UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE NOVA ANDRADINA
CURSO DE MATEMÁTICA, LICENCIATURA

WESLEI VENÍCIOS PEREIRA BARBOSA

Critérios de Divisibilidade

NOVA ANDRADINA
2020

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE NOVA ANDRADINA
CURSO DE MATEMÁTICA, LICENCIATURA

WESLEI VENÍCIOS PEREIRA BARBOSA

Trabalho de Conclusão de Curso - TCC apresentado na Universidade Estadual de Mato Grosso do Sul - UEMS como requisito básico para conclusão do curso de Matemática, Licenciatura.

Orientador: Prof. Me. Luiz Oreste Cauz

NOVA ANDRADINA

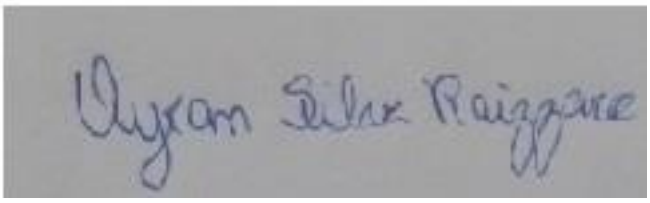
2020

Critérios de Divisibilidade

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Estadual de Mato Grosso do Sul, como requisito final para a obtenção do Título de Licenciado em Matemática sob a orientação do Prof. Me. Luiz Oreste Cauz.

Banca Examinadora

Prof. Me. Luiz Oreste Cauz Orientador
Universidade Estadual de Mato Grosso do Sul



Prof. Dr. Oyran Silva Rayzaro
Universidade Estadual de Mato Grosso do Sul

Prof. Dr. Sonner Arfux de Figueiredo
Universidade Estadual de Mato Grosso do Sul

Agradecimentos

Quero agradecer em primeiro lugar a Deus por estar sempre comigo em todos os momentos de minha vida, me abençoando e me protegendo em todas as decisões que eu tomo e me dando forças para continuar.

Quero agradecer a minha família que sempre esteve ao meu lado me apoiando em todos os momentos, me dando suporte sempre que precisei e pelos ensinamentos que me deram ao longo da minha vida.

Quero agradecer a todos os professores da UEMS, em especial o meu orientador Prof. Luiz Oreste Cauz, que ao longo do meus anos letivos, buscaram sempre transmitir um conhecimento amplo das disciplinas presentes nesse curso, sempre se preocupando e se dedicando ao máximo para que nós acadêmicos tivéssemos um ensino de qualidade.

Agradeço também aos meus amigos acadêmicos que me apoiaram e estiveram junto comigo ao longo dessa caminhada, onde compartilhamos conhecimentos e tivemos muitas experiências que levaremos para nossa vida inteira.

Quero deixar a seguinte frase como forma de inspiração: “Se você ainda respira então, você pode lutar, então lute pelos seus sonhos e viva intensamente.”

Resumo

O presente trabalho teve como objetivo fazer um estudo sobre os critérios de divisibilidade de números inteiros por números primos. Alguns dos critérios apresentados são frequentes nos livros de aritmética e, portanto, o chamaremos de Critérios Comuns. Outros critérios que foram apresentados se baseiam ou se assemelham à aplicação de um teorema conhecido como "Teorema de Sebá", os quais denominaremos de Critérios Incomuns. A importância do estudo deste tema pelo fato de que a divisibilidade permeia toda atividade humana e, além disso, é de grande importância na formação de um professor de Matemática. A metodologia empregada na pesquisa foi a clássica em pesquisas de Matemática, isto é, pesquisa bibliográfica em livros e artigos relacionados ao tema. Todo processo é demonstrado utilizando a divisibilidade para números inteiros, o máximo divisor comum, o algoritmo de Euclides e a aritmética dos restos. Por fim foi apresentado o resultado principal, o "Teorema de Sebá".
Palavras-chave: Números Inteiros. Algoritmo de Euclides. Aritmética dos Restos. Teorema de Sebá.

