2.8.2 Proposição 2.1:

Se $r < p$, as afirmações (i) e (ii), dadas abaixo, são equivalentes:

(i) $N \equiv r \ mod \ p$;

(ii) $r = a_0$.

Como corolário desta proposição, Rodrigues apresenta aquele que vai ser o critério de divisibilidade, de fácil dedução.

2.8.3 Corolário 2.1 da Proposição 2.1:

Um número N é divisível por p se, e somente se, $a_0 = 0$.

Em outras palavras, o que o COROLÁRIO 2.1 da PROPOSIÇÃO 2.1, nos diz é que todo numeral terminado em zero é divisível pela base do sistema de numeração, assim como todo número divisível pela base deve ter sua representação terminada em zero. Não é à toa, portanto, que este é o critério de divisibilidade do número dez, já que esta é a base do Sistema de Numeração Posicional Decimal (SNPD).

2.9 Lemas que serão utilizados nas demonstrações dos métodos geradores de critérios de divisibilidades.

Nesta subseção enunciaremos e demonstraremos dois lemas que serão utilizados nas demonstrações dos métodos geradores de critérios de divisibilidades.

2.9.1 Lema 2.2: Soma de múltiplos ou Lema de Euclides

Sejam N, p e k, números inteiros, com p diferente de zero é. N divisível por p se, e somente se, $N - k.p$ é divisível por p.

Demonstração:

$(\Rightarrow)$: Se N é divisível por p, então $N - k.p$ é divisível por p.

Se N é divisível por p, então existe $t \in \mathbb{Z}$ tal que $N = t.p$, assim $N - k.p = t.p - k.p$, ou seja, $N - k.p = (t - k).p$, como $t - k \in \mathbb{Z}$, logo $N - k.p$ é divisível por p.

$(\Leftarrow)$: Se $N - k.p$ é divisível por p, então N é divisível por p.

Se $N - k.p$ é divisível por p, então existe $y \in \mathbb{Z}$ tal que $N - k.p = y.p$, assim $N = y.p + k.p$, ou seja, $N = (y + k).p$, como $y + k \in \mathbb{Z}$, logo N é divisível por p.

$\blacksquare$

2.9.2 Lema 2.3: Um dos fatores coprimo com o divisor.

Considere d, c e $p > 1$ inteiros, com c e p primos entre si. $x = c \cdot d$ é divisível por p se, e somente se, d é divisível por p.

Demonstração:

$(\Rightarrow)$: p e c são coprimos e p divide $x \Rightarrow p$ divide d.

Como p e c, são coprimos, então existe s e $t \in \mathbb{Z}$ tal que $p \cdot s + c \cdot t = 1$, logo mutiplicando d pela expressão $p \cdot s + c \cdot t = 1$ temos:

$$d \cdot p \cdot s + d \cdot c \cdot t = d$$

$$p | d \cdot p \cdot s \ e \ p | c \cdot d \Rightarrow p | d \cdot c \cdot t$$

$$\Rightarrow p | p \cdot d \cdot s + d \cdot c \cdot t = d$$

$(\Leftarrow)$: p e c são coprimos e p divide $d \Rightarrow p$ divide x.

Como p e c, são coprimos e p divide d existe $k_2 \in \mathbb{Z}$ tal que $d = p.k_2$, logo temos: $x = c \cdot d = c \cdot p.k_2$, assim p divide x.

$\blacksquare$

Capítulo 3

MÉTODOS GERADORES DE CRITERIOS DE DIVISIBILIDADE.

3.1 Introdução

Nosso objetivo é apresentar dois métodos para generalizar e estender os processos para gerar critérios de divisibilidades de forma abrangente, permitindo que eles sejam gerados a partir destes métodos. Vários critérios de divisibilidades existentes na literatura podem ser obtidos a partir deles. Este capítulo está organizado da seguinte maneira. Na Seção 3.1, temos uma breve introdução, trazendo o objetivo; na Seção 3.2, temos o desenvolvimento da ideia de representação de números inteiros em algarismos generalizados; na Seção 3.3, temos o método gerador de critérios de divisibilidades tipo alfa e apresentamos o Teorema 3.1 e alguns corolários deste método; na Seção 3.4, temos o método gerador de critérios de divisibilidades tipo beta;

3.2 Representação de um número natural em algarismos generalizados.

O objetivo desta subseção é a apresentação de representação de números naturais em algarismos generalizados para o desenvolvimento de métodos geradores de critérios de divisibilidades que as utilizem.

Para o desenvolvimento da ideia de representação de um número natural em algarismos generalizadas, faremos as seguintes definições:

Definição 1: Um conjunto $P = \{s_h, \ldots, s_1\} \subset \mathbb{N}$, para o qual $s_h > s_{h-1} > \cdots > s_1 > 0$, é denominado partição.

Exemplo 1:

Consideremos, por exemplo, o número com representação decimal $N = 32.005.768$ $.979$ e um conjunto partição $P = \{9, 6, 2\}$. A partição pode ser escrita da seguinte forma $N = \underbrace{32}_{A_3} | \underbrace{005}_{A_2} | \underbrace{7689}_{A_1} | \underbrace{79}_{A_0}$.

Exemplo 2:

Consideremos, por exemplo, o número com representação decimal $-N = -68.979$ e um conjunto partição $P = \{9, 6, 2\}$. A partição pode ser escrita da seguinte forma $-N = \underbrace{0}_{A_3} | \underbrace{000}_{A_2} | \underbrace{-689}_{A_1} | \underbrace{-79}_{A_0}$.

Exemplo 3:

Consideremos, por exemplo, o número com representação decimal $-N = -79$ e um conjunto partição $P = \{9, 5, 3\}$. A partição pode ser escrita da seguinte forma $-N = \underbrace{0}_{A_3} | \underbrace{0000}_{A_2} | \underbrace{00}_{A_1} | \underbrace{-079}_{A_0}$.

Definição 2: Dado um número natural $N = (a_t a_{t-1} \ldots a_1 a_0)_{10}$ e um conjunto partição $P = \{s_h, \ldots, s_1\}$. Dizemos que

$$A_0 = (a_{s_1-1} \ldots a_1 a_{s_0})_{10};$$

$$A_1 = (a_{s_2-1} \ldots a_{s_1})_{10};$$

$$\vdots$$

$$A_h = (a_t \ldots a_{s_h})_{10};$$

com $s_0 = 0$, são algarismos generalizados de N com respeito a partição $P = \{s_h, \ldots, s_1\}$, se $N = \sum_{r=0}^{h} 10^{s_r} \cdot A_r$.

Utilizaremos a notação $(A_h|\cdots|A_0)_{(s_h,\cdots,s_1)}$ para indicar que $A_h, \ldots, A_0$ são algarismos generalizados de N com respeito a $\{s_h, \ldots, s_1\}$.

Exemplo:

Consideremos os dados do exemplo anterior, onde $s_3 = 9$, $s_2 = 6$ e $s_1 = 2$. A divisão em algarismos generalizados escrita na forma $N = \underbrace{32}_{A_3} | \underbrace{005}_{A_2} | \underbrace{7689}_{A_1} | \underbrace{79}_{A_0}$, que utilizando a notação tomada teremos $(A_3|A_2|A_1|A_0)_{(s_3,s_2,s_1)} = (32|5|7689|79)_{(9,6,2)}$.

Vejamos alguns exemplos ilustrativos a seguir:

Exemplo 1:

Consideremos um exemplo numérico, para $N = 132.564.798$ com o conjunto partição $P = \{5, 3, 2\}$. Neste caso teremos quatro algarismos generalizados A_0, A_1, A_2 e A_3 a discutir, pois $h = 3$. No caso, a partição referida terá a forma $N = \underbrace{1325}_{A_3} | \underbrace{64}_{A_2} | \underbrace{7}_{A_1} | \underbrace{98}_{A_0}$, que utilizando a notação tomada teremos $(A_3|A_2|A_1|A_0)_{(s_3,s_2,s_1)} = (1325|64|7|98)_{(5,3,2)}$, em que 1325 na notação será A_3, 64 será A_2, 7 será A_1 e 98 será A_0.

Exemplo 2:

Consideremos, por exemplo, o conjunto partição $P = \{2\}$. Neste caso só teremos dois algarismos generalizados A_0 e A_1 a discutir, pois $h = 1$. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \ldots a_2}_{A_1} | \underbrace{a_1 a_0}_{A_0} \right)_{(2)}$, em que $a_t \ldots a_2$ na notação tomada será A_1 e $a_1 a_0$ será A_0.

Exemplo 3:

Consideremos, por exemplo, o conjunto partição $P = \{3\}$. Neste caso teremos dois algarismos generalizados A_0 e A_1 a discutir, pois $h = 1$. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \dots a_3}_{A_1} | \underbrace{a_2 a_1 a_0}_{A_0}\right)_{(3)}$, em que $a_t \dots a_3$ na notação tomada será A_1 e $a_2a_1a_0$ será A_0.

Exemplo 4:

Consideremos, por exemplo, o conjunto partição $P = \{3, 2\}$. Neste caso teremos três algarismos generalizados A_0, A_1 e A_2 a discutir, pois $h = 2$. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \dots a_3}_{A_2} | \underbrace{a_2}_{A_1} | \underbrace{a_1 a_0}_{A_0}\right)_{(3,2)}$.

3.2.1 Proposição 3.1: Representação única em algarismos generalizados.

Fixado um conjunto partição $P = \{s_h, \dots, s_1\}$, todo número natural possui representação única em algarismos generalizados, ou seja, existem $A_h, \dots, A_0$ tais que $N = \sum_{r=0}^{h} 10^{s_r} \cdot A_r$, com $0 \leq A_r < 10^{s_{(r+1)} - s_r}, r = 0, 1, \dots, h-1$ e $A_h \geq 0$.

Demonstração:

Primeiro vamos mostrar a existência, ou seja, que fixado um conjunto partição $P = s_h, \dots, s_1$, existem os algarismos generalizados $A_h, \dots, A_0$ de N tais que $N = \sum_{r=0}^{h} 10^{s_r} \cdot A_r$, com $0 \leq A_r < 10^{s_{(r+1)} - s_r}, r = 0, 1, \dots, h-1$ e $A_h \geq 0$. Iniciaremos pela divisão de N por 10^{s_1} obtendo o quociente q_0 e o resto A_0. Em seguida dividiremos q_0 por $10^{s_2 - s_1}$ obtendo o quociente q_1 e resto A_1, e, prosseguindo desta forma, obteremos a seguinte sequência de igualdades:

$$N = 10^{s_1 - s_0} \cdot q_0 + A_0;$$

$$q_0 = 10^{s_2 - s_1} \cdot q_1 + A_1;$$

$$q_1 = 10^{s_3 - s_2} \cdot q_2 + A_2;$$

$$\vdots$$

$$q_{h-3} = 10^{s_{h-1} - s_{h-2}} \cdot q_{h-2} + A_{h-2};$$

$$q_{h-2} = 10^{s_h - s_{h-1}} \cdot A_h + A_{h-1}.$$

Agora, na primeira destas equações, substituindo o valor de q_0 dado na segunda. Em seguida substituindo, nesta expressão, o valor de q_1 dado na terceira, e assim sucessivamente, obtendo:

$$
\begin{aligned}
N &= 10^{s_1-s_0} \cdot q_0 + A_0; \\
&= 10^{s_1-s_0} \cdot (10^{s_2-s_1} \cdot q_1 + A_1) + A_0; \\
&= 10^{s_2-s_0} \cdot q_1 + 10^{s_1-s_0} \cdot A_1 + A_0; \\
&= 10^{s_2-s_0} \cdot (10^{s_3-s_2} \cdot q_2 + A_2) + 10^{s_1-s_0} \cdot A_1 + A_0; \\
&= 10^{s_3-s_0} \cdot q_2 + 10^{s_2-s_0} \cdot A_2 + 10^{s_1-s_0} \cdot A_1 + A_0; \\
&\vdots \\
&= 10^{s_{h-1}-s_0} \cdot q_{h-2} + 10^{s_{h-2}-s_0} \cdot A_{h-2} + \cdots + 10^{s_1-s_0} \cdot A_1 + A_0; \\
&= 10^{s_{h-1}-s_0} \cdot (10^{s_h-s_{h-1}} \cdot A_h + A_{h-1}) + 10^{s_{h-2}-s_0} \cdot A_{h-2} + \cdots + 10^{s_1-s_0} \cdot A_1 + A_0; \\
&= 10^{s_h-s_0} \cdot A_h + 10^{s_{h-1}-s_0} \cdot A_{h-1} + 10^{s_{h-2}-s_0} \cdot A_{h-2} + \cdots + 10^{s_1-s_0} \cdot A_1 + A_0.
\end{aligned}
$$

Como $s_0 = 0$, logo temos:

$$N = 10^{s_h} \cdot A_h + 10^{s_{h-1}} \cdot A_{h-1} + 10^{s_{h-2}} \cdot A_{h-2} + \cdots + 10^{s_1} \cdot A_1 + 10^{s_0} \cdot A_0,$$

com $0 \leq A_r < 10^{s_{r+1}-s_r}, r = 0, 1, \ldots, h-1$ e $A_h \geq 0$.

Nos resta mostrar, agora, a unicidade desta representação. Para provarmos a unicidade, assumimos a existência de uma outra representação, ou seja, $N = \sum_{r=0}^{h} 10^{s_r} \cdot B_r$ com $0 \leq B_r < 10^{s_{r+1}-s_r}, r = 0, 1, \ldots, h-1$ e $B_h \geq 0$. Se A_r e B_r não são todos iguais, pela subtração membro a membro, de $\sum_{r=0}^{h} 10^{s_r} \cdot A_r$ da equação $\sum_{r=0}^{h} 10^{s_r} \cdot B_r$ obtemos:

$$0 = \sum_{r=0}^{z} 10^{s_r} \cdot (A_r - B_r)$$

onde z é o maior valor de r para o qual $A_r \neq B_r$. Logo, $A_r - B_r \neq 0$. Note que $z = 0$, temos uma contradição pois estamos assumindo que $\sum_{r=0}^{h} 10^{s_r} \cdot B_r$ seja diferente de $\sum_{r=0}^{h} 10^{s_r} \cdot A_r$. Se $z > 0$, temos

$$|A_r - B_r| \leq 10^{s_{r+1}-s_r} - 1, \text{ para } 1 \leq r \leq z-1;$$

$$10^{s_z} \cdot (A_z - B_z) = -\sum_{r=0}^{z-1} 10^{s_r} \cdot (A_r - B_r).$$

e, portanto

$$10^{s_z} \leq |10^{s_z} \cdot (A_z - B_z)| = \left|\sum_{r=0}^{z-1} 10^{s_r} \cdot (A_r - B_r)\right| \leq \sum_{r=0}^{z-1} 10^{s_r} \cdot |A_r - B_r|$$
$$\leq \sum_{r=0}^{z-1} 10^{s_r} \cdot (10^{s_{r+1}-s_r} - 1) = \sum_{r=0}^{z-1} (10^{s_{r+1}} - 10^{s_r}) = 10^{s_z} - 1.$$

o que é, também, uma contradição. Desta forma concluímos que os $A_r{}'S$ e $B_r{}'S$ são todos iguais, isto é, $A_r = B_r, r = 0, 1, \ldots, h$, e portanto, a representação em algarismos generalizados é única.