Abstract

The present work had as objective to make a study on the criteria of divisibility of integers numbers by prime numbers. Some of the basic criteria are considered in the arithmetic books and, therefore, we will call it Common Criteria. Other criteria that were necessary are based on or similar to the application of a theorem known as “Seba's theorem”, which we will call Unusual Criteria. The importance of studying this topic due to the fact that divisibility permeates all human activity and, in addition, is of great importance in the formation of a mathematics teacher. The methodology used in the research was the classic one in Mathematics research, that is, bibliographic research in books and articles related to the theme. The whole process is using divisibility for integers numbers, the greatest common divisor, Euclid's algorithm and an arithmetic of the remainders. Finally, the main result, the “Sebá's theorem”, was presented.
Keywords: Integers Numbers. Euclid's Algorithm. Arithmetic of the Remains. Seba's Theorem.

SUMÁRIO

Introdução

A aplicação da divisão vem desde o Período Paleolítico (3,5 milhões de anos a.C a 10000 a.C) onde os seres humanos se dividiam em bandos, e suas tarefas eram divididas da seguinte forma: os homens ficavam responsáveis pela caça, a pesca e a construção, as mulheres ficavam responsáveis pela coleta, pelo preparo do alimento e por cuidar das crianças. Podemos afirmar que isso representou a primeira divisão do Trabalho. Ao longo dos anos o homem foi aperfeiçoando suas habilidades até a chegada da Idade dos Metais (~4000 a.C) onde o homem precisava controlar as quantidades de mercadorias e os impostos, calcular preços, pesos e medidas. Como tinham essa necessidade, inventaram sinais e símbolos, que deram origem à escrita e à numeração. Só que nessa sociedade eram divididas as pessoas que teriam acesso à leitura e escrita, sendo elas só alguns funcionários do estado, o rei e os sacerdotes. Apenas os filhos desses tinham direito a aprender. A outra parte da população que era a maioria não tinha direito a esse conhecimento.

Segundo historiadores (BOYER, 1989) foi Tales de Mileto (624 – 558 a.C) o criador da geometria demonstrativa, ele introduziu o estudo matemático na Grécia. É estimado que ele tenha passado por terras egípcias e por diversos povoados e cidades do Oriente Médio, que foi o que proporcionou o contato com a matemática e a engenharia egípcia. Foi o que lhe proporcionou uma maior precisão para os estudos astronômicos e lhe permitiu formular o Teorema de Tales, que foi o cálculo que na época permitia descobrir a altura de uma pirâmide a partir do comprimento de retas paralelas e de retas transversais. A aplicação do Teorema de Tales diz que retas paralelas, cortadas por retas transversais formam segmentos correspondentes proporcionais. A diferença entre a matemática dos egípcios e dos gregos eram que, para os egípcios ela tratava-se de uma arte que os auxiliavam em seus trabalhos de engenharia e de agrimensura, enquanto que para os gregos, assumia um caráter científico, dada a atitude filosófica e especulativa que eles tinham face à vida.

Em seguida foram Pitágoras (580 – 497 a.C) e sua escola (que durou vários séculos) que se encarregaram de ulteriormente desenvolver e difundir a Matemática pela Grécia e suas colônias. Ele foi um matemático e filosofo grego. Autor do “Teorema de Pitágoras”, que em um triângulo retângulo, o quadrado da hipotenusa é igual à soma dos quadrados dos catetos. E foi ele o fundador da “Escola Pitagórica”, que era mais do que uma escola, era uma espécie de irmandade religiosa dedicada à matemática, em sua escola que se encarregaram de desenvolver e difundir a matemática pela Grécia e suas colônias. Além do famoso “Teorema de Pitágoras”,

os pitagóricos descobriram os números figurados e os números perfeitos, e eles adotaram a aritmética como fundamento de seu sistema filosófico. Sabe-se que quase nada sobrou dos escritos originais dessa fase da matemática grega, chegando a nós apenas referências e comentários feitos por outros matemáticos posteriores. Os gregos tinham uma forte inclinação para a filosofia e a lógica, tendo tudo isso influenciado fortemente toda a sua cultura, em particular o seu modo de fazer matemática.