■

Vejamos alguns exemplos ilustrativos a seguir:

Exemplo 1:

Consideremos um exemplo numérico, para $N = 0$ com o conjunto partição $P = \{5, 3, 2\}$. Logo utilizando a notação tomada teremos $(A_3|A_2|A_1|A_0)_{(s_3,s_2,s_1)} = (0|0|0|0)_{(5,3,2)}$, podemos ainda representar a partição da seguinte forma:

$$N = \left(\underbrace{0}_{A_3} | \underbrace{00}_{A_2} | \underbrace{0}_{A_1} | \underbrace{00}_{A_0}\right)_{(5,3,2)}.$$

Exemplo 2:

Consideremos um exemplo numérico, para $N = 1$ com o conjunto partição $P = \{5, 3, 2\}$. Logo utilizando a notação tomada teremos $(A_3|A_2|A_1|A_0)_{(s_3,s_2,s_1)} = (0|0|0|1)_{(5,3,2)}$, podemos ainda representar a partição da seguinte forma:

$$N = \left(\underbrace{0}_{A_3} | \underbrace{00}_{A_2} | \underbrace{0}_{A_1} | \underbrace{01}_{A_0}\right)_{(5,3,2)}.$$

Exemplo 3:

Consideremos um exemplo numérico, para $N = 7.000$ com o conjunto partição $P = \{5, 3, 2\}$. Logo utilizando a notação tomada teremos $(A_3|A_2|A_1|A_0)_{(s_3,s_2,s_1)} = (0|7|0|0)_{(5,3,2)}$, podemos ainda representar a partição da seguinte forma:

$$N = \left(\underbrace{0}_{A_3} | \underbrace{07}_{A_2} | \underbrace{0}_{A_1} | \underbrace{00}_{A_0} \right)_{(5,3,2)}.$$

3.3 Método Gerador de Critérios de divisibilidade do tipo Alfa

Nesta seção iremos apresentar o método denominado tipo Alfa para gerar critérios de divisibilidade de forma mais sistemática. Este método baseia-se na Congruência Modular, assunto comumente abordado em livros de Teoria dos Números. De fato, o nome Alfa é apenas um modo didático de considerar a categorização que obtivemos para a ideia de gerar critérios de divisibilidade. Como modo de organização do texto é enunciado alguns resultados básicos que conduzirão ao teorema central do método (Teorema 3.1) ao qual se seguirão alguns corolários. A notação apresentada, de nossa criação, carrega em si os invariantes para aplicação do método e será determinante na sua utilização, buscando padronizar a utilização em todos os métodos que seguirão neste trabalho, exceto o último método que é o método gerador de critérios de divisibilidade por produto de coprimos.

A partir de agora, apresentaremos o método gerador de critério de divisibilidade por $p > 1$ do tipo Alfa. A essência deste método, que será posteriormente demonstrado na subseção 3.4.1, consiste em considerar os algarismos generalizados $\alpha_h, \ldots, \alpha_0$ do natural N com respeito a partição $P = \{s_h, \ldots, s_1\}$ e os números $w_r \equiv 10^{s_r}\ mod(p)$ para $r = 0, 1, \ldots, h$ tal que $N \equiv \sum_{r=0}^{h} w_r \cdot \alpha_r\ mod(p)$. Por exemplo, vamos considerar $P = \{3, 2\}$. Neste caso teremos três algarismos generalizados α_0, α_1 e α_2 conforme a partição $N = \left(\underbrace{a_t \ldots a_3}_{\alpha_2} | \underbrace{a_2}_{\alpha_1} | \underbrace{a_1 a_0}_{\alpha_0} \right)_{(3,2)}$.

Assim,

$$N = 10^{s_2} \cdot \alpha_2 + 10^{s_1} \cdot \alpha_1 + 10^{s_0} \cdot \alpha_0;$$

$$N = 10^3 \cdot \alpha_2 + 10^2 \cdot \alpha_1 + 10^0 \cdot \alpha_0.$$

Para $p = 11$, temos que,

$$N \equiv 10^3 \cdot \alpha_2 + 10^2 \cdot \alpha_1 + 10^0 \cdot \alpha_0\ mod(11);$$

$$N \equiv -\alpha_2 + \alpha_1 + \alpha_0 \ mod(11).$$

Neste caso, estamos dizendo que na divisão por 11 em que a partição tomada para o número tem três algarismos generalizados $\alpha_0 = a_1a_0$, $\alpha_1 = a_2$ e $\alpha_2 = a_t \ldots a_3$, o número dado, reduz-se a forma $-\alpha_2 + \alpha_1 + \alpha_0$ módulo 11. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 11 ocorre ou não.

Um exemplo numérico seria verificar se o número $N = 345.216$ é divisível por p=11. Utilizando a partição já dada $P = \{3, 2\}$, temos os algarismos generalizados $\alpha_2 = 345$, $\alpha_1 = 2$ e $\alpha_0 = 16$. A partir de $-\alpha_2 + \alpha_1 + \alpha_0$ temos:

$$-\alpha_2 + \alpha_1 + \alpha_0 = -345 + 2 + 16;$$

$$-\alpha_2 + \alpha_1 + \alpha_0 = -327.$$

Replicando o método em -327, temos $\alpha_2 = 0$, $\alpha_1 = -3$ e $\alpha_0 = -27$:

$$-\alpha_2 + \alpha_1 + \alpha_0 = -0 - 3 - 27;$$

$$-\alpha_2 + \alpha_1 + \alpha_0 = -30.$$

Como -30 não é divisível por 11, então 345.216 também não é.

A seguir, enunciaremos e demonstraremos o teorema denominado Método Gerador de Critérios de Divisibilidade do tipo Alfa que nos permitirá gerar critérios de divisibilidade para números inteiros maiores que 1.

3.3.1 Teorema 3.1: Método Gerador de Critérios de Divisibilidade do tipo Alfa

Sejam α_0, α_1,..., α_h algarismos generalizados de N com respeito a partição $P = \{s_h, \ldots, s_1\}$, $M = \sum_{r=0}^{h} w_r \cdot \alpha_r$ com $w_r \in \mathbb{Z}$ e $p > 1$ inteiro tal que $w_r \equiv 10^{s_r}$ $mod(p)$. Então p divide N se, e somente se, p divide $\sum_{r=0}^{h} w_r \cdot \alpha_r$.

Demonstração:

Considere $\alpha_0 = (a_{s_1-1}\dots a_1 a_{s_0})_{10}$, $\alpha_1 = (a_{s_2-1}\dots a_{s_1})_{10}$, ..., $\alpha_{h-1} = (a_{s_h-1}\dots a_{s_h-1})_{10}$, $\alpha_h = (a_{s_{h+1}-1}\dots a_{s_{h+1}-1})_{10}$ algarismos generalizados de N com respeito a partição $P = \{s_h, \dots, s_1\}$. Observe que semelhante a seção 3.3, estamos "partindo" N em $h+1$ algarismos generalizados, como na ilustração a seguir:

$$N = \left(\underbrace{a_t \dots a_{s_h}}_{\alpha_h} | \underbrace{a_{s_h-1}\dots a_{s_{h-1}}}_{\alpha_{h-1}} | \dots | \underbrace{a_{s_2-1}\dots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1}\dots a_1 a_{s_0}}_{\alpha_0} \right)_{(s_h,\dots,s_1)}.$$

Desta forma, vemos por definição que,

$$N = \sum_{r=0}^{h} 10^{s_r} \cdot \alpha_r. \tag{1}$$

Fixada a partição P de N, desejamos construir o M da forma

$$M = \sum_{r=0}^{h} w_r \cdot \alpha_r, \text{ com } w_r \in Z, \text{com } w_r \equiv 10^{s_r} \mod(p). \tag{2}$$

Assim, por (1) e (2), temos que,

$$N = M + \sum_{r=0}^{h} (10^{s_r} - w_r) \cdot \alpha_r.$$

Como $p > 1$ inteiro tal que $p|10^{s_r} - w_r$, $\forall\ r = 0, \dots, h$ temos pelo Lema 2.2 que $p|N$ se, e somente se $p|M$. Este fato nos dará os critérios de divisibilidade por p do tipo Alfa que definiremos adiante.

Primeiramente, vamos encontrar $w_0, \dots, w_h$, tais que $p|10^{s_r} - w_r$, isto é, $w_r \equiv 10^{s_r}$ $mod(p)$, $\forall\ r = 0, \dots, h$. Note que a equação de congruência possui infinitas soluções para cada $r = 0, \dots, h$, o que nos fornecerá infinitos critérios de divisibilidade.

Obtidos os $w_0, \dots, w_h$, temos que $p|N \Leftrightarrow p|\sum_{r=0}^{h} w_r \cdot \alpha_r$. Desta forma para cada escolha dos coeficientes w_r's, criamos um critério de divisibilidade por p para qualquer número natural N.

Utilizaremos a seguinte notação,

$$A_p(w_h, \dots, w_0)_{(s_h,\dots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r.$$

Que representa o critério de divisibilidade por p, do tipo Alfa, definido pelos coeficientes $w_h, \ldots, w_0$ dos algarismos generalizados $\alpha_h, \ldots, \alpha_0$ com respeito da partição $P = \{s_h, \ldots, s_1\}$ de N. Em outras palavras, a notação $A_p(w_h, \ldots, w_0)_{(s_h,\ldots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r$. está representada a sentença "p divide N se, somente se, p divide $\sum_{r=0}^{h} w_r \cdot \alpha_r$".

■

Vejamos alguns exemplos detalhados de como usar o método para facilitar a compreensão da teoria desenvolvida até agora:

Exemplo 1:

Consideremos, por exemplo, $p = 3$. Analisemos o caso em que $h = 1$.

Assim, substituindo os valores $p = 3$ e $h = 1$ na notação tomada teremos:

$$A_p(w_h, \ldots, w_0)_{(s_h,\ldots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_3(w_1, w_0)_{(s_1)} = \sum_{r=0}^{1} w_r \cdot \alpha_r;$$

$$A_3(w_1, w_0)_{(s_1)} = w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

Neste caso só teremos dois algarismos generalizados α_0 e α_1 a discutir. As congruências mencionadas serão da forma $w_0 \equiv 10^{s_0}\ mod(3)$ e $w_1 \equiv 10^{s_1}\ mod(3)$.

Como $s_0 = 0$, tem-se a primeira congruência reduzida a

$$w_0 \equiv 1 mod(3).$$

Ora, o conjunto das soluções de tal congruência é da forma $\{1 + 3u | u \in \mathbb{Z}\}$. Escolheremos como solução representativa o caso $u = 0$ que nos dá $w_0 = 1$.

Para $s_1 = 1$ a segunda congruência acima listada, reduz-se $w_1 \equiv 10\ mod(3)$, cujo o conjunto solução é $\{10 + 3u | u \in \mathbb{Z}\}$.

Para $u = -3$ teremos $w_1 = 1$ e para $u = -4$ teremos $w_1 = -2$. Outros valores de u trariam soluções desinteressantes para nossos propósitos. Portanto teremos as notações correspondentes para o caso em análise:

$$A_3(1,1)_{(1)} = \alpha_1 + \alpha_0 \text{ ou } A_3(-2,1)_{(1)} = -2 \cdot \alpha_1 + \alpha_0.$$

No caso 1, estamos dizendo que na divisão por 3 em que a partição tomada para o número tem dois algarismos generalizados α_0 e α_1, o número dado, reduz-se a forma $\alpha_1 + \alpha_0$. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 3 ocorre ou não.

Consideremos $N = 9282$ com $h = 1$ e $s_1 = 1$, os elementos da partição serão: $\alpha_1 = 928$ e $\alpha_0 = 2$. Na notação tomada, tem-se

$$A_3(1,1)_{(1)} = \alpha_1 + \alpha_0;$$
$$A_3(1,1)_{(1)} = 928 + 2 = 930.$$

Replicando o método, os elementos da partição tomada, terá como elementos, $\alpha_1 = 93$ e $\alpha_0 = 0$.

$$A_3(1,1)_{(1)} = 93 + 0 = 93.$$

Replicando mais um vez o método, os elementos da partição tomada, terá como elementos, $\alpha_1 = 9$ e $\alpha_0 = 3$.

$$A_3(1,1)_{(1)} = 9 + 3 = 12.$$

Conclusão é que, como 12 é divisível por 3, o número 9282 também é divisível por 3.

Exemplo 2:

Consideremos o caso em que $h = 2$ com p ainda igual a 3.

Assim, substituindo os valores $p = 3$ e $h = 2$ na notação tomada temos:

$$A_p(w_h, \ldots, w_0)_{(s_h,\ldots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_3(w_2, w_1, w_0)_{(s_2,s_1)} = \sum_{r=0}^{2} w_r \cdot \alpha_r;$$

$$A_3(w_2, w_1, w_0)_{(s_2,s_1)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

A partição de N agora é $N = \left(\underbrace{a_t \ldots a_{s_2}}_{\alpha_2} | \underbrace{a_{s_2-1} \ldots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1} \ldots a_1 a_0}_{\alpha_{s_0}}\right)_{(s_2,s_1)}$ em que os algarismos generalizados tomados estão separadas pelas barras verticais, ou seja, $\alpha_0 = a_{s_1-1} \ldots a_1 a_0$, $\alpha_1 = a_{s_2-1} \ldots a_{s_1}$ e $\alpha_2 = a_{s_3-1} \ldots a_{s_2}$. Para este caso, as congruências tomadas são $w_0 \equiv 10^{s_0}\ mod(3), w_1 \equiv 10^{s_1}\ mod(3)$ e $w_2 \equiv 10^{s_2}\ mod(3)$.

Considerando $s_1 = 1$ e $s_2 = 2$, tais congruências tem soluções triviais módulo 3 dadas por: $w_0 = 1, w_1 = -2$ e $w_2 = -2$ ou $w_0 = 1$, $w_1 = 1$ e $w_2 = 1$. Portanto, $A_3(-2, -2, 1)_{(2,1)} = -2 \cdot \alpha_2 - 2 \cdot \alpha_1 + \alpha_0$ ou $A_3(1, 1, 1)_{(2,1)} = \alpha_2 + \alpha_1 + \alpha_0$. Isto é, na divisão por 3 em que o número de algarismos generalizados da partição é 3, a saber, $\alpha_0 = a_0, \alpha_1 = a_2$ e $\alpha_2 = a_t \ldots a_2$, o número N se reduz às formas $\alpha_2 + \alpha_1 + \alpha_0$ ou $-2 \cdot \alpha_2 - 2 \cdot \alpha_1 + \alpha_0$ módulo 3.

Consideremos $N = 357214$ com $h = 2$, $s_1 = 1$ e $s_2 = 2$, os elementos da partição serão: $\alpha_2 = 3572$, $\alpha_1 = 1$ e $\alpha_0 = 4$. Na notação tomada, tem-se

$$A_3(1, 1, 1)_{(2,1)} = \alpha_2 + \alpha_1 + \alpha_0;$$

$$A_3(1, 1, 1)_{(2,1)} = 3572 + 1 + 4 = 3577.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\alpha_2 = 35$, $\alpha_1 = 7$ e $\alpha_0 = 7$.

$$A_3(1, 1, 1)_{(2,1)} = 35 + 7 + 7 = 49.$$

Conclusão é que, como 49 não é divisível por 3, o número 357214 também não é divisível por 3.

Exemplo 3:

Consideremos, por exemplo, $p = 7$. Analisemos o caso em que $h = 1$.

Assim, substituindo os valores $p = 7$ e $h = 1$ na notação tomada temos:

$$A_p(w_h, \ldots, w_0)_{(s_h,\ldots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_7(w_1, w_0)_{(s_1)} = \sum_{r=0}^{1} w_r \cdot \alpha_r;$$

$$A_7(w_1, w_0)_{(s_1)} = w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

Neste caso só teremos dois algarismos generalizados α_0 e α_1 a discutir. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \ldots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1} \ldots a_1 a_{s_0}}_{\alpha_0}\right)_{(s_1)}$, em que $a_{s_2-1} \ldots a_{s_1}$ na notação tomada será α_1 e $a_{s_1-1} \ldots a_1 a_{s_0}$ será α_0. As congruências mencionadas serão da forma $w_0 \equiv 10^{s_0}\ mod(7)$ e $w_1 \equiv 10^{s_1}\ mod(7)$ Como sempre teremos $S_0 = 0$, tem-se a primeira congruência reduzida a

$$w_0 \equiv 1 mod(7).$$

Ora, o conjunto das soluções de tal congruência é da forma $\{1 + 7u | u \in \mathbb{Z}\}$. Escolheremos como solução representativa o caso $u = 0$ que nos dá $w_0 = 1$.

Para $s_1 = 2$ a segunda congruência acima listada, reduz-se $w_1 \equiv 100\ mod(7)$, cujo o conjunto solução é $\{100 + 7u | u \in \mathbb{Z}\}$.

Para $u = -14$ teremos $w_1 = 2$ e para $u = -15$ teremos $w_1 = -5$. Outros valores de u trariam soluções desinteressantes para nossos propósitos. Portanto teremos as notações correspondentes para o caso em análise:

$$A_7(2, 1)_{(2)} = 2 \cdot \alpha_1 + \alpha_0 \text{ ou } A_7(-5, 1)_{(2)} = -5 \cdot \alpha_1 + \alpha_0.$$

No caso 1, estamos dizendo que na divisão por 7 em que a partição tomada para o número tem dois algarismos generalizados $\alpha_0 = a_1 a_0$ e $\alpha_1 = a_t \ldots a_2$, o número dado, reduz-se a forma $2 \cdot \alpha_1 + \alpha_0$. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 7 ocorre ou não.

Consideremos $N = 9282$ com $h = 1$ e $s_1 = 2$, os elementos da partição serão: $\alpha_1 = 92$ e $\alpha_0 = 82$. Na notação tomada, tem-se

$$A_7(2,1)_{(2)} = 2 \cdot \alpha_1 + \alpha_0;$$
$$A_7(2,1)_{(2)} = 2 \cdot 92 + 82 = 266.$$

Replicando o método, os elementos da partição tomada, terá como elementos, $\alpha_1 = 2$ e $\alpha_0 = 66$.

$$A_7(2,1)_{(2)} = 2 \cdot 2 + 66 = 70.$$

Conclusão é que, como 70 é divisível por 7, o número 9282 também é divisível por 7.

Exemplo 4:

Consideremos o caso em que $h = 2$ com p ainda igual a 7.

Assim, substituindo os valores $p = 7$ e $h = 2$ na notação tomada temos:

$$A_p(w_h, \ldots, w_0)_{(s_h,\ldots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$
$$A_7(w_2, w_1, w_0)_{(s_2,s_1)} = \sum_{r=0}^{2} w_r \cdot \alpha_r;$$
$$A_7(w_2, w_1, w_0)_{(s_2,s_1)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

A partição de N agora é $N = \left(\underbrace{a_t \ldots a_{s_2}}_{\alpha_2} | \underbrace{a_{s_2-1} \ldots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1} \ldots a_1 a_{s_0}}_{\alpha_0} \right)_{(s_2,s_1)}$, onde os algarismos generalizados tomados estão separadas pelas barras verticais, ou seja, $\alpha_0 = a_{s_1-1} \ldots a_1 a_{s_0}, \alpha_1 = a_{s_2-1} \ldots a_{s_1}$ e $\alpha_2 = a_{s_3-1} \ldots a_{s_2}$. Para este caso, as congruências tomadas são $w_0 \equiv 10^{s_0}\ mod(7)$, $w_1 \equiv 10^{s_1}\ mod(7)$ e $w_2 \equiv 10^{s_2}\ mod(7)$.

Considerando $s_1 = 1$ e $s_2 = 3$, tais congruências tem soluções triviais módulo 7 dadas por: $w_0 = 1, w_1 = -4$ e $w_2 = -1$ ou $w_0 = 1, w_1 = 3$ e $w_2 = -1$. Portanto,

$A_7(-1,-4,1)_{(3,1)} = -\alpha_2 - 4 \cdot \alpha_1 + \alpha_0$ ou $A_7(-1,3,1)_{(3,1)} = -\alpha_2 + 3 \cdot \alpha_1 + \alpha_0$. Isto é, na divisão por 7 em que o número de algarismos generalizados da partição é 3, a saber, $\alpha_0 = a_0$, $\alpha_1 = a_2a_1$ e $\alpha_2 = a_t \dots a_3$. O número N se reduz às formas $-\alpha_2 - 4 \cdot \alpha_1 + \alpha_0$ ou $-\alpha_2 + 3 \cdot \alpha_1 + \alpha_0$.

Consideremos $N = 357214$ com $h = 2$, $s_1 = 1$ e $s_2 = 3$, os elementos da partição serão: $\alpha_2 = 357$, $\alpha_1 = 21$ e $\alpha_0 = 4$. Na notação tomada, tem-se

$$A_7(-1,3,1)_{(3,1)} = -\alpha_2 + 3 \cdot \alpha_1 + \alpha_0;$$
$$A_7(-1,3,1)_{(3,1)} = -357 + 3 \cdot 21 + 4 = -290.$$

Replicando o método, os elementos da partição tomada, terá como elementos,$\alpha_2 = 0$ $\alpha_1 = -29$ e $\alpha_0 = 0$.

$$A_7(-1,3,1)_{(3,1)} = -1 \cdot 0 \cdot (-29) + 1 \cdot 0 = -87.$$

Conclusão é que, como -87 não é divisível por 7, o número 357214 também não é divisível por 7. Há de se notar a brusca redução do valor de N com o método.

Exemplo 5:

Consideremos, por exemplo, $p = 11$. Analisemos o caso em que $h = 1$. Assim, substituindo os valores p=11 e h=1 na notação tomada temos:

$$A_p(w_h, \dots, w_0)_{(s_h,\dots,s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_{11}(w_1, w_0)_{(s_1)} = \sum_{r=0}^{1} w_r \cdot \alpha_r;$$
$$A_{11}(w_1, w_0)_{(s_1)} = w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

Neste caso só teremos dois algarismos generalizados α_0 e α_1 a discutir. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \dots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1} \dots a_1 a_{s_0}}_{\alpha_0} \right)_{(s_1)}$, em que $a_{s_2-1} \dots a_{s_1}$

na notação tomada será α_1 e $a_{s_1-1}\dots a_1a_{s_0}$ será α_0. As congruências mencionadas serão da forma $w_0 \equiv 10^{s_0}\ mod(11)$ e $w_1 \equiv 10^{s_1}\ mod(11)$ Como $s_0 = 0$, tem-se a primeira congruência reduzida a

$$w_0 \equiv 1mod(11).$$

Ora, o conjunto das soluções de tal congruência é da forma $\{1 + 11u|u \in \mathbb{Z}\}$. Escolheremos como solução representativa o caso $u = 0$ que nos dá $w_0 = 1$.

Para $s_1 = 2$ a segunda congruência acima listada, reduz-se $w_1 \equiv 100\ mod(11)$, cujo o conjunto solução é $\{100 + 11u|u \in \mathbb{Z}\}$.

Para $u = -9$ teremos $w_1 = 1$ e para $u = -10$ teremos $w_1 = -10$. Outros valores de u trariam soluções desinteressantes para nossos propósitos. Portanto teremos as notações correspondentes para o caso em análise:

$$A_{11}(1,1)_{(2)} = \alpha_1 + \alpha_0 \text{ ou } A_{11}(-10,1)_{(2)} = -10\cdot\alpha_1 + \alpha_0.$$

No caso 1, estamos dizendo que na divisão por 11 em que a partição tomada para o número tem dois algarismos generalizados $\alpha_0 = a_1a_0$ e $\alpha_1 = a_t\dots a_2$, o número dado, reduz-se a forma $\alpha_1 + \alpha_0$. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 11 ocorre ou não. Consideremos $N = 2574$ com $h = 1$ e $s_1 = 2$, os elementos da partição serão: $\alpha_1 = 25$ e $\alpha_0 = 74$. Na notação tomada, tem-se

$$A_{11}(1,1)_{(2)} = \alpha_1 + \alpha_0;$$
$$A_{11}(1,1)_{(2)} = 25 + 74 = 99.$$

Conclusão é que, como 99 é divisível por 11, o número 2574 também é divisível por 11.

Exemplo 6:

Consideremos o caso em que $h = 2$ com p ainda igual a 11. Assim, substituindo os valores $p = 11$ e $h = 2$ na notação tomada temos:

$$A_p(w_h, \ldots, w_0)_{(s_h, \ldots, s_1)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_{11}(w_2, w_1, w_0)_{(s_2, s_1)} = \sum_{r=0}^{2} w_r \cdot \alpha_r;$$

$$A_{11}(w_2, w_1, w_0)_{(s_2, s_1)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0.$$

A partir $N = \left(\underbrace{a_t \ldots a_{s_2}}_{\alpha_2} | \underbrace{a_{s_2-1} \ldots a_{s_1}}_{\alpha_1} | \underbrace{a_{s_1-1} \ldots a_1 a_0}_{\alpha_{s_0}} \right)_{(s_2, s_1)}$ em que os algarismos generalizados tomados estão separadas pelas barras verticais, ou seja, $\alpha_0 = a_{s_1-1} \ldots a_1 a_{s_0}$, $\alpha_1 = a_{s_2-1} \ldots a_{s_1}$ e $\alpha_2 = a_{s_3-1} \ldots a_{s_2}$. Para este caso, as congruências tomadas são $w_0 \equiv 10^{s_0}\ mod(11)$, $w_1 \equiv 10^{s_1}\ mod(11)$ e $w_2 \equiv 10^{s_2}\ mod(11)$.

Considerando $s_1 = 2$ e $s_2 = 3$, tais congruências tem soluções triviais módulo 11 dadas por: $w_0 = 1, w_1 = 1$ e $w_2 = -1$ ou $w_0 = 1, w_1 = -10$ e $w_2 = 10$. Portanto, $A_{11}(-1, 1, 1)_{(3,2)} = -\alpha_2 + \alpha_1 + \alpha_0$ ou $A_{11}(10, -10, 1)_{(3,2)} = 10 \cdot \alpha_2 - 10 \cdot \alpha_1 + \alpha_0$.

Isto é, na divisão por 11 em que o número de classes da partição é 3, a saber, $\alpha_0 = a_1 a_0$, $\alpha_1 = a_2$ e $\alpha_2 = a_t \ldots a_3$. O número N se reduz às formas $-\alpha_2 + \alpha_1 + \alpha_0$ ou $10 \cdot \alpha_2 - 10 \cdot \alpha_1 + \alpha_0$.

Consideremos $N = 357.214$ com $h = 2, s_1 = 2$ e $s_2 = 3$, os elementos da partição serão: $\alpha_2 = 357, \alpha_1 = 2$ e $\alpha_0 = 14$. Na notação tomada, tem-se

$$A_{11}(-1, 1, 1)_{(3,2)} = -\alpha_2 + \alpha_1 + \alpha_0;$$

$$A_{11}(-1, 1, 1)_{(3,2)} = -357 + 2 + 14 = -341.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\alpha_2 = 0, \alpha_1 = 3$ e $\alpha_0 = 41$.

$$A_{11}(-1, 1, 1)_{(3,2)} = -0 + 3 + 41 = 44.$$

Conclusão é que, como 44 é divisível por 11, o número 357214 também é divisível por 11.

Exemplo 7:

Como exemplo, construiremos o critério de divisibilidade para os números 13 usando a expressão $A_p(w_2, w_1, w_0)_{(3,2)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0$, e depois verifiquemos a divisibilidade do mesmo aplicando-o em 13.241.798.

Primeiro vamos construir o critério para o número 13, ou seja, teremos que calcular os coeficientes w_0, w_1 e w_2.

Assim,

$$\begin{cases} w_0 \equiv 10^{s_0} \ mod(13) \\ w_1 \equiv 10^{s_1} \ mod(13) \\ w_2 \equiv 10^{s_2} \ mod(13) \end{cases}$$

$$\begin{cases} w_0 \equiv 10^{0} \ mod(13) \\ w_1 \equiv 10^{2} \ mod(13) \\ w_2 \equiv 10^{3} \ mod(13) \end{cases}$$

$$\begin{cases} w_0 \equiv 1 \ mod(13) \\ w_1 \equiv 9 \ mod(13) \\ w_2 \equiv 12 \ mod(13) \end{cases}$$

Portanto, $A_{13}(12, 9, 1)_{(3,2)} = 12 \cdot \alpha_2 + 9 \cdot \alpha_1 + \alpha_0$ ou $A_{13}(-1, -4, 1)_{(3,2)} = -\alpha_2 - 4 \cdot \alpha_1 + \alpha_0$.

Resta agora aplicarmos o critério obtido no número 13.241.798, os elementos da partição serão: $\alpha_2 = 13241, \alpha_1 = 7$ e $\alpha_0 = 98$. Na notação tomada, tem-se

$$A_{13}(-1, -4, 1)_{(3,2)} = -13241 - 4 \cdot 7 + 98 = -13171.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\alpha_2 = -13, \alpha_1 = -1$ e $\alpha_0 = -71$.

$$A_{13}(-1, -4, 1)_{(3,2)} = -(-13) - 4 \cdot (-1) + (-71) = -54.$$

A conclusão é que, como -54 não é divisível por 13, o número 13.241.798 também não é divisível por 13.

Exemplo 8:

Como exemplo, construiremos o critério de divisibilidade para os números 17 usando a expressão $A_p(w_2, w_1, w_0)_{(3,2)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0$, e depois verifiquemos a divisibilidade do mesmo aplicando-o em 23.251.793.

Primeiro vamos construir o critério para o número 13, ou seja, teremos que calcular os coeficientes w_0, w_1 e w_2.

Assim,

$$\begin{cases} w_0 \equiv 10^{s_0} \ mod(17) \\ w_1 \equiv 10^{s_1} \ mod(17) \\ w_2 \equiv 10^{s_2} \ mod(17) \end{cases}$$

$$\begin{cases} w_0 \equiv 10^{0} \ mod(17) \\ w_1 \equiv 10^{2} \ mod(17) \\ w_2 \equiv 10^{3} \ mod(17) \end{cases}$$

$$\begin{cases} w_0 \equiv 1 \ mod(17) \\ w_1 \equiv 15 \ mod(17) \\ w_2 \equiv 14 \ mod(17) \end{cases}$$

Portanto, $A_{17}(14, 15, 1)_{(3,2)} = 14 \cdot \alpha_2 + 15 \cdot \alpha_1 + \alpha_0$ ou $A_{17}(-3, -2, 1)_{(3,2)} = -3 \cdot \alpha_2 - 2 \cdot \alpha_1 + \alpha_0$.

Aplicando o critério encontrado em 23.251.793, logo os elementos da partição serão: $\alpha_2 = 23251, \alpha_1 = 7$ e $\alpha_0 = 93$. Na notação tomada, tem-se

$$A_{17}(-3, -2, 1)_{(3,2)} = -3 \cdot 23251 - 2 \cdot 7 + 93 = -69674.$$

Replicando o método, os elementos da partição tomada, terá como elementos

$\alpha_2 = -69, \alpha_1 = -6$ e $\alpha_0 = -74$.

$$A_{17}(-3,-2,1)_{(3,2)} = -3 \cdot (-69) - 2 \cdot (-6) + (-74) = -145.$$

Replicando mais uma vez o método, os elementos da partição tomada, terá como elementos $\alpha_2 = 0, \alpha_1 = -1$ e $\alpha_0 = -45$.

$$A_{17}(-3,-2,1)_{(3,2)} = -3 \cdot 0 - 2 \cdot (-1) + (-45) = -43.$$

Conclusão é que, como -43 não é divisível por 17, o número 23.251.793 também não é divisível por 17.

Exemplo 9:

Como exemplo, construiremos o critério de divisibilidade para os números 19 usando a expressão $A_p(w_2, w_1, w_0)_{(3,2)} = w_2 \cdot \alpha_2 + w_1 \cdot \alpha_1 + w_0 \cdot \alpha_0$, e depois verifiquemos a divisibilidade do mesmo aplicando-o em 23.251.793.

Primeiro vamos construir o critério para o número 19, ou seja, teremos que calcular os coeficientes w_0, w_1 e w_2.