Com toda a herança cultural, por volta do ano 300 a.C, em pleno florescimento da cultura helenística, quando Alexandria no Egito, era o centro do saber da época, surgiu Euclides de Alexandria, que foi um escritor grego e talvez o mais importante matemático da Grécia Antiga, sendo considerado o "pai da geometria". Os Elementos de Euclides, foi um tratado que se tornaria um dos marcos mais importantes da matemática. Se sabe pouco sobre os dados de sua bibliografia, tendo chegado a nós, através de várias edições, este tratado que é composto por 13 livros, onde podemos encontrar sistematizada a maior parte do conhecimento matemático da época. Aparentemente, Euclides não criou muitos resultados, mas tem o mérito de estabelecer um padrão de apresentação de rigor na matemática, que jamais foi alcançado anteriormente, ele é tido como um exemplo a ser seguido nos milênios que se sucederam. Ele elaborou 13 livros de Os Elementos, desses 13 livros, dez versões sobre a geometria e três sobre a aritmética, livros VII, VIII e IX, Euclides desenvolveu a teoria dos números naturais, sempre com uma visão geométrica. No seu livro VII, estão definidos os conceitos de divisibilidade, de números primos, de números perfeitos, de máximo divisor comum e de mínimo múltiplo comum, entre outros. Nesse mesmo livro, além das definições citadas, todas elas são bem postos e até hoje são utilizadas, encontra-se enunciada a divisão com resto de um número natural por outro, que é chamada de divisão Euclidiana. Através do uso repetitivo desta divisão, Euclides estabeleceu o algoritmo mais eficiente, até os dias atuais conhecido, para o cálculo do máximo divisor comum de dois inteiros chamado de Algoritmo de Euclides, que vamos apresentar nesse trabalho.

Este trabalho tem por objetivo fazer um estudo sobre critérios de divisibilidade de números inteiros por um número primo qualquer. Para isto, com base nas referências [2], [3] e [4] foram apresentados preliminarmente alguns conceitos clássicos da Teoria dos Números, como exemplo, Algoritmo da divisão de Euclides, Teorema Fundamental da Aritmética e Aritmética dos Restos. Todos estes conceitos foram importantes para podermos por fim apresentar o resultado principal dos estudos, o Teorema de Sebá, que fornece um critério

simples e robusto para verificar se um número inteiro é divisível por número primo maior do que cinco ([5] e [6]).

CAPÍTULO 1

Nesse capítulo serão apresentados vários resultados básicos relacionados a divisibilidade no conjunto dos inteiros. Mais detalhes sobre o assunto podem ser encontrados nas referências [2], [3] e [4].

1.1. Definição de divisibilidade

Dado dois números inteiros a e b com $a \neq 0$, diremos que a divide b, escrevendo $a \mid b$ quando existir $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso diremos que a é divisor de b, ou ainda, que b é um múltiplo de a.

Observe que a representação $a \mid b$ não retrata nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma resolução que diz ser verdade que b é múltiplo de a. E a negação dessa resolução é representada por $a \nmid b$.

Proposição 1.1.1: Sejam $a, b \in \mathbb{Z}$

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

(ii) $0 \mid a \Leftrightarrow a = 0$.

(iii) $a \mid b \Leftrightarrow |a| \mid |b|$

(iv) Se $a \mid b$ e $b \mid c \implies a \mid c$.

Demonstração:

(i) Isto é decorrente das igualdades $a = 1a, a = a \cdot 1$ e $0 = a \cdot 0$.

(ii) Suponhamos que $0 \mid a$, logo existe um $b \in \mathbb{Z}$ onde $a = 0b \implies a = 0$. Mutuamente, basta observar que $0 \mid 0$, que já foi provado anteriormente.

(iii) Suponhamos que $a \mid b$, logo $\exists\ c \in \mathbb{Z}$ tal que $b = ac \implies |b| = |ac| \implies |b| = |a| \cdot |c|$. Logo $|a| \mid |b|$. Mutuamente, temos que se $|a| \mid |b|$ existe $c \in \mathbb{Z}$ tal que $|b| = |a| \cdot c \implies |b| = |ac| \implies b = ac$, desta forma $a \mid b$.

(iv) Se $a \mid b$, logo $\exists\ q \in \mathbb{N}$ tal que $b = aq$, e se $b \mid c$ então $\exists$ p $\in \mathbb{Z}$ tal que $c = bp$. Assim, temos que $c = aqp \Longrightarrow c = at, com\ t = qp$. Portanto $a \mid c$.