Assim,

$$\begin{cases} w_0 \equiv 10^{s_0} \ mod(19) \\ w_1 \equiv 10^{s_1} \ mod(19) \\ w_2 \equiv 10^{s_2} \ mod(19) \end{cases}$$

$$\begin{cases} w_0 \equiv 10^{0} \ mod(19) \\ w_1 \equiv 10^{2} \ mod(19) \\ w_2 \equiv 10^{3} \ mod(19) \end{cases}$$

$$\begin{cases} w_0 \equiv 1 \ mod(19) \\ w_1 \equiv 5 \ mod(19) \\ w_2 \equiv 12 \ mod(19) \end{cases}$$

Portanto, $A_{19}(12,5,1)_{(3,2)} = 12 \cdot \alpha_2 + 5 \cdot \alpha_1 + \alpha_0$ ou $A_{13}(-6,5,1)_{(3,2)} = -6 \cdot \alpha_2 + 5 \cdot \alpha_1 + \alpha_0$.

Agora aplicaremos o critério obtido no número 23.251.793. Assim, os elementos da partição serão: $\alpha_2 = 23251, \alpha_1 = 7$ e $\alpha_0 = 93$, que substituindo na notação tomada, tem-se

$$A_{19}(-6, 5, 1)_{(3,2)} = -6 \cdot 23251 + 5 \cdot 7 + 93 = -139448.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\alpha_2 = -139, \alpha_1 = -4$ e $\alpha_0 = -48$.

$$A_{19}(-6, 5, 1)_{(3,2)} = -6 \cdot (-139) + 5 \cdot (-4) + (-48) = -766.$$

Replicando mais uma vez o método, os elementos da partição tomada, terá como elementos $\alpha_2 = 0, \alpha_1 = -7$ e $\alpha_0 = -66$.

$$A_{19}(-6, 5, 1)_{(3,2)} = -6 \cdot 0 + 5 \cdot (-7) + (-66) = -101.$$

Replicando novamente o método, os elementos da partição tomada, terá como elementos $\alpha_2 = 0, \alpha_1 = -1$ e $\alpha_0 = -01$.

$$A_{19}(-6, 5, 1)_{(3,2)} = -6 \cdot 0 + 5 \cdot (-1) + (-01) = -6.$$

Conclusão é que, como -6 não é divisível por 19, o número 23.251.793 também não é divisível por 19.

A seguir, enunciaremos e demonstraremos o Corolário 1 do Teorema 3.1 que nos permitirá gerar critérios que dará o resto na divisibilidade por p, usando o método Alfa.

3.3.2 Corolário 1 do Teorema 3.1: Resto na divisibilidade por p usando o método Alfa.

No método Alfa, N deixa resto R na divisão por p se, e somente se, $\sum_{r=0}^{h} w_r \cdot \alpha_r$ deixa resto R na divisão por p.

Demonstração:

($\Rightarrow$): Como $N \equiv \sum_{r=0}^{h} w_r \cdot \alpha_r mod(p)$ e $N \equiv R\, mod(p)$, logo teremos que $\sum_{r=0}^{h} w_r \cdot \alpha_r \equiv N \equiv R\, mod(p)$.

($\Leftarrow$): Como $N \equiv \sum_{r=0}^{h} w_r \cdot \alpha_r mod(p)$ e $\sum_{r=0}^{h} w_r \cdot \alpha_r \equiv R\ mod(p)$, logo teremos que $N \equiv \sum_{r=0}^{h} w_r \cdot \alpha_r \equiv R\ mod(p)$.

Assim, concluímos que N deixa resto R na divisão por p se, e somente se, $\sum_{r=0}^{h} w_r \cdot \alpha_r$ deixa resto R na divisão por p.

Portanto, o método gerador de critério de divisibilidade do tipo Alfa dá o resto na divisibilidade por p.

$\blacksquare$

A seguir, enunciaremos e demonstraremos o Corolário 2 do Teorema 3.1 que nos permitirá gerar critérios de divisibilidade para números p que divide o valor da expressão $10^v - b$.

3.3.3 Corolário 2 do Teorema 3.1: Divisibilidade por p, com p pertencente a $D(10^v - b)$.

No Teorema 3.1, considere $P = \{hv, \ldots, 3v, 2v, v\}$ e $p \in D(10^v - b) = \{p : p|10^v - b, v \in \mathbb{N}^*, p > 1\}$, com $b \in \mathbb{Z}$. Então p divide N se, somente se, p divide $\sum_{r=0}^{h} b^r \cdot \alpha_r$.

Demonstração:

Considere $p \in D(10^v - b)$, ou seja, $10^v \equiv b\ mod(p)$, logo teremos:

$$w_r \equiv 10^{r \cdot v} mod(p);$$

$$w_r \equiv (10^v)^r mod(p);$$

$$w_r \equiv b^r mod(p).$$

Assim,

$$A_p(w_h, \ldots, w_0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} w_r \cdot \alpha_r;$$

$$A_p(b^h, \ldots, b^0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} b^r \cdot \alpha_r.$$

Portanto, p divide N se, somente se, p divide $\sum_{r=0}^{h} b^r \cdot \alpha_r$.

Com isso, temos uma expressão prática para gerar critérios de divisibilidade do tipo Alfa com a seguinte fórmula $A_p(b^h, \ldots, b^0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} b^r \cdot \alpha_r$.

$\blacksquare$

Exemplos:

1) Como exemplo, construiremos o critério de divisibilidade para o número 49, usando a expressão $A_p(b^h, \ldots, b^0)_{(hv,\ldots,3v,2v,v)} = \displaystyle\sum_{r=0}^{h} b^r \cdot \alpha_r$ e verificando a seguir sua aplicação para o número 23.251.793.

Como $p = 49$, logo $v = 2$ segue do método que:

$$10^v \equiv b \ mod(p);$$

$$10^2 \equiv b \ mod(49);$$

$$b \equiv 2 \ mod(49).$$

Assim, a expressão acima fica:

$$A_{49}(2^h, \ldots, 2^0)_{(2h,\ldots,4,2)} = \sum_{r=0}^{h} 2^r \cdot \alpha_r.$$

Para $N = 23.251.793$ o bom é tomarmos $h = 3$.

A expressão reduz-se a:

$$A_{49}(2^3, 2^2, 2^1, 2^0)_{(6,4,2)} = \sum_{r=0}^{3} 2^r \cdot \alpha_r.$$

Aqui:

$\alpha_0 = 93$, $\alpha_1 = 17$, $\alpha_2 = 25$ e $\alpha_3 = 23$ e portanto ficamos com:

$$A_{49}(8, 4, 2, 1)_{(6,4,2)} = 8 \cdot 23 + 4 \cdot 25 + 2 \cdot 17 + 1 \cdot 93 = 411.$$

Resta tomar h = 1. Logo: $\alpha_0 = 11$ e $\alpha_1 = 4$.

$$A_{49}(2,1)_{(2)} = 2 \cdot 4 + 1 \cdot 11 = 19.$$

Verificando que N não é divisível por 49.

Nota-se, como dissemos na introdução, a iteratividade do método e sua rapidez de definição: com apenas dois passos, reduzimos a divisibilidade de $N = 23.251.793$ por 49 à divisibilidade de 19 por 49.

2) Como exemplo, construiremos o critério de divisibilidade para o número 102, usando a expressão $A_p(b^h, \ldots, b^0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} b^r \cdot \alpha_r$ e verificando a seguir sua aplicação para o número 23.251.793.

Como $p = 102$, logo $v = 2$ segue do método que:

$$10^v \equiv b \; mod(p);$$

$$10^2 \equiv b \; mod(102);$$

$$b \equiv -2 \; mod(102).$$

Assim, a expressão acima fica:

$$A_{102}((-2)^h, \ldots, (-2)^0)_{(2h,\ldots,4,2)} = \textstyle\sum_{r=0}^{h} (-2)^r \cdot \alpha_r.$$

Para $N = 23.251.793$ o bom é tomarmos $h = 3$.

A expressão reduz-se a:

$$A_{102}((-2)^3, (-2)^2, (-2)^1, (-2)^0)_{(6,4,2)} = \textstyle\sum_{r=0}^{3} (-2)^r \cdot \alpha_r.$$

Aqui:

$\alpha_0 = 93$, $\alpha_1 = 17$, $\alpha_2 = 25$ e $\alpha_3 = 23$ e portanto ficamos com:

$$A_{102}(-8, 4, -2, 1)_{(6,4,2)} = -8 \cdot 23 + 4 \cdot 25 - 2 \cdot 17 + 1 \cdot 93 = -25.$$

Verificando que N não é divisível por 102.

Nota-se, como dissemos na introdução, a iteratividade do método e sua rapidez de definição: com apenas um passo, reduzimos a divisibilidade de $N = 23.251.793$ por 102 à divisibilidade de -25 por 102.

Nos corolários 3 a 10 do teorema 3.1, mostraremos alguns critérios de divisibilidade tradicional revisitados.

A seguir, enunciaremos e demonstraremos o Corolário 3 do Teorema 3.1 que nos permitirá gerar critérios de divisibilidade para números da forma $2^v \cdot 5^u$.

3.3.4 Corolário 3 do Teorema 3.1: Divisibilidade por $\mathbf{p} = 2^v \cdot 5^u$.

No Teorema 3.1, considere $P = \{s_1\}$ e $p = 2^v \cdot 5^u$, com $s_1 \geq max\{u, v\} \geq 1$. Então $2^v \cdot 5^u$ divide N se, e somente se, $2^v \cdot 5^u$ divide α_0.

Demonstração:

Note que $p = 2^v \cdot 5^u \in D(10^{max\{u,v\}} - 0)$, logo pelo corolário 2 do Teorema 3.1, teremos:

$$A_{2^v . 5^u}(b^1, b^0)_{(s_1)} = b^1 \cdot \alpha_1 + b^0 \cdot \alpha_0;$$

$$A_{2^v . 5^u}(0, 1)_{(s_1)} = 0 \cdot \alpha_1 + 1 \cdot \alpha_0.$$

Assim,

$$A_{2^v . 5^u}(0, 1)_{(s_1)} = \alpha_0.$$

Portanto, concluímos que $2^v \cdot 5^u$ divide N se, e somente se, $2^v \cdot 5^u$ divide α_0.

$\blacksquare$

A seguir, enunciaremos e demonstraremos os critérios de divisibilidade para números da forma 2^v.

3.3.5 Corolário 4 do Teorema 3.1: Divisibilidade por $\mathbf{p} = 2^v$.

No Teorema 3.1, considere $P = \{s_1\}$ e $p = 2^v$, com $s_1 \geq v \geq 1$. Então 2^v divide N se, e somente se, 2^v divide α_0.

Demonstração:

Note que $p = 2^v \in D(10^v - 0)$, logo pelo corolário 2 do Teorema 3.1, teremos:

$$A_{2^v}(b^1, b^0)_{(s_1)} = b^1 \cdot \alpha_1 + b^0 \cdot \alpha_0;$$

$$A_{2^v}(0, 1)_{(s_1)} = 0 \cdot \alpha_1 + 1 \cdot \alpha_0.$$

Assim,

$$A_{2^v}(0, 1)_{(s_1)} = \alpha_0.$$

Portanto, concluímos que 2^v divide N se, e somente se, 2^v divide α_0.

■

A seguir, enunciaremos e demonstraremos os critérios de divisibilidade para números da forma 5^v.

3.3.6 Corolário 5 do Teorema 3.1: Divisibilidade por $\mathbf{p} = 5^u$

No Teorema 3.1, considere $P = s_1$ e $p = 5^u$, com $s_1 \geq u \geq 1$. Então 5^u divide N se, e somente se, 5^u divide α_0.

Demonstração:

Análogo ao caso $p = 2^v$.

■

3.3.7 Corolário 6 do Teorema 3.1: Divisibilidade por 3.

No Teorema 3.1, considere $p = 3$. Então 3 divide N se, e somente se, 3 divide $\sum_{r=0}^{h} \alpha_r$.

Demonstração:

Note que $10 \equiv 1\ mod(3)$, logo $w_r \equiv 10^{s_r}\ mod(3) \equiv 1^{s_r}\ mod(3)$, $\forall r = 0, \ldots, h$.

Assim, teremos:

$$A_3(1^{s_h}, \ldots, 1^{s_0})_{(s_h, \ldots, s_1)} = \sum_{r=0}^{h} \alpha_r.$$

Portanto, 3 divide N se, e somente se, 3 divide $\sum_{r=0}^{h} \alpha_r$. Perceba que se $h = t$, então $\sum_{r=0}^{h} \alpha_r$ representa a soma dos dígitos de $N = a_t a_{t-1} \ldots a_1 a_0$.

■

A seguir, enunciaremos e demonstraremos um critério de divisibilidade por 9.

3.3.8 Corolário 7 do Teorema 3.1: Divisibilidade por 9.

No Teorema 3.1, considere $p = 9$. Então 9 divide N se, e somente se, 9 divide $\sum_{r=0}^{h} \alpha_r$.

Demonstração:

Note que $10 \equiv 1\ mod(3)$, logo $w_r \equiv 10^{s_r}\ mod(9) \equiv 1^{s_r}\ mod(9)$, $\forall r = 0, \ldots, h$.

Assim, teremos:

$$A_9(1^{s_h}, \ldots, 1^{s_0})_{(s_h, \ldots, s_1)} = \sum_{r=0}^{h} \alpha_r.$$

Portanto, 9 divide N se, e somente se, 9 divide $\sum_{r=0}^{h} \alpha_r$. Perceba que se $h = t$, então $\sum_{r=0}^{h} \alpha_r$ representa a soma dos dígitos de $N = a_t a_{t-1} \ldots a_1 a_0$.

■

A seguir, enunciaremos e demonstraremos um critério de divisibilidade por 11.

3.3.9 Corolário 8 do Teorema 3.1: Divisibilidade por 11.

No Teorema 3.1, considere $p = 11$. Então 11 divide N se, e somente se, 11 divide $\sum_{r=0}^{h} (-1)^{s_r} \cdot \alpha_r$.

Demonstração:

Note que $10 \equiv -1 \ mod(11)$, logo $w_r \equiv 10^{s_r} \ mod(11) \equiv (-1)^{s_r} \ mod(11)$, $\forall r = 0, \ldots, h$.

Assim, teremos:

$$A_{11}((-1)^{s_h}, \ldots, (-1)^{s_0})_{(s_h, \ldots, s_1)} = \sum_{r=0}^{h} (-1)^{s_r} \cdot \alpha_r.$$

Portanto, 11 divide N se, e somente se, 11 divide $\sum_{r=0}^{h} (-1)^{s_r} \cdot \alpha_r$. Perceba que se $h = t$, então $\sum_{r=0}^{h} (-1)^{s_r} \cdot \alpha_r$ representa a diferença entre as somas dos dígitos de ordens impares com os de ordens pares de $N = a_t a_{t-1} \ldots a_1 a_0$.

■

3.3.10 Corolário 9 do Teorema 3.1: Divisibilidade por p, com p pertencente ao conjunto D(10^v - 1).

No Teorema 3.1, considere $P = \{hv, \ldots, 3v, 2v, v\}$ e $p \in D(10^v - 1) = \{p : p | 10^v - 1, v \in \mathbb{N}^*, p > 1\}$. Então p divide N se, e somente se, p divide $\sum_{r=0}^{h} \alpha_r$.

Demonstração:

Note que $p \in D(10^v - 1)$, logo pelo corolário 2 do Teorema 3.1, teremos:

$$A_p(b^h, \ldots, b^0)_{(hv, \ldots, 3v, 2v, v)} = \sum_{r=0}^{h} b^r \cdot \alpha_r;$$

$$A_p(1^h, \ldots, 1^0)_{(hv, \ldots, 3v, 2v, v)} = \sum_{r=0}^{h} \alpha_r.$$

Portanto, concluímos que p divide N se, somente se, p divide $\sum_{r=0}^{h} \alpha_r$.

■

3.3.11 Corolário 10 do Teorema 3.1: Divisibilidade por p, com p pertencente ao conjunto $D(10^v + 1)$.

No Teorema 3.2, considere $P = \{hv, \ldots, 3v, 2v, v\}$ e $p \in D(10^v + 1) = \{p : p|10^v + 1, v \in \mathbb{N}^*, p > 1\}$. Então p divide N se, e somente se, p divide $\sum_{r=0}^{h} (-1)^r \cdot \alpha_r$.

Demonstração:

Note que $p \in D(10^v + 1)$, logo pelo corolário 2 do Teorema 3.1, teremos:

$$A_p(b^h, \ldots, b^0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} b^r \cdot \alpha_r;$$
$$A_p((-1)^h, \ldots, (-1)^0)_{(hv,\ldots,3v,2v,v)} = \sum_{r=0}^{h} (-1)^r \cdot \alpha_r.$$

Portanto, concluímos que p divide N se, somente se, p divide $\sum_{r=0}^{h} (-1)^r \alpha_r$.

∎

3.4 Método Gerador de Critérios de Divisibilidade do tipo Beta

Na subseção 3.5.1 desenvolveremos no teorema 3.2 os condicionantes do método gerador a que chamamos de tipo Beta. Aborda-se então, de modo sistemático, a geração de critérios de divisibilidade para números terminados em 1, 3, 7 ou 9. No caso, a notação tem significado semelhante àquela adotada para o método Alfa. O método se justifica, pois agora temos uma forma diferente de cálculo para os coeficientes. Vale salientar que a ideia está proposta no artigo em Guedes (1988, p. 24-27) escrito para a Revista do Professor de Matemática.

Como por uma questão didática, no método Alfa os algarismos generalizados foram representados por α_r's, e pela mesma razão representaremos os algarismos generalizados no método Beta por β_j's.

Vamos obter critérios de divisibilidade para números p naturais maiores que 1 terminados em 1, 3, 7, 9. Assim, se considerarmos $\beta_0, \beta_1, \ldots, \beta_m$ algarismos generalizados de um número natural N com respeito a partição $P = \{s_m, \ldots, s_1\}$ e supusermos $10^{s_m - s_j} \cdot k_j \equiv 1 \ mod(p)$ com $k_j \in \mathbb{Z}$, então o método consiste em analisar a congruência $N \equiv \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j \ mod(p)$. Demonstraremos o fato na subseção 3.5.1, como exemplo esclarecedor, consideremos a partição $P = \{3, 2\}$. Neste caso teremos três algarismos generalizados β_0, β_1 e β_2 conforme a partição $N = \left(\underbrace{a_t \ldots a_3}_{\beta_2} | \underbrace{a_2}_{\beta_1} | \underbrace{a_1 a_0}_{\beta_0} \right)_{(3,2)}$

Assim,

$$N = 10^3 \cdot \beta_2 + 10^2 \cdot \beta_1 + 10^0 \cdot \beta_0. \tag{1}$$

Fixada a partição $P = \{3, 2\}$ de N, construir o M da seguinte forma:

$$M = \beta_2 + k_1 \cdot \beta_1 + k_0 \cdot \beta_0. \tag{2}$$

Logo, por (1) e (2), temos que,

$$N = 10^3 \cdot (M - k_1 \cdot \beta_1 - k_0 \cdot \beta_0) + 10^2 \cdot \beta_1 + 10^0 \cdot \beta_0;$$
$$N = 10^3 \cdot M + 10^2 \cdot (1 - 10^{3-2} \cdot k_1) \cdot \beta_1 + 10^0 \cdot (1 - 10^{3-0} \cdot k_0) \cdot \beta_0.$$

Se supusermos que $1 - 10^{3-2} \cdot k_1 \equiv 0 \ mod(p)$ e $1 - 10^{3-0} \cdot k_0 \equiv 0 \ mod(p)$, logo temos pelos Lemas 3.1 e 3.2 que $p|N$ se, e somente se $p|M$.

$$N = 10^3 \cdot M + 10^2 \cdot (1 - 10^{3-2} \cdot k_1) \cdot \beta_1 + 10^0 \cdot (1 - 10^{3-0} \cdot k_0) \cdot \beta_0;$$
$$N \equiv 10^3 \cdot M \ mod(p);$$
$$N \equiv M \ mod(p).$$

Logo, p divide N se, e somente se, p divide M.

Portanto, é M que define o método gerador de critérios de divisibilidade para o tipo Beta. Para $p = 11$ e $P = \{3, 2\}$, temos que,

$$\begin{cases} 1 - 10^{3-2} \cdot k_1 \equiv 0 \ mod(p) \\ 1 - 10^{3-0} \cdot k_0 \equiv 0 \ mod(p) \end{cases}$$

$$\begin{cases} 1 - 10 \cdot k_1 \equiv 0 \; mod(11) \\ 1 - 10^3 \cdot k_0 \equiv 0 \; mod(11) \end{cases}$$

$$\begin{cases} k_1 \equiv -1 \; mod(11) \\ k_0 \equiv -1 \; mod(11) \end{cases}$$

Neste caso, estamos dizendo que na divisão por 11 em que a partição tomada para o número tem três algarismos generalizados $\beta_0 = a_1 a_0$, $\beta_1 = a_2$ e $\beta_2 = a_t \dots a_3$, o número dado, reduz-se a forma $\beta_2 - \beta_1 - \beta_0$. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 11 ocorre ou não.

Um exemplo numérico seria verificar se o número $N = 345.216$ é divisível por $p = 11$. Utilizando a partição já dada $P = \{3, 2\}$, temos os algarismos generalizados $\beta_2 = 345$, $\beta_1 = 2$ e $\beta_0 = 16$. A partir de $\beta_2 - \beta_1 - \beta_0$ temos:

$$\beta_2 - \beta_1 - \beta_0 = 345 - 2 - 16;$$

$$\beta_2 - \beta_1 - \beta_0 = 327.$$

Replicando o método em 327, temos $\beta_2 = 0$, $\beta_1 = 3$ e $\beta_0 = 27$:

$$\beta_2 - \beta_1 - \beta_0 = 0 - 3 - 27;$$

$$\beta_2 - \beta_1 - \beta_0 = -30.$$

Como -30 não é divisível por 11, então 345.216 também não é.

De fato, o método e a notação usada por nós, recebe consolidação com o que já está demonstrado às páginas 24 a 27 da R.P.M. 12, que considera o conjunto partição $P = \{1\}$. Neste caso teremos dois algarismos generalizados β_0 e β_1 conforme a partição $N = \left(\underbrace{a_t \dots a_1}_{\beta_1} | \underbrace{a_0}_{\beta_0} \right)_{(1)}$.

Assim,

$$N = 10^1 \cdot \beta_1 + 10^0 \cdot \beta_0. \tag{3}$$

Fixada a partição $P = \{1\}$ de N, construir o M da seguinte forma:

$$M = \beta_1 + k_0 \cdot \beta_0. \tag{4}$$

Logo, por (3) e (4), temos que,

$$N = 10^1 \cdot (M - k_0 \cdot \beta_0) + 10^0 \cdot \beta_0;$$
$$N = 10^1 \cdot M + 10^0 \cdot (1 - 10^{1-0} \cdot k_0) \cdot \beta_0.$$

Se supusermos que $1 - 10^{1-0} \cdot k_0 \equiv 0 mod(p)$, logo temos pelos Lemas 3.1 e 3.2 que $p|N$ se, e somente se $p|M$

$$N \equiv 10^1 \cdot M + 10^0 \cdot (1 - 10^{1-0} \cdot k_0) \cdot \beta_0 \ mod(p);$$
$$N \equiv 10^{1-0} \cdot M \ mod(p).$$

Logo, p divide N se, e somente se, p divide M.

Portanto, é M que define o método gerador de critérios de divisibilidade para o tipo Beta, como já visto no exemplo anterior.

Para $p = 7$, temos que,

$$1 - 10 \cdot k_0 \equiv 0 \ mod(7);$$
$$k_0 \equiv 5 \ mod(7).$$

Neste caso, estamos dizendo que na divisão por 7 em que a partição tomada para o número tem três algarismos generalizados $\beta_0 = a_0$ e $\beta_1 = a_t \dots a_1$, o número dado, reduz-se as formas $\beta_1 - 2 \cdot \beta_0$ e $\beta_1 + 5 \cdot \beta_0$ O processo pode ser repetido até ter-se clareza de se a divisibilidade por 7 ocorre ou não.

Um exemplo numérico seria verificar se o número $N = 345.216$ é divisível por $p = 7$. Utilizando a partição já dada $P = \{1\}$, temos os algarismos generalizados $\beta_1 = 34521$ e $\beta_0 = 6$. A partir de $\beta_1 - 2 \cdot \beta_0$ temos:

$$\beta_1 - 2 \cdot \beta_0 = 34521 - 2 \cdot 6,$$
$$\beta_1 - 2 \cdot \beta_0 = 34509.$$

Replicando o método em 34509, temos $\beta_1 = 3450$ e $\beta_0 = 9$:

$$\beta_1 - 2 \cdot \beta_0 = 3450 - 2 \cdot 9;$$
$$\beta_1 - 2 \cdot \beta_0 = 3432.$$

Replicando novamente o método em 3432, temos $\beta_1 = 3430$ e $\beta_0 = 2$:

$$\beta_1 - 2 \cdot \beta_0 = 342 - 2 \cdot 2;$$
$$\beta_1 - 2 \cdot \beta_0 = 338.$$

Replicando mais uma vez o método em 338, temos $\beta_1 = 33$ e $\beta_0 = 8$:

$$\beta_1 - 2 \cdot \beta_0 = 33 - 2 \cdot 8;$$
$$\beta_1 - 2 \cdot \beta_0 = 17.$$

Como 17 não é divisível por 7, então 345.216 também não é. Vamos então à demonstração do método.

3.4.1 Teorema 3.2: Método Gerador de Critérios de Divisibilidade do tipo Beta

Considere p número natural maior que 1 com algarismo da unidade 1, 3, 7 ou 9. Sejam β_0, β_1, ... ,β_m algarismos generalizados de um número natural N com respeito a partição $P = \{s_m, \ldots, s_1\}$, e defina $M = \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j$, com $k_j \in \mathbb{Z}$ tal que $10^{s_m - s_j} \cdot k_j \equiv 1\ mod(p)$. Então, p divide N se, e somente se, p divide $\beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j$.

Demonstração:

Seja p um número natural maior que um, terminado em 1, 3, 7 ou 9. Note que existem k_j tais que $p|1 - 10^{s_m - s_j} \cdot k_j$, $\forall\ j = 0, 1, \ldots, m-1$. Considere $\beta_0 = (a_{s_1-1} \ldots a_1 a_{s_0})_{10}$, $\beta_1 = (a_{s_2-1} \ldots a_{s_1})_{10}, \ldots, \beta_{m-1} = (a_{s_m-1} \ldots a_{s_{m-1}})_{10}$ e $\beta_m = (a_t \ldots a_{s_m})_{10}$ algarismos generalizados de N com respeito a partição $P = \{s_m, \ldots, s_1\}$, logo semelhante ao método Alfa, estamos "particionando" N em $m+1$ algarismos generalizados, como na ilustração a seguir:

$$N = \left(\underbrace{a_t \ldots a_{s_m}}_{\beta_m} | \underbrace{a_{s_m-1} \ldots a_{s_{m-1}}}_{\beta_{m-1}} | \ldots | \underbrace{a_{s_2-1} \ldots a_{s_1}}_{\beta_1} | \underbrace{a_{s_1-1} \ldots a_1 a_0}_{\beta_0} \right)_{(s_m, \ldots, s_1)}.$$

Logo, pela definição 2 temos que,

$$N = \beta_m \cdot 10^{s_m} + \sum_{j=0}^{m-1} 10^{s_j} \cdot \beta_j. \tag{1}$$

Fixada a partição P de N, construir o M da seguinte forma:

$$M = \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j, \text{ com } k_j \in \mathbb{Z}. \tag{2}$$

Assim, por (1) e (2), temos que,

$$N = M \cdot 10^{s_m} + \sum_{j=0}^{m-1} 10^{s_j} \cdot (1 - 10^{s_m - s_j} \cdot k_j) \cdot \beta_j, \text{ com } s_0 = 0.$$

Como já sabemos, o processo se resume em achar os números k_j tal que N seja um múltiplo do número P se, e somente se, M for múltiplo de P.

Ora, como sabemos p divide $1 - 10^{s_m - s_j} \cdot k_j$ e $m.d.c.(p, 10) = 1$, logo pelos lemas 2.2 e 2.3 aplicados a expressão $N = M \cdot 10^{s_m} + \sum_{j=0}^{m-1} 10^{s_j} \cdot (1 - 10^{s_m - s_j} \cdot k_j) \cdot \beta_j$, então deduzimos que p divide N se, e somente se, p divide M.

Assim, obtidos os coeficientes $k_0, \ldots, k_{m-1}$, usando a equação $10^{s_m - s_j} \cdot k_j \equiv 1$ $mod(p)$, temos que $p|N \Leftrightarrow p|\beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j$. Desta forma para cada escolha dos k_j's, criamos um critério de divisibilidade por p aplicado a qualquer número natural N.

Utilizaremos a seguinte notação,

$$B_p(1, k_{m-1}, \ldots, k_0)_{(s_m, \ldots, s_1)} = \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j.$$

Que representa o critério de divisibilidade por p, do tipo Beta, aplicado ao número N, definida pelos coeficientes $1, k_{m-1}, \ldots, k_0$ dos algarismos generalizados $\beta_m, \ldots, \beta_0$ conforme partição $P = \{s_m, \ldots, s_1\}$ de N.

$\blacksquare$

Perceba que esta notação é análoga a notação do método Alfa. Queremos crer que a notação tomada, nesse caso, bem como no caso Alfa, carregam em si a essência da demonstração dos teoremas formatadores dos métodos, sendo por eles explicada.

A escolha deste método Beta se justifica, no que pese a evidente similaridade dele com o método Alfa. De fato, em determinados casos, o método Alfa falha ou por não conduzir a valores de N menores, para análise da sua divisibilidade por p, ou por deixar N fixo. Por exemplo, consideremos $p = 31$. Temos que, pelo método Alfa, se $N = a_t a_{t-1} \dots a_1 a_0$ em que a partição tomada seja com os algarismos generalizados $\alpha_1 = a_t a_{t-1} \dots a_1$ e $\alpha_0 = a_0$, então obteremos $w_0 = 1$ e $w_1 \equiv 10^{s_1}\ mod(31)$, isto é, $w_1 \equiv 10$ $mod(31)$.

Portanto,

$$w_1 \equiv 10 + 31 \cdot u, u \in \mathbb{Z}.$$

Valores "bons" para u seriam $u = 0$ ou $u = -1$, o que determinariam $w_1 = 10$ ou $w_1 = -21$.

Nestes casos teríamos $A_{31}(10, 1)_{(1)} = 10 \cdot \alpha_1 + \alpha_0$ que é o próprio N ou $A_{31}(-21, 1)_{(1)} = -21 \cdot \alpha_1 + \alpha_0$, que tem valor absoluto maior que N.

Em ambos os casos, o método falha no sentido indicado.

Agora, é fácil ver que $B_{31}(1, 28)_{(1)} = \beta_1 + 28 \cdot \beta_0$ ou $B_{31}(1, -3)_{(1)} = \beta_1 - 3 \cdot \beta_0$ dão valores menores que N.

Isto é, o método Beta aplicado à mesma divisão por 31 em que N é tomado com iguais algarismos generalizados de partição que no método Alfa, apresenta diminuição dos valores para sua reaplicação, sendo pois, vantajoso neste caso.