No item (i) e (iii) temos qualquer número inteiro é divisível por ± 1 e por ele mesmo. Note também que $0 \mid 0$, portanto todo número natural também divide zero. Logo é notório que, o zero tem infinitos divisores. Suponha que $a \mid b$ e seja um $q \in \mathbb{Z}$ tal que $b = aq$, com $a\ e\ b \in \mathbb{Z}$ e $a \neq 0$. O número natural q é chamado de quociente de b por a e denotado por $q = b/a$. Observe que b/a só está definido quando $a \neq 0$ e $a \mid b$.

Proposição 1.1.2: Sejam $a, b, c\ e\ d \in \mathbb{Z}$, com $a \neq 0$ e c $\neq 0$. Então se $a \mid b$ e $c \mid d$ logo $ac \mid bd$.

Demonstração. De fato, se $a \mid b$ e $c \mid d$, então existem q e p $\in \mathbb{Z}$ tal que $b = aq$ e $d = cp$. Logo, temos então $bd = (aq)(cp) = ac \cdot qp = ac \cdot t$, com $t = qp$. Portanto, $ac \mid bd$.

Em particular, se $a \mid b$, então $ac \mid bc$, com todo $c \in \mathbb{Z}$. A demonstração nesse caso é análoga a proposição acima.

Proposição 1.1.3: Sejam $a, b\ e\ c \in \mathbb{Z}$, com $a \neq 0$, tais que $a \mid (b \pm c)$. Então $a \mid b$ se e somente se $a \mid c$.

Demonstração. Supondo que $a \mid (b \pm c)$. Logo $b \pm c = aq$, com $q \in \mathbb{Z}$ (I).

Assim, se $a \mid b$, logo $b = ap$, com $p \in \mathbb{Z}$ (II)

Substituindo (II) na (I) temos: $ap \pm c = aq$. Implica que $c = a(q \pm p)$, implica $c = at$, com q ± p = t. Portanto $a \mid c$. A prova de volta da implicação é equivalente.

Proposição 1.1.4: Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$, e $x, y \in \mathbb{Z}$, tais que $a \mid b$ e $a \mid c$, logo $a \mid (xb \pm yc)$.

Demonstração. Como $a \mid b$ e $a \mid c$ implicam que existem $p\ e\ q \in \mathbb{Z}$ tais que $b = ap\ e\ c = aq$. Logo, $xb \pm yc = x(ap) \pm y(aq) = a(xp \pm yq)$, o que prova o resultado.

Proposição 1.1.5: Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, $a \mid b \Longrightarrow |a| \leq |b|$.

Demonstração. De modo, se $a \mid b$, existe $q \in \mathbb{Z}$ tal que $b = aq$ com $q \neq 0$ pois $b \neq 0$. Aplicando módulo, temos que $|b| = |a| \cdot |q|$. Como $1 \leq |q| \Longrightarrow |a| \leq |a| \cdot |q|$ e como $|a| \cdot |q| = |b|$. Portanto temos que $|a| \leq |b|$.

Proposição 1.1.6: Sejam $a\ e\ b \in \mathbb{Z}$, então $a - b \mid a^n - b^n$, para todo $n \in \mathbb{N}$.

Demonstração. Para provar isso utilizaremos a indução sobre n. Como $a - b \mid 0$, logo para $n = 0$ a afirmação é verídica. Suponha então, que seja válido para n (hipótese de indução). Pelo fato de $a - b \mid a^n - b^n$ então $a^n - b^n = (a - b) \cdot q$, com $q \in \mathbb{Z}$. Assim $a^n - b^n = (a - b) \cdot q \Longrightarrow a^n = (a - b) \cdot q + b^n$.

Provaremos que vale para $n + 1$. Como $a^{n+1} - b^{n+1} = (a^n \cdot a) - b^{n+1}$. Logo substituindo o valor de a^n, temos que:

$$a^{n+1} - b^{n+1} = [(a - b) \cdot q + b^n] \cdot a - b^{n+1}$$
$$\Longrightarrow a^{n+1} - b^{n+1} = (a - b) \cdot aq + ab^n - b^{n+1}$$
$$\Longrightarrow a^{n+1} - b^{n+1} = (a - b) \cdot aq + (a - b) \cdot b^n$$
$$\Longrightarrow a^{n+1} - b^{n+1} = (a - b) \cdot (aq + b^n) = (a - b) \cdot t$$

Tomando $t = (aq + b^n)$. Logo temos que $a - b \mid a^{n+1} - a^{n+1}$. Portanto $a - b \mid a^n - b^n$ Para todo $n \in \mathbb{N}$.