Vejamos alguns exemplos detalhados de como usar o método para facilitar a compreensão da teoria desenvolvida até agora:

Exemplo 1:

Consideremos, por exemplo, $p = 7$. Analisemos o caso em que $m = 1$. Neste caso só teremos β_0 e β_1 a discutir. No caso, a partição referida terá a forma $N = \left(\underbrace{a_t \dots a_{s_1}}_{\beta_1} | \underbrace{a_{s_1-1} \dots a_1 a_{s_0}}_{\beta_0}\right)_{(s_1)}$, em que $a_{s_2-1} \dots a_{s_1}$ na notação tomada será β_1 e $a_{s_1-1} \dots a_1 a_0$ será β_0. As congruências mencionadas serão da forma $10^{s_1} \cdot k_0 \equiv 1\ mod(7)$ e

$10^0 \cdot k_1 \equiv 1 \; mod(7)$.

No caso $s_1 = 1$ tem-se a primeira congruência reduzida a

$$10 \cdot k_0 \equiv 1 \; mod(7).$$

Ora, o conjunto das soluções de tal congruência é da forma $\{5 + 7u | u \in \mathbb{Z}\}$. Escolheremos como solução representativa, o caso $u = 0$ que nos dá $k_0 = 5$ e para $u = -1$ teremos $k_0 = -2$. Outros valores de u trariam soluções desinteressantes para nossos propósitos.

Para a segunda congruência acima listada, reduz-se $k_1 \equiv 1 \; mod(7)$, cujo o conjunto solução é $\{1 + 7u | u \in \mathbb{Z}\}$.

Para $u = 0$ teremos $k_1 = 1$. Portanto teremos as notações correspondentes para o caso em análise:

$$B_7(1, 5)_{(1)} = \beta_1 + 5 \cdot \beta_0 \text{ ou } B_7(1, -2)_{(1)} = \beta_1 - 2 \cdot \beta_0.$$

No caso 1, estamos dizendo que na divisão por 7 em que a partição tomada para o número tem duas classes β_0 e β_1, o número dado, reduz-se a forma $\beta_1 + 5 \cdot \beta_0$. O processo pode ser repetido até ter-se clareza de se a divisibilidade por 7 ocorre ou não.

Exemplo 2:

Consideremos o caso em que $h = 2$ com p ainda igual a 7.

A partição de N agora é $N = \left(\underbrace{a_t \dots a_{s_2}}_{\beta_2} | \underbrace{a_{s_2-1} \dots a_{s_1}}_{\beta_1} | \underbrace{a_{s_1-1} \dots a_1 a_{s_0}}_{\beta_0} \right)_{(s_2, s_1)}$ onde as classes tomadas estão separadas pelas barras verticais, ou seja $\beta_0 = a_{s_1-1} \dots a_1 a_0$, $\beta_1 = a_{s_2-1} \dots a_{s_1}$ e $\beta_2 = a_t \dots a_{s_2}$. Para este caso, as congruências tomadas são $10^{s_m - s_0} \cdot k_0 \equiv 1 \; mod(7)$, $10^{s_m - s_1} \cdot k_1 \equiv 1 \; mod(7)$ e $10^{s_m - s_2} \cdot k_2 \equiv 1 \; mod(7)$.

Considerando $s_1 = 2$ e $s_2 = 3$, tais congruências tem soluções módulo 7 dadas por: $k_0 = -1$, $k_1 = -2$ e $k_2 = 1$ ou $k_0 = 6$, $k_1 = 5$ e $k_2 = 1$. Portanto,$B_7(1, -2, 1)_{(1,2)} = \beta_2 - 2 \cdot \beta_1 - \beta_0$ ou $B_7(1, 5, 6)_{(1,2)} = \beta_2 + 5 \cdot \beta_1 + 6 \cdot \beta_0$. Isto é, na divisão por 7 em que o número de classes da partição é 3, a saber, β_0, β_1 e β_2. O número N se reduz às formas $\beta_2 - 2 \cdot \beta_1 - \beta_0$ ou $\beta_2 + 5 \cdot \beta_1 + 6 \cdot \beta_0$.

Consideremos $N = 357214$ com $h = 2$, $s_1 = 2$ e $s_2 = 3$, os elementos da partição serão: $\beta_2 = 357$, $\beta_1 = 2$ e $\beta_0 = 14$. Na notação tomada, tem-se

$$B_7(1,-2,1)_{(1,2)} = \beta_2 - 2 \cdot \beta_1 - \beta_0;$$

$$B_7(1,-2,1)_{(1,2)} = 357 - 2 \cdot 2 - 14 = 339.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\beta_2 = 0$, $\beta_1 = 3$ e $\beta_0 = 39$.

$$B_7(1,-2,1)_{(1,2)} = 0 - 2 \cdot 3 - 39 = -45.$$

Conclusão é que, como 45 não é divisível por 7, o número 357214 também não é divisível por 7.

Exemplo 3:

Construiremos o critério de divisibilidade para o número 13 usando a expressão $B_p(k_2, k_1, k_0)_{(3,2)} = k_2 \cdot \beta_2 + k_1 \cdot \beta_1 + k_0 \cdot \beta_0$, e depois verifiquemos a divisibilidade do mesmo aplicando-o em 13.241.798. Primeiro vamos construir o critério para o número 13, ou seja, teremos que calcular os coeficientes k_0, k_1 e k_2.

Assim,

$$\begin{cases} 10^{s_2 - s_0} \cdot k_0 \equiv 1 \ mod(13) \\ 10^{s_2 - s_1} \cdot k_1 \equiv 1 \ mod(13) \\ 10^{s_2 - s_2} \cdot k_2 \equiv 1 \ mod(13) \end{cases}$$

$$\begin{cases} 10^3 \cdot k_0 \equiv 1 \ mod(13) \\ 10^1 \cdot k_1 \equiv 1 \ mod(13) \\ 10^0 \cdot k_2 \equiv 1 \ mod(13) \end{cases}$$

$$\begin{cases} k_0 \equiv 12 \ mod(13) \\ k_1 \equiv 4 \ mod(13) \\ k_2 \equiv 1 \ mod(13) \end{cases}$$

Portanto, $B_{13}(1,4,12)_{(3,2)} = \beta_2+4\cdot\beta_1+12\cdot\beta_0$ ou $B_{13}(1,4,-1)_{(3,2)} = \beta_2+4\cdot\beta_1-\beta_0$.

Resta agora aplicarmos o critério encontrado em 13.241.798, os elementos da partição serão: $\beta_2 = 13241$, $\beta_1 = 7$ e $\beta_0 = 98$. Na notação tomada, tem-se

$$B_{13}(1,4,-1)_{(3,2)} = 13241 + 4 \cdot 7 - 98 = 13171.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\beta_2 = 13$, $\beta_1 = 1$ e $\beta_0 = 71$.

$$B_{13}(1,4,-1)_{(3,2)} = 13 + 4 \cdot 1 - 71 = -54.$$

Conclusão é que, como -54 não é divisível por 13, o número 13.241.798 também não é divisível por 13.

Exemplo 4:

Construiremos um critério de divisibilidade para os números 17 usando a expressão $B_p(k_2,k_1,k_0)_{(3,2)} = k_2 \cdot \beta_2 + k_1 \cdot \beta_1 + k_0 \cdot \beta_0$, e depois verificaremos a divisibilidade de 23.251.793 por 7 aplicando o critério obtido. Primeiro vamos construir o critério para o número 17, ou seja, teremos que calcular os coeficientes k_0, k_1 e k_2.

Assim,

$$\begin{cases} 10^{s_2-s_0} \cdot k_0 \equiv 1 \; mod(17) \\ 10^{s_2-s_1} \cdot k_1 \equiv 1 \; mod(17) \\ 10^{s_2-s_2} \cdot k_2 \equiv 1 \; mod(17) \end{cases}$$

$$\begin{cases} 10^{3} \cdot k_0 \equiv 1 \; mod(17) \\ 10^{1} \cdot k_1 \equiv 1 \; mod(17) \\ 10^{0} \cdot k_2 \equiv 1 \; mod(17) \end{cases}$$

$$\begin{cases} k_0 \equiv 3 \; mod(17) \\ k_1 \equiv 12 \; mod(17) \\ k_2 \equiv 1 \; mod(17) \end{cases}$$

Portanto, $B_{17}(1,12,3)_{(3,2)} = \beta_2 + 12 \cdot \beta_1 + 3 \cdot \beta_0$ ou $B_{17}(1,-5,3)_{(3,2)} = \beta_2 - 5 \cdot \beta_1 + 3 \cdot \beta_0$.

Resta agora aplicarmos o critério encontrado em 23.251.793, os elementos da partição serão: $\beta_2 = 23251$, $\beta_1 = 7$ e $\beta_0 = 93$. Na notação tomada, tem-se

$$B_{17}(1, -5, 3)_{(3,2)} = 23251 - 5 \cdot 7 + 3 \cdot 93 = 23495.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\beta_2 = 23$, $\beta_1 = 4$ e $\beta_0 = 95$.

$$B_{17}(1, -5, 3)_{(3,2)} = 23 - 5 \cdot 4 + 3 \cdot 95 = 288.$$

Replicando mais uma vez o método, os elementos da partição tomada, terá como elementos $\beta_2 = 0$, $\beta_1 = 2$ e $\beta_0 = 88$.

$$B_{17}(1, -5, 3)_{(3,2)} = 0 - 5 \cdot 2 + 3 \cdot 88 = 254.$$

Conclusão é que, como 254 não é divisível por 17, o número 23.251.793 também não é divisível por 17.

Exemplo 5:

Construiremos o critério de divisibilidade para os números 19 usando a expressão $B_p(k_2, k_1, k_0)_{(3,2)} = k_2 \cdot \beta_2 + k_1 \cdot \beta_1 + k_0 \cdot \beta_0$, e depois verificaremos a divisibilidade de 23.251.793 por 19 aplicando o critério obtido. Primeiro vamos construir o critério para o número 19, ou seja, teremos que calcular os coeficientes k_0, k_1 e k_2.

Assim,

$$\begin{cases} 10^{s_2 - s_0} \cdot k_0 \equiv 1 \; mod(19) \\ 10^{s_2 - s_1} \cdot k_1 \equiv 1 \; mod(19) \\ 10^{s_2 - s_2} \cdot k_2 \equiv 1 \; mod(19) \end{cases}$$

$$\begin{cases} 10^{3} \cdot k_0 \equiv 1 \; mod(19) \\ 10^{1} \cdot k_1 \equiv 1 \; mod(19) \\ 10^{0} \cdot k_2 \equiv 1 \; mod(19) \end{cases}$$

$$\begin{cases} k_0 \equiv 8 \; mod(17) \\ k_1 \equiv 2 \; mod(17) \\ k_2 \equiv 1 \; mod(17) \end{cases}$$

Portanto, $B_{19}(1,2,8)_{(3,2)} = \beta_2 + 2\cdot\beta_1 + 8\cdot\beta_0$ ou $B_{19}(1,-17,-11)_{(3,2)} = \beta_2 - 17\cdot\beta_1 - 11\cdot\beta_0$.

Resta agora aplicarmos o critério encontrado em 23.251.793. Os elementos da partição serão: $\beta_2 = 23251$, $\beta_1 = 7$ e $\beta_0 = 93$. Na notação tomada, tem-se

$$B_{19}(1,2,8)_{(3,2)} = \beta_2 + 2\cdot\beta_1 + 8\cdot\beta_0;$$

$$B_{19}(1,2,8)_{(3,2)} = 23251 + 2\cdot 7 + 8\cdot 93 = 24009.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\beta_2 = 24$, $\beta_1 = 0$ e $\beta_0 = 09$.

$$B_{19}(1,2,8)_{(3,2)} = 24 + 2\cdot 0 + 8\cdot 09 = 96.$$

Conclusão é que, como 96 não é divisível por 19, o número 23.251.793 também não é divisível por 19.

A seguir, enunciaremos e demonstraremos o Corolário 1 do Teorema 3.2 que nos permitirá gerar critérios de divisibilidade por p que dará o resto usando o método Beta.

3.4.2 Corolário 1 do Teorema 3.2: Resto na divisibilidade por p usando o método Beta.

No método Beta, N deixa resto R na divisão por p se, e somente se, $10^{s_m}\cdot\sum_{j=0}^{m} k_j\cdot\beta_j$ deixa resto R na divisão por p.

Demonstração:

Trivial, pois $N \equiv 10^{s_m}\cdot\sum_{j=0}^{m} k_j\cdot\beta_j \ mod(p)$.

$\blacksquare$

Agora, considere $w_j \equiv 10^{s_m}\cdot k_j \ mod(p)$ para $j = 0,1,\ldots,m$, logo teremos

$$N \equiv \sum_{j=0}^{m} w_j\cdot\beta_j \ mod(p).$$

Assim, teremos o método gerador de critérios que dá o resto na divisibilidade por p, no método tipo Beta que denotaremos por:

$$RB_p(w_m, \ldots, w_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} w_j \cdot \beta_j.$$

Exemplo 6:

O critério $B_7(1, -2)_{(1)} = \beta_1 - 2\beta_0$ é bem definido na literatura. Com ele só conseguimos afirmar se o número é ou não é divisível por 7. Porém, ele não nos dá condições de determinar o resto.

Com a aplicação do corolário 1 do Teorema 3.2 temos como encontrar o resto da divisão de um número natural por 7.

Vejamos como aplicar tal corolário.

Construiremos o critério do resto para a divisibilidade por 7 usando a expressão $RB_p(w_1, w_0)_{(1)} = w_1 \cdot \beta_1 + w_0 \cdot \beta_0$, e depois verificaremos a divisibilidade de 724 por 7 aplicando o critério obtido. Primeiro vamos construir o critério para o número 7, ou seja, teremos que calcular os coeficientes w_0, w_1.

Assim,

$$\begin{cases} w_0 \equiv 10^{s_1} \cdot k_0 \; mod(7) \\ w_1 \equiv 10^{s_1} \cdot k_1 \; mod(7) \end{cases}$$

$$\begin{cases} w_0 \equiv 10^1 \cdot (-2) \; mod(7) \\ w_1 \equiv 10^1 \cdot 1 \; mod(7) \end{cases}$$

$$\begin{cases} w_0 \equiv 1 \; mod(7) \\ w_1 \equiv 3 \; mod(7) \end{cases}$$

Portanto, $RB_7(3, 1)_{(1)} = 3 \cdot \beta_1 + \beta_0$.

Resta agora aplicarmos o critério encontrado em 724. Os elementos da partição serão: $\beta_1 = 72$ e $\beta_0 = 4$. Na notação tomada, tem-se

$$RB_7(3,1)_{(1)} = 3 \cdot \beta_1 + \beta_0;$$

$$RB_7(3,1)_{(1)} = 3 \cdot 72 + 4 = 220.$$

Replicando o método, os elementos da partição tomada, terá como elementos $\beta_1 = 22$ e $\beta_0 = 0$.

$$RB_7(3,1)_{(1)} = 3 \cdot 22 + 0 = 66.$$

Aplicando novamente o método, os elementos da partição tomada, terá como elementos $\beta_1 = 6$ e $\beta_0 = 6$.

$$RB_7(3,1)_{(1)} = 3 \cdot 6 + 6 = 24.$$

Replicando novamente o método, os elementos da partição tomada, terá como elementos $\beta_1 = 2$ e $\beta_0 = 4$.

$$RB_7(3,1)_{(1)} = 3 \cdot 2 + 4 = 10.$$

Aplicando novamente o método, os elementos da partição tomada, terá como elementos $\beta_1 = 1$ e $\beta_0 = 0$.

$$RB_7(3,1)_{(1)} = 3 \cdot 1 + 0 = 3.$$

Conclusão é que 3 é o resto da divisão de 724 por 7.

Nos corolários 2 a 4 do teorema 3.2, mostraremos alguns critérios de divisibilidade tradicional revisitados, que dão os mesmos resultados que os corolários 8 a 10 do teorema 3.1.

3.4.3 Corolário 2 do Teorema 3.2: Divisibilidade por 11.

No Teorema 3.2, considere $p = 11$. Então 11 divide N se, e somente se, 11 divide $\sum_{j=0}^{m}(-1)^{s_m - s_j} \cdot \beta_j$.

Demonstração:

Considere $p = 11$, logo $10 \equiv -1 \ mod(11)$, logo teremos:

$$10^{s_m - s_j} \cdot k_j \equiv 1 \ mod(p)$$

$$(-1)^{s_m - s_j} \cdot k_j \equiv 1 \ mod(11)$$

$$k_j \equiv (-1)^{s_m - s_j} \ mod(11).$$

Assim,

$$B_{11}((-1)^{s_m - s_m}, \ldots, (-1)^{s_m - s_0})_{(s_m, \ldots, s_1)} = \sum_{j=0}^{m} (-1)^{s_m - s_j} \cdot \beta_j.$$

Portanto, 11 divide N se, e somente se, 11 divide $\sum_{j=0}^{m} (-1)^{s_m - s_j} \cdot \beta_j$.

■

3.4.4 Corolário 3 do Teorema 3.2: Divisibilidade por p, com p pertencente ao conjunto D(10^n - 1).

No Teorema 3.2, considere $P = \{mn, \ldots, 3n, 2n, n\}$ e $p \in D(10^n - 1) = \{\boldsymbol{p} : \boldsymbol{p} | 10^n - 1, n \in \mathbb{N}^*, p > 1\}$. Então p divide N se, somente se, p divide $\sum_{j=0}^{m} \beta_j$.

Demonstração:

Considere $p \in D(10^n - 1)$, ou seja, $10^n \equiv 1 \ mod(p)$, logo teremos:

$$10^{(m-j) \cdot n} \cdot k_j \equiv 1 \ mod(p)$$

$$(10^n)^{m-j} \cdot k_j \equiv 1 \ mod(p)$$

$$1^{m-j} \cdot k_j \equiv 1 \ mod(p)$$

$$k_j \equiv 1^{m-j} \ mod(p).$$

Assim,

$$B_p(1^0, \ldots, 1^m)_{(mn, \ldots, 3n, 2n, n)} = \sum_{j=0}^{m} \beta_j.$$

Portanto concluímos que p divide N se, somente se, p divide $\sum_{j=0}^{m} \beta_j$.

■

3.4.5 Corolário 4 do Teorema 3.2: Divisibilidade por p, com p pertencente ao conjunto D(10^n + 1).

No Teorema 3.2, considere $P = \{mn, \ldots, 3n, 2n, n\}$ e $p \in D(10^n+1) = \{\boldsymbol{p} : \boldsymbol{p}|10^n+1, n \in \mathbb{N}^*, p > 1\}$. Então p divide N se, somente se, p divide $\sum_{j=0}^{m}(-1)^{m-j}\beta_j$.

Demonstração:

Considere $p \in D(10^n + 1)$ ou seja, $10^n \equiv -1\ mod(p)$, logo teremos:

$$10^{(s_m - s_j)} \cdot k_j \equiv 1\ mod(p)$$

$$10^{(m-j)\cdot n} \cdot k_j \equiv 1\ mod(p)$$

$$(10^n)^{m-j} \cdot k_j \equiv 1\ mod(p)$$

$$(-1)^{m-j} \cdot k_j \equiv 1\ mod(p)$$

$$k_j \equiv (-1)^{m-j}\ mod(p).$$

Assim,

$$B_p((-1)^0, \ldots, (-1)^m)_{(mn,\ldots,3n,2n,n)} = \sum_{j=0}^{m}(-1)^{m-j} \cdot \beta_j.$$

Portanto, concluímos que p divide N se, somente se, p divide $\sum_{j=0}^{m}(-1)^{m-j} \cdot \beta_j$.

■

3.5 Teorema que será utilizado nas demonstrações de alguns métodos construtores de critérios de divisibilidades do tipo Beta.

Nesta subseção enunciaremos e demonstraremos o Lema 3.1 que será utilizado nas demonstrações dos corolários de 7 e 8 do Teorema 3.2.

3.5.1 Lema 3.1:

Se a é inteiro maior que 1 tal que $b \equiv 1 \ mod \ (a)$, então $b^{a^{n-1}} \equiv 1 \ mod \ (a^n)$ com $n \geq 1$.

Demonstração:

Para provarmos, basta mostrar que a^n divide $1 - b^{a^{n-1}}$. Então vejamos esta prova por indução matemática:
(i) : Para $n = 1$, temos que a divide $1 - b$;
(ii) : Vamos supor que seja verdade para $n = k$, ou seja, a^k divide $1 - b^{a^{k-1}}$.

Logo temos que $b^{a^{k-1}} = 1 - a^k \cdot t$.

Agora vamos provar que é verdade para $n = k + 1$.

Assim,

$$1 - b^{a^{k+1-1}} = 1 - (b^{a^{k-1}})^a = 1 - (1 - a^k \cdot t)^a = 1 - \sum_{j=0}^{a} \binom{a}{j} \cdot a^{k \cdot j} \cdot t^j \cdot (-1)^j$$

$$-\sum_{j=1}^{a} \binom{a}{j} \cdot a^{k \cdot j} \cdot t^j \cdot (-1)^j.$$

Como cada termo do somatório é divisível por a^{k+1} concluímos por indução matemática que $b^{a^{n-1}} \equiv 1 \ mod \ (a^n)$.

■

A seguir, enunciaremos e demonstraremos o corolário 5 do Teorema 3.2 denominado Método Construtores de Critérios de Divisibilidade tipo Beta para $p = 10x + 1$.

3.5.2 Corolário 5 do Teorema 3.2: Método construtor de Critérios de divisibilidade do tipo Beta para números inteiros terminados em 1.

No Teorema 3.2, considere $p = 10x + 1$ e $k_j \equiv c_j \cdot x^{s_m - s_j} \ mod(10x + 1)$, $\forall \ x \in \mathbb{N}^*$. Então teremos uma expressão construtoras de critérios de divisibilidades dada por B_{10x+1}

$(k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$, com $c_j = (-1)^{s_m - s_j}$.

Demonstração:

Seja $k_j \equiv c_j \cdot x^{s_m - s_j}\ mod(10x+1)$, $\forall\ x \in \mathbb{N}^*$, queremos determinar c_j de modo que $10^{s_m - s_j} \cdot k_j \equiv 1\ mod\ (p)$ onde $j = 0, 1, 2, \ldots, m-1$, temos:

$$10^{sm - s_j} \cdot (c_j \cdot x^{s_m - sj}) \equiv 1\ mod\ (10x+1);$$

$$c_j \cdot 10^{sm - s_j} \cdot x^{s_m - sj} \equiv 1\ mod\ (10x+1);$$

$$c_j \cdot (10x)^{sm - s_j} \equiv 1\ mod\ (10x+1);$$

$$c_j \cdot [(10x)^{s_m - s_j} + (10x)^{s_m - s_j - 1} - (10x)^{s_m - s_j - 1} - (10x)^{s_m - s_j - 2} + (10x)^{s_m - s_j - 2} + \cdots$$
$$+(-1)^{s_m - s_j - 1}(10x)^0 + (-1)^{s_m - s_j}(10x)^0] \equiv 1\ mod\ (10x+1);$$

$$c_j \cdot \sum_{r=0}^{s_m - s_j - 1} (-1)^r (10x)^{s_m - s_j - 1 - r}[10x+1] + c_j \cdot (-1)^{s_m - s_j} \equiv 1\ mod\ (10x+1);$$

$$c_j \cdot (-1)^{s_m - s_j} \equiv 1\ mod\ (10x+1);$$

$$c_j \equiv (-1)^{s_m - s_j}\ mod\ (10x+1).$$

Portanto,
$B_{10x+1}\ (k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$, com $k_j \equiv (-x)^{s_m - s_j} mod(10x+1)$.

■

Exemplo 6:

Como exemplo, construiremos o critério de divisibilidade para o número 141, usando a expressão $B_{10x+1}\ (k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$ e verificando a seguir sua aplicação para o número 23.251.793.

Para $x = 14$, temos que $p = 10x + 1 = 10 \cdot 14 + 1 = 141$.

Logo,

$$k_j \equiv (-14)^{s_m - s_j} mod(141).$$

Para $P = \{6, 4, 2\}$ temos $s_3 = 6$, $s_2 = 4$ e $s_1 = 2$.

Assim,

$$\begin{cases} k_0 \equiv (-14)^{6-0}\ mod(141) \\ k_1 \equiv (-14)^{6-2}\ mod(141) \\ k_2 \equiv (-14)^{6-4}\ mod(141) \\ k_3 \equiv (-14)^{6-6}\ mod(141) \end{cases}$$

$$\begin{cases} k_0 \equiv 5\ mod(141) \\ k_1 \equiv 64\ mod(141) \\ k_2 \equiv 55\ mod(141) \\ k_3 \equiv 1\ mod(141) \end{cases}$$

Logo,

$$B_{141}\,(1, 55, 64, 5)_{(6,4,2)} = \beta_3 + 55 \cdot \beta_2 + 64 \cdot \beta_1 - 5 \cdot \beta_0.$$

Para $N = 23.251.793$ e aplicando a expressão acima temos que:

$\beta_0 = 93$, $\beta_1 = 17$, $\beta_2 = 25$ e $\beta_3 = 23$ e portanto ficamos com:

$$B_{141}\,(1, 55, 64, 5)_{(6,4,2)} = \beta_3 + 55 \cdot \beta_2 + 64 \cdot \beta_1 - 5 \cdot \beta_0;$$

$$B_{141}\,(1, 55, 64, 5)_{(6,4,2)} = 23 + 55 \cdot 25 + 64 \cdot 17 - 5 \cdot 93 = 2021.$$

Verificando que N não é divisível por 141!

Nota-se, como dissemos na introdução, a iteratividade do método e sua rapidez de definição, já com $B_{141}\,(1, 55, 64, 5)_{(6,4,2)}$, reduzimos a divisibilidade de $N = 23.251.793$ por 141 à divisibilidade de 2021 por 141!

A seguir, enunciaremos e demonstraremos o corolário 6 do Teorema 3.2 denominado Método Construtores de Critérios de Divisibilidade tipo Beta para $p = 10x - 1$, que permitirá construir critérios de divisibilidade para números inteiros maiores que 1 terminados em 9.

3.5.3 Corolário 6 do Teorema 3.2: Métodos construtores de Critérios de divisibilidade do tipo Beta para números inteiros terminados em 9.

No teorema 3.2, considere $p = 10x - 1$ e $k_j \equiv c_j \cdot x^{s_m - s_j}\ mod(10x - 1)$, $\forall\ x \in \mathbb{N}^*$. Então teremos uma expressão construtora de critérios de divisibilidades dada por B_{10x-1} $(k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$, , com $c_j = 1^{s_m - s_j}$.

Demonstração:

Considere $k_j \equiv c_j \cdot x^{s_m - s_j}$, $\forall\ x \in \mathbb{N}^*$, logo substituindo na equação $10^{s_m - s_j} \cdot k_j \equiv 1$ $mod\ (p)$ onde $j = 0, 1, 2, \ldots, m - 1$, temos:

$$10^{s_m - s_j} \cdot (c_j \cdot x^{s_m - sj}) \equiv 1\ mod\ (10x - 1);$$

$$c_j \cdot 10^{s_m - s_j} \cdot x^{s_m - sj} \equiv 1\ mod\ (10x - 1);$$

$$c_j \cdot (10x)^{s_m - s_j} \equiv 1\ mod\ (10x - 1);$$

$$c_j \cdot [(10x)^{s_m - s_j} - (10x)^{s_m - s_j - 1} + (10x)^{s_m - s_j - 1} - (10x)^{s_m - s_j - 2} + (10x)^{s_m - s_j - 2} + \cdots$$

$$-(10x)^0 + (10x)^0] \equiv 1 \; mod \; (10x-1);$$

$$c_j \cdot \sum_{r=0}^{s_m-s_j-1} (10x)^{s_m-s_j-1-r}[10x-1] + c_j \cdot 1^{s_m-s_j} \equiv 1 \; mod \; (10x-1);$$

$$c_j \cdot 1^{s_m-s_j} \equiv 1 \; mod \; (10x-1);$$

$$c_j \equiv 1^{s_m-s_j} \; mod \; (10x-1).$$

Portanto,
$B_{10x-1}\,(k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$, com $k_j \equiv x^{s_m-s_j} mod(10x-1)$.

■

Exemplo 7:

Como exemplo, construiremos o critério de divisibilidade para o número 129, usando a expressão $B_{10x-1}\,(k_m, \cdots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m} k_j \cdot \beta_j$ e verificando a seguir sua aplicação para o número 23.251.793.

Para $x = 13$, temos que $p = 10x - 1 = 10 \cdot 1311 = 129$.

Logo,

$$k_j \equiv 13^{s_m-s_j} mod(129)$$

Para $P = \{6, 4, 2\}$ temos $s_3 = 6$, $s_2 = 4$ e $s_1 = 2$.

Assim,

$$\begin{cases} k_0 \equiv (13)^{6-0} \; mod(129) \\ k_1 \equiv (13)^{6-2} \; mod(129) \\ k_2 \equiv (13)^{6-4} \; mod(129) \\ k_3 \equiv (13)^{6-6} \; mod(129) \end{cases}$$

$$\begin{cases} k_0 \equiv 16 \ mod(129) \\ k_1 \equiv 52 \ mod(129) \\ k_2 \equiv 40 \ mod(129) \\ k_3 \equiv 1 \ mod(129) \end{cases}$$

Logo,

$$B_{129}\,(1,40,52,16)_{(6,4,2)} = \beta_3 + 40 \cdot \beta_2 + 52 \cdot \beta_1 + 16 \cdot \beta_0.$$

Para $N = 23.251.793$ e aplicando a expressão acima temos que:

$\beta_0 = 93$, $\beta_1 = 17$, $\beta_2 = 25$ e $\beta_3 = 23$ e portanto ficamos com:

$$B_{129}\,(1,40,52,16)_{(6,4,2)} = \beta_3 + 40 \cdot \beta_2 + 52 \cdot \beta_1 + 16 \cdot \beta_0;$$

$$B_{129}\,(1,40,52,16)_{(6,4,2)} = 23 + 40 \cdot 25 + 52 \cdot 17 + 16 \cdot 93 = 3.395.$$

Verificando que N não é divisível por 129!

Nota-se, como dissemos na introdução, a iteratividade do método e sua rapidez de definição: com apenas dois passos, reduzimos a divisibilidade de $N = 23.251.793$ por 129 à divisibilidade de 3395 por 129!

A seguir, enunciaremos e demonstraremos o corolário 7 do Teorema 3.2 denominado Método Construtores de Critérios de Divisibilidade tipo Beta para $p = 10x + 3$, que permitirá construir critérios de divisibilidade para números inteiros maiores que 1 terminados em 3.

3.5.4 Corolário 7 do Teorema 3.2: Método construtores de Critérios de divisibilidade do tipo Beta para números inteiros terminados em 3.

No Teorema 3.2, considere $p = 10x + 3$ e $k_j \equiv c_j \cdot x^{s_m - s_j} + d_j \ mod(10x + 3)$, $\forall \ x \in \mathbb{N}$. Então teremos uma expressão construtora de critérios de divisibilidades dada por $B_{10x+3}\,(k_m, \ldots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m}[c_j \cdot x^{s_m - s_j} + d_j] \cdot \beta_j$, com $c_j = \frac{1 - 10{3^{s_m - s_j - 1}}}{3^{s_m - s_j}}$ e

$d_j = 10^{3^{s_m-s_j-1}-s_m-s_j}$.