Proposição 1.1.7: Sejam $a\ e\ b \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $a + b \neq 0$. Temos que $a + b \mid a^{2n+1} + b^{2n+1}$.

Demonstração. A prova é por indução em relação a n.

A afirmação é claramente verídica para n = 0, pois $a^{2n+1} + b^{2n+1} = a^{2 \cdot 0 + 1} + b^{2 \cdot 0 + 1} = a + b$ e logo $a + b \mid a + b$.

Consideremos, agora, que vale para n. Então $a^{2n+1} + b^{2n+1} = (a+b) \cdot q$ para $q \in \mathbb{Z}$. Logo

$$a^{2n+1} = (a+b) \cdot q - b^{2n+1} \text{ (I)}$$

Agora demonstraremos que é válido para $n+1$. Temos que

$$a^{2\cdot(n+1)+1} + b^{2\cdot(n+1)+1} = a^{2n+3} + b^{2n+3} = a^{2n+1} \cdot a^2 + b^{2n+3} \text{ (II)}$$

Substituindo (I) na (II) temos:

$$a^{2\cdot(n+1)+1} + b^{2\cdot(n+1)+1} = [(a+b) \cdot q - b^{2n+1}] \cdot a^2 + b^{2n+3} = (a+b) \cdot a^2 q -$$
$$a^2 b^{2n+1} + b^{2n+3} = (a+b) \cdot a^2 q - b^{2n+1} \cdot (a^2 - b^2).$$

Como $(a^2 - b^2) = (a+b) \cdot (a-b)$, segue que

$$a^{2\cdot(n+1)+1} + b^{2\cdot(n+1)+1} = (a+b) \cdot a^2 q - b^{2n+1} \cdot [(a+b) \cdot (a-b)].$$

Colocando $(a+b)$ em evidência, temos:

$$a^{2\cdot(n+1)+1} + b^{2\cdot(n+1)+1} = (a+b) \cdot [a^2 q - b^{2n+1} \cdot (a-b)].$$

Portanto, temos que $a+b \mid a^{2n+1} + b^{2n+1}$ para todo $n \in \mathbb{N}$.

Proposição 1.1.8: Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b \mid a^{2n} - b^{2n}$.

Demonstração: Repetidamente utilizaremos indução sobre n.

A afirmação é verídica para $n = 0$, pois $a^{2n} - b^{2n} = a^0 - b^0 = 1 - 1 = 0$ e temos que pelo item (i) da Proposição 1.1.1, que qualquer número divide zero. Supondo que vale para n, logo teremos $a^{2n} - b^{2n} = (a+b) \cdot q$ com $q \in \mathbb{Z}$, ou seja,

$$a^{2n} - b^{2n} = (a+b) \cdot q$$
$$a^{2n} = (a+b) \cdot q + b^{2n}$$

Iremos demonstrar que vale para $n+1$, isto é

$$a+b \mid a^{2n+2} - b^{2n+2}$$

Sabendo que $a^{2n+2} - b^{2n+2} = a^{2n} \cdot a^2 - b^{2n+2}$, substituindo os valores temos que

$$a^{2n+2} - b^{2n+2} = [(a+b) \cdot q + b^{2n}] \cdot a^2 - b^{2n+2} = (a+b) \cdot a^2 q + a^2 b^{2n} - b^{2n+2}$$
$$= (a+b) \cdot a^2 q + b^{2n} \cdot (a^2 - b^2)$$

Como $(a^2 - b^2) = (a+b) \cdot (a-b)$, então

$$a^{2n+2} - b^{2n+2} = (a+b) \cdot a^2 q + b^{2n} \cdot (a+b) \cdot (a-b) = (a+b) \cdot p + (a+b) \cdot t$$

com $p = a^2 q$ e $t = b^{2n} \cdot (a-b)$. Segue da Proposição 1.1.4, que $a + b \mid a^{2n+2} - b^{2n+2}$. Portanto $a + b \mid a^{2n} - b^{2n}$ para todo $n \in \mathbb{N}$.