Demonstração:

Seja $k_j \equiv c_j \cdot x^{s_m-s_j} + d_j \; mod(10x+3)$, $\forall \; x \in \mathbb{N}$, logo substituindo na equação $10^{s_m-s_j} \cdot k_j \equiv 1 \; mod \; (p)$ onde $j = 0, 1, 2, \ldots, m-1$, temos:

$$10^{s_m-s_j} \cdot (c_j \cdot x^{s_m-s_j} + d_j) \equiv 1 \; mod \; (10x+3);$$

$$c_j \cdot 10^{s_m-s_j} \cdot x^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1 \; mod \; (10x+3);$$

$$c_j \cdot (10x)^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1 \; mod \; (10x+3);$$

$$\begin{gathered} c_j \cdot [(10x)^{s_m-s_j} + 3^1(10x)^{s_m-s_j-1} - 3^1(10x)^{s_m-s_j-1} - 3^2(10x)^{s_m-s_j-2} \\ +3^2(10x)^{s_m-s_j-2} + \cdots + (-1)^{s_m-s_j-1}3^{s_m-s_j}(10x)^0 \\ +(-1)^{s_m-s_j}3^{s_m-s_j}(10x)^0] + 10^{s_m-s_j} \cdot d_j \equiv 1 \; mod \; (10x+3); \end{gathered}$$

$$c_j \cdot \sum_{r=0}^{s_m-s_j-1} (-3)^r(10x)^{s_m-s_j-1-r}[10x+3] + c_j \cdot (-3)^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1 \; mod \; (10x+3);$$

$$c_j \cdot (-3)^{s_m-s_j} + 10^{sm-s_j} \cdot d_j \equiv 1 \; mod \; (10x+3);$$

$$c_j \cdot (-3)^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j = 1.$$

Como $10 \equiv 1 \; mod \; (3)$ e considerando $d_j = 10^{3^{s_m-s_j-1}-s_m+s_j}$, logo pelo Lema 2.2 temos que: $c_j = \frac{1-10^{3^{s_m-s_j-1}}}{(-3)^{s_m-s_j}} \in \mathbb{Z}$, ou seja, a expressão $(c_j, \, dj)$ é uma solução da equação $c_j \cdot (-3)^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j = 1$.

Portanto,

$B_{10x+3}\,(1, k_{m-1}, \ldots, k_0)_{(s_m,\ldots,s_1)} = \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j$, com $k_j \equiv \frac{1-10^{3^{s_m-s_j-1}}}{(-3)^{s_m-s_j}} \cdot x^{s_m-s_j} + 10^{3^{s_m-s_j-1}-s_m+s_j}$ $mod(10x+3)$.

■

A seguir, enunciaremos e demonstraremos o corolário 8 do Teorema 3.2 denominado Método Construtores de Critérios de Divisibilidade tipo Beta para $p = 10x - 3$, que permitirá construir critérios de divisibilidade para números inteiros positivos terminados em 7.

3.5.5 Corolário 8 do Teorema 3.2: Método construtores de Critérios de divisibilidade do tipo Beta para números inteiros terminados em 7.

No Teorema 3.2, considere $p = 10x - 3$ e $k_j \equiv c_j \cdot x^{s_m-s_j} + d_j$ $mod(10x-3)$, $\forall\ x \in \mathbb{N}^*$. Então teremos uma expressão construtoras de critérios de divisibilidades dada por $B_{10x-3}\,(k_m, \ldots, k_0)_{(s_m,\ldots,s_1)} = \sum_{j=0}^{m}[c_j \cdot x^{s_m-s_j} + d_j] \cdot \beta_j$, com $c_j = \frac{1-10^{3^{s_m-s_j-1}}}{3^{s_m-s_j}}$ e $d_j = 10^{3^{s_m-s_j-1}-s_m-s_j}$.

Demonstração:

Seja $k_j \equiv c_j \cdot x^{s_m-s_j} + d_j$ $mod(10x-3)$, $\forall\ x \in \mathbb{N}^*$, logo substituindo na equação $10^{s_m-s_j} \cdot k_j \equiv 1$ $mod\ (p)$ onde $j = 0, 1, 2, \ldots, m-1$, temos:

$$10^{s_m-s_j} \cdot (c_j \cdot x^{s_m-s_j} + d_j) \equiv 1\ mod\ (10x-3);$$

$$c_j \cdot 10^{s_m-s_j} \cdot x^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1\ mod\ (10x-3);$$

$$c_j \cdot (10x)^{s_m-s_j} \cdot +10^{s_m-s_j} \cdot d_j \equiv 1\ mod\ (10x-3);$$

$$c_j \cdot [(10x)^{s_m-s_j} - 3^1(10x)^{s_m-s_j-1} - 3^2(10x)^{s_m-s_j-2} + 3^2(10x)^{s_m-s_j-2} - \cdots - 3^{s_m-s_j}$$

$$(10x)^0 + 3^{s_m-s_j}(10x)^0] + 10^{s_m-s_j} \cdot d_j \equiv 1 \ mod \ (10x-3);$$

$$c_j \cdot \sum_{r=0}^{s_m-s_j-1} 3^r(10x)^{s_m-s_j-1-r}[10x-3] + c_j \cdot 3^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1 \ mod \ (10x-3);$$

$$c_j \cdot 3^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j \equiv 1 \ mod \ (10x-3);$$

$$c_j \cdot 3^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j = 1.$$

Como $10 \equiv 1 \ mod \ (3)$ e considerando $d_j = 10^{3^{s_m-s_j-1}-s_m-s_j}$, logo pelo Lema 2.2 temos que: $c_j = \frac{1-10^{3^{s_m-s_j-1}}}{3^{s_m-s_j}} \in \mathbb{Z}$, ou seja, a expressão $(c_j,\, d_j)$ é uma solução da equação $c_j \cdot 3^{s_m-s_j} + 10^{s_m-s_j} \cdot d_j = 1$.

Portanto,
$B_{10x-3}(1, k_{m-1}, \ldots, k_0)_{(s_m,\ldots,s_1)} = \beta_m + \sum_{j=0}^{m-1} k_j \cdot \beta_j$, com $k_j \equiv \frac{1-10^{3^{s_m-s_j-1}}}{3^{s_m-s_j}} \cdot x^{s_m-s_j} + 10^{3^{s_m-s_j-1}-s_m+s_j} \ mod(10x-3)$.

■

Capítulo 4

CONCLUSÕES, CONTRIBUIÇÕES E TRABALHOS FUTUROS.

Este capítulo apresenta as conclusões da dissertação, bem como as principais contribuições. Ao final, alguns trabalhos futuros que podem dar prosseguimento a esta pesquisa.

4.1 Conclusões

De nossa parte, além do trabalho tomado, em uma tentativa de compilar uma coletânea de métodos que chamamos geradores de critérios de divisibilidades, os quais propiciam o suporte teórico para aqueles métodos que chamamos de construtores daqueles critérios, restou-nos a lacuna de descrever, através de exemplos, cada um dos métodos trabalhados. Isto contudo, apesar de feito, demandaria um aumento considerável do número de páginas da dissertação, caso considerássemos colocá-los. Outrossim, de importância para trabalhos futuros, gostaríamos de salientar: a determinação de algoritmos computacionais para implementação dos métodos tratados e o estudo de critérios que, comparativamente, delineiem a eficiência de um método em relação a outro.

Ressalta-se que o importante agora, é levar os resultados obtidos para que todos possam ter acesso as mesmas e possam contribuir para seu uso na educação básica e para o aprimoramento do professor.

Ainda como observações finais, podemos notar que a coletânea de métodos geradores de critérios de divisibilidade aqui desenvolvidos, representam uma abordagem generalizada para desenvolvimento de critérios, permitindo construir critérios de divisibilidade.

Podemos ainda observar que os métodos apresentados geram funções construtoras de critérios, e consequentemente, o mesmo para os resultados dessas funções, que são os critérios de divisibilidade propriamente ditos, que poderão ser aplicados em trabalhos futuros em diversas áreas. Acrescente-se que não esgotamos as possibilidades dos resultados obtidos, ficando como continuação, não só a ampliação da coletânea, bem como suas aplicações em algumas áreas de conhecimento.

4.2 Contribuições

A partir desta dissertação, notamos que há contribuições e apontamos as seguintes:

Para a primeira contribuição podemos apontar uma reunião de métodos geradores de critérios de divisibilidades que poderão ser utilizados pelos profissionais que atuam na educação básica.

Como segunda contribuição podemos apontar os métodos construtores de critérios de divisibilidade, bem como seus casos especiais.

Como terceira contribuição apontamos a notação que padroniza a maioria dos métodos aqui expostos. Como quarta contribuição podemos apontar o desenvolvimento de critérios de divisibilidade para os números inteiros maiores que 1 diferentes dos comumente usados.

Na sequência são apresentadas algumas alternativas de trabalhos futuros que podem ser realizados a partir desta pesquisa.

4.3 Trabalhos futuros

Como trabalho futuro, entendemos que é um trabalho que pode vir a sobrepor algumas limitações encontradas nos trabalhos existentes, ampliando e explicando os resultados.

Como sugestão, acreditamos que se pode desenvolver novos critérios de divisibilidades, utilizando os métodos geradores e construtores, conforme capítulo 3.

Outra sugestão é que podemos escrever os métodos e os critérios apresentados nesta dissertação da base 10 para uma base qualquer.

Espera-se ainda a criação de um software semiautomático para ajudar a gerar e construir critérios de divisibilidade, e ajudar os "matemáticos" a encontrar soluções de situações que podem não ter sido resolvidas até o presente momento. Este software conteria bibliotecas com os várias métodos geradores e construtores para resolver situações-problemas.

REFERÊNCIAS

ALENCAR FILHO, E. **Teoria elementar dos números.** São Paulo: Nobel, 1988.

BRASIL, Ministério da Educação e do Desporto. Secretaria de Educação Fundamental. Parâmetros Curriculares Nacionais: **Matemática.** Brasília, DF, 1998.

CARDOSO, M. L . GONÇALVES, O. A. **Uma interpretação geométrica do MMC.** Rio de Janeiro: RPM v. 32, p. 27 – 28, 1996.

CARVALHO, Fernando Ramires, BARBOSA, Gabriela dos Santos. COSTA, Roberta Marcele Vaz da. **Números primos e o teorema fundamental da aritmética no sexto ano do ensino fundamental.** 2015. 55f. Dissertação (Mestrado em Matemática Profissional). Instituto de Matemática Pura e Aplicada. Rio de Janeiro, RJ.

COELHO, S.; MACHADO, S. e MARANHÃO, C. **Como é utilizado o Teorema Fundamental da Aritmética por atores do Ensino Fundamental?** Atas do CIBEM V, Cd-rom, Cidade do Porto, 2005.

COSTA, Ronaldo Diniz. **Critério de divisibilidade no ensino básico.** 2014. 24f. Dissertação de Mestrado. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2014.

DANTE, Luíz Roberto. Restos, congruência e divisibilidade. in: **Revista do Professor de Matemática.** Nº 10, 1º semestres de 1987. pp. 33-40. HEFEZ, A. **Aritmética**. 2ª Ed. Rio de Janeiro: SBM, 2013. (Coleção PROFMAT).

HEFEZ, A. **Elementos de aritmética**. Rio de Janeiro, 2005.

EVES, H. **Introdução à história da matemática**. Campinas, SP: UNICAMP, 2008.

EVES, Howard. **Introdução à história da matemática**. – São Paulo: Editora da Unicamp, 2004.

FARIA, Alexandre Agusto Cavalcante de. **Teoria dos números: uma introdução motivadora direcionada aos docentes do ensino básico**. 2015. 178f. Dissertação de Mestrado. Universidade Federal de Alagoas, Maceió, 2015.

GUEDES, Mário Gustavo Pinto. Outros critérios de divisibilidade. in: **Revista do Professor de Matemática**. Nº 12, 1º semestre de 1988. pp. 24-27.

IGRAH, Georges. **História universal dos algarismos**. Vol. I. A Inteligência dos homens contada pelos números e pelos cálculos – Rio de Janeiro: Nova Fronteira, 1997.

LANDAU, Edmundo George Hermann. **Teoria elementar dos números**. Rio de Janeiro: Editora Ciência Moderna, 2002.

NETO, A. C. M. **Tópicos de Matemática Elementar**: Teoria dos Números. 1ª Ed. Rio de Janeiro: SBM, v. 5, 2012 (Coleção do Professor de Matemática; 28).

LIMA, Elon L - **Análise Real**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPq, 1998.

ROCHA, J. S. **Aprendizagem de matemática na educação a distância online: especificações de uma interface que facilite o tratamento algébrico para aprendizagem colaborativa entre pares**. 2012. 151 f. Dissertação de Mestrado. Universidade Federal de Pernambuco, Recife, 2012.

RODRIGUES, A. E. A. **Sistemas de numeração: evolução histórica, fundamento**

e sugestões para o ensino. 2013. 166 f. Dissertação (Mestrado em Matemática Profissional). Universidade Federal do Oeste do Pará (UFOPA). Santarém (PA)

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPq, 1998.

TÁBOAS, Carmen M. G., RIBEIRO, Hermano de Souza. Sobre critérios de divisibilidade. in: **Revista do Professor de Matemática**. N° 06, 1° semestres de 1985. pp. 21-24.

APÊNDICE

Alguns problemas propostos.

1) Prove que a soma dos dígitos de um número natural N, com réplica do processo da soma dos dígitos até obtermos apenas um dígito, é equivalente aos noves fora de N.

2) Prove os seguintes critérios de divisibilidades:

a) Um número natural N será divisível por 3 se, e somente se, os noves fora de N for 0, 3 ou 6.

b) Um número natural N será divisível por 9 se, e somente se, os noves fora de N for "0" (zero).

c) Um número natural N será divisível por 3 se, e somente se, os três fora de N for "0" (zero).

3) Construa os critérios de divisibilidade usando o método tipo Alfa para os números 6, 7, 11, 13, 14 e 18, com $P = \{3, 2\}$.

4) Construa os critérios de divisibilidade usando o método tipo Beta para os números 7, 11, 13, 17 e 19, com $P = \{3, 1\}$.

5) Construa os critérios de divisibilidade usando os métodos do tipo Alfa e do tipo Beta para os números 7, 11, 13, 17, 19, 21 e 23, com $P = \{3, 2, 1\}$.

6) Verifique a divisibilidade usando o método tipo Beta, de N=3.215.232 pelos números

7, 11, 13, 17 e 19, com o conjunto partição $P = \{2\}$.

7) No Teorema 3.1, considere o conjunto partição $P = \{s_1\}$ e $p = 10^{s_1}$. Então prove que $p = 10^{s_1}$ divide N se, e somente se, N for um número terminado em pelo menos s_1 zeros.

8) No Teorema 3.1, considere o conjunto partição $P = \{s_1\}$ e $p = 2^{s_1}$. Então prove que $p = 2^{s_1}$ divide N se, e somente se, os s_1 últimos dígitos de N, for um número divisível por $p = 2^{s_1}$.

9) No Teorema 3.1, considere o conjunto partição $P = \{s_1\}$ e $p = 5^{s_1}$. Então prove que 5^{s_1} divide N se, e somente se, os s_1 últimos dígitos de N, for um número divisível por 5^{s_1}.

10) Verifique se N = 3.472.458 é divisível por 17, usando os critérios dadas pelas expressões $A_{17}(-2, 1)_{(2)}$ e $A_{17}(-3, -2, 1)_{(3,2)}$, comparando as eficiências dos processos.

11) Verifique se N = 6.972.354 é divisível por 21, usando o critério dado pela expressão $B_{21}(1, 8, -6)_{(3,1)}$.

12) Use o método tipo Alfa para elaborar um critério de divisibilidade por 97.

13) Agora, use o metodo tipo Beta para elaborarum critério de divisibilidade por 97. Compare o resultado com aquele conseguido no problema 12.

14) Use o método tipo Alfa para obter critérios de divisibilidade para números menores que 100, com as seguintes conjuntos de partições:

a) $P = \{2\}$;

b) $P = \{3\}$;

c) $P = \{3, 2\}$.

15)Use o método tipo Beta para obter critérios de divisibilidade para números menores que 100, com os seguintes conjuntos de partições:

a) $P = \{2\}$;

b) $P = \{3\}$;

c) $P = \{3, 2\}$;

d) $P = \{1\}$.