Exemplo 2.1 Demonstre que $25 \mid 4^{70} + 3^{70}$.
Note que podemos escrever $25 = 16 + 9 = 4^2 + 3^2$. E conseguimos notar também $4^{70} + 3^{70} = (4^2)^{2.17+1} + (3^2)^{2.17+1}$, sendo assim, pela proposição 1.1.7, temos que $4^2 + 3^2 \mid (4^2)^{2.17+1} + (3^2)^{2.17+1}$. Portanto, $25 \mid 4^{70} + 3^{70}$.

Exemplo 2.2 Sabemos que $6 \mid 24$ e $6 \mid 30$, prove que $6 \mid 4854$
Podemos escrever $4854 = 101 \cdot 24 + 81 \cdot 30$ e pela proposição 1.1.4, como $6 \mid 24$ e $6 \mid 30$ temos que $6 \mid 4854$.

1.3. Divisão Euclidiana

Mesmo quando um número inteiro $a \neq 0$ não divide $b \in \mathbb{Z}$, Euclides mostra que é possível fazer a divisão de b por a, com resto. Esses resultados que mostraremos logo abaixo, não só é um importante instrumento na obra de Euclides, de maneira que também é o resultado central da teoria.

Teorema 1.3.1. (Divisão de Euclides). Dado a e $b \in \mathbb{Z}$ com $0 < a < b$, podem-se determinar q e r como dois números inteiros, tais que

$$\text{b} = \text{a} \cdot q + \text{r}, \text{com } 0 \leq r < \text{a}.$$

Demonstração: Suponha que $b > a$ e considere os números $b, b-a, b-2a, \cdots, b - n \cdot a$, de forma que o menor dos números dessa sequência seja maior ou igual que 0.

Utilizando a Propriedade da Boa Ordem, o conjunto S formado pelos dados acima tem um menor elemento $r = b - q \cdot a$. Vamos demonstrar que r < a.

Se $a \mid b$, logo $r = 0$ e nada mais temos a demonstrar. Se, por outro lado, $a \nmid b$, logo $r \neq 0$, e, logo, basta demonstrar que não pode acontecer $r > a$. De fato, se isto acontece-se, existiria um número inteiro $c < r$ tal que $r = c + a$. Logo como resultado $r = c + a = b - q \cdot a$, obteríamos

$$c = b - (q + 1) \cdot a \in S, \text{ com } c < r,$$

contraditória com o fato de r ser o menor elemento de S.

Consequentemente, temos que $b = a \cdot q + r$ com $r < a$, o mostra a existência de q e r.

Contudo, vamos demonstrar a unicidade. Veja que, dados dois componentes distintos de S, a diferença entre o maior e o menor desses componentes, existindo um múltiplo de a, é pelo menos a. Agora, se $r = b - a \cdot q$ e $r_1 = b - a \cdot q_1$, com $r < r_1 < a$, obteríamos $r_1 - r \geq a$, o que determinaria $r_1 \geq r + a \geq a$, absurdo. Por isso, $r = r_1$

Por causa disso segue que b – a · q = b – a · q_1, o que acarreta que $a \cdot q = a \cdot q_1$ e, logo $q = q_1$.

■

Nas circunstâncias do teorema acima, os números q e r são chamados, relativamente, de quociente e de resto da divisão de b por a.

Se o resto da divisão de b por a é zero, logo a divide b.

A demonstração do teorema proporciona um algoritmo (um procedimento executável) para calcular o quociente e o resto da divisão de um número por outro, por subtrações consecutivas.

Exemplo 1.3.1. Encontre o quociente e o resto 31 por 7.

Analise as diferenças consecutivas:

31 – 7 = 24, 31 – 2 · 7 = 17, 31 – 3 · 7 = 10, 31 – 4 · 7 = 3 < 7.

Isto nos resulta em q = 4 e r = 3.

Note que, não haveria necessidade de se mostrar a unicidade de q e r no Teorema 1.3.1, pois o resultado de cada passo do algoritmo é único e, portanto, r e q têm valores determinados. O caso é que exibimos um método para indicar q e r, atendendo as exigências do teorema, mas

não temos garantia que, usando outra forma, não teremos outros valores para q e r; de maneira que a necessidade de se provar a unicidade.

Exemplo 1.3.2. Demonstraremos que o resto da divisão de 10^n por 9 é sempre 1, para qualquer número natural n.

Faremos isso através de indução. Para n = 0, obtemos que $10^0 = 9 \cdot 0 + 1$; logo, o resultado é válido.

Supondo, agora o resultado apropriado para um certo n, isto é, $10^n = 9 \cdot q + 1$. Considere a semelhança

$10^{n+1} = 10 \cdot 10^n = (9 + 1)\ 10^n = 9 \cdot 10^n + 10^n = 9 \cdot 10^n + 9 \cdot q + 1 = 9\ (10^n + q) + 1$, afirmando que o resultado é válido para n + 1, logo vale para todo $n \in \mathbb{N}$.

Corolário. Sejam a e b dois números inteiros com $1 < a \leq b$, existe um número inteiro n tal que

$$na \leq b < (n + 1) \cdot a$$

Demonstração: Pela divisão euclidiana, temos que existem $q, r \in \mathbb{Z}$ com $r < a$, simplesmente determinados, tais que $b = a \cdot q + r$. Basta agora tomar $n = q$.

Exemplo 1.3.3. Seja um número natural $n \in \mathbb{Z}^*$ qualquer, existem duas possibilidades.

i) o resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{Z}$ tal que n = 2q; ou

ii) o resto da divisão de n por 2 é 1, ou seja, existe $q \in \mathbb{Z}$ tal que n = 2q + 1.

Logo notamos que, os números naturais se dividem em dois níveis, a dos números da forma 2q para um certo $q \in \mathbb{Z}$, chamados de números pares, e dos números da forma 2q + 1, chamados de números ímpares. Desde Pitágoras a 500 anos antes de cristo, os naturais são classificados em pares e ímpares.

Exemplo 1.3.4. Note, que fixando um número inteiro $m \geq 2$, consegue escrever um número qualquer n, de modo único, na determinada forma $n = mk + r$, onde $k, r \in \mathbb{Z}$ e $r < m$.

Tendo como exemplo, todo número inteiro n podendo ser escrito das seguintes formas: 3k, 3k + 1, ou 3k + 2.

Ou todo número inteiro n pode ser escrito das seguintes formas: 4k, 4k + 1, 4k + 2, 4k + 3.

Exemplo 1.3.5. Sejam $a, n \in \mathbb{Z}^*$, com $a > 2$ e ímpar, demonstraremos a paridade $\frac{(a^n-1)}{2}$.

Dado que a é ímpar, temos que $a^n - 1$ é par, logo $\frac{(a^n-1)}{2}$ é um número inteiro. Portanto, é coerente procurar definir sua paridade.

Sabemos que:

$$\frac{(a^n - 1)}{2} = \frac{(a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)}{2}$$

Sendo a ímpar, notamos que é $a^{n-1} + a^{n-2} + \cdots + a + 1$ ímpar ou par, logo $a^n - 1$ é par ou ímpar. Logo a análise limita à procurar a paridade de (a – 1) / 2.

Sendo a ímpar, podemos escrever a das seguintes formas $4k + 1$ ou $4k + 3$, com $k \in \mathbb{Z}^*$. Caso $a = 4k + 1$, então $\frac{(a^n-1)}{2}$ é par, na mesma proporção que, se $a = 4k + 3$, então $\frac{(a^n-1)}{2}$ é ímpar.

Sintetizando, temos que $(a^n - 1) / 2$ é par, apenas se n é par ou a está na forma 4k + 1.

1.4. Sistema de Numeração

No sistema decimal, todo número é representado por uma sequência formada pelos algarismos

1, 2, 3, 4, 5, 6, 7, 8, 9.

Acrescidos do símbolo 0 (zero), que representa a ausência de algarismo. Por serem dez algarismos é chamado de decimal.

O sistema também é chamado posicional, logo cada algarismo, além do seu valor intrínseco, tem um peso que lhe é concedido em função da posição que ele ocupa no número. Esse peso, sempre uma potência de dez, varia do seguinte modo:

O algarismo da extrema direita tem peso um, o seguinte da direita pra esquerda possui peso dez, o próximo possui peso cem, o próximo possui peso mil, e assim sucessivamente.

Portanto, os números de um a nove são representados pelos algarismos de 1 a 9, correspondentes. O número dez é representado por 10, o número cem por 100, o número mil por 1000.

Por exemplo, o número 15097, na base 10, é representado por

$1 \cdot 10^4 + 5 \cdot 10^3 + 0 \cdot 10^2 + 9 \cdot 10 + 7 = 1 \cdot 10^4 + 5 \cdot 10^3 + 9 \cdot 10 + 7.$

Cada algarismo de um número possui uma ordem contando da direita para a esquerda. Assim, no exemplo acima, o 1 é de quinta ordem, o 7 é de primeira ordem, o 9 é de segunda ordem, enquanto o 5 é de quarta ordem.

Cada terna de ordens, também contadas da direita pra esquerda, forma uma classe. As classes são, as vezes, separadas umas das outras por meio de um ponto.

Os sistemas de numeração posicionais baseiam-se no teorema que temos a seguir, que é uma aplicação da divisão euclidiana.

Teorema 1.4.1. Dados $a, b \in \mathbb{Z}$, com $b > 1$, existem números inteiros $m_0, m_1, \cdots, m_n$ menores do que b, univocamente determinados, tais que $a = m_0 + m_1 b + m_2 b^2 + \cdots + m_n b^n$.

Demonstração: Vamos demonstrar o teorema utilizando a segunda forma do Princípio de Indução Matemática sobre a. Se $a = 0$, ou se $a = 1$, basta tomar $n = 0$ e $m_0 = a$.

Supondo o resultado válido para todo inteiro menor do que a, vamos prova-lo para a. Pela divisão euclidiana, $\exists$ q e r únicos tais que

$$a = bq + r, com\, r < b.$$

Temos que $q < a$, logo pela hipótese de indução, procede que existem números inteiros n' e $d_0, d_1, \cdots, d_{n'}$ com $d_j < b$, para todo j, tais que

$$q = d_0 + d_1 b + \cdots + d_{n'} b^{n'}.$$

Considerando as igualdades acima destacadas, temos que

$$a = bq + r = b(d_0 + d_1 b + \cdots + d_{n'} b^{n'}) + r.$$

Por isso o resultado segue-se pondo $m_0 = r, n = n' + 1$ e $c_j = d_{j-1}$ para $j = 1, \cdots, n.$ e logo concluímos a demonstração.

Exemplo 1.4.1.1. Escreva os números a seguir na base dez:

a) 725.
b) 3547.
c) 791683.
d) Generalize para qualquer número.

Respostas das resoluções:

a) O número 725, na base 10 é escrito da forma $7 \cdot 10^2 + 2 \cdot 10 + 5$.
b) O número 3547, na base 10 é escrito da forma $3 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 7$.
c) O número 791683, na base 10 é escrito da forma $7 \cdot 10^5 + 9 \cdot 10^4 + 1 \cdot 10^3 + 6 \cdot 10^2 + 8 \cdot 10 + 3$.
d) Dado o número $t = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$, onde o a_i é o algarismo de número, na base 10, escrevemos t na seguinte forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

1.5. Máximo divisor comum

Definição 1.5.1. Sejam $a, b, d \in \mathbb{Z}$, com $d > 0$, logo dizemos que d é máximo divisor comum de a e b, e denotamos por $mdc\ (a.b) = d$ se tiver as seguintes propriedades:

i) d é um divisor comum de a e de b,

ii) d é divisível por todo divisor comum de a e b ou seja, se $c \mid a$ e $c \mid b$, então $c \mid d$.

Exemplo 1.5.1. Sejam a e $b \in \mathbb{Z}$, logo temos que:

i) $mdc\ (1, a) = 1$

ii) $mdc\ (0, a) = a$

iii) $mdc\ (a, a) = a$

iv) $mdc\ (1, b) = 1$

v) $mdc\ (0, b) = 0$

vi) $mdc\ (b, b)$ = b

vii) $mdc\ (a, b) = mdc\ (-a, b) = mdc\ (a, -b) = mdc(-a, -b)$

Teorema 1.5.1. Dado $a, b, g\ e\ r \in \mathbb{Z}$, onde $a = bg + r$, então temos que:

$$mdc(a, b) = mdc\ (b, r).$$

Demonstração: Seja $d = mdc\ (a, b)$. Logo pela Proposição 1.1.4 como $d \mid a\ e\ \ d \mid b$ e $g \in \mathbb{Z}$ logo temos que $d \mid a - bg = r$.

Agora supomos que $c \mid b\ e\ c \mid r = a - bg$, então pela Proposição 1.1.4, temos que $c \mid bg + a - bg = a$, logo $c \mid d$.

Lema 1.5.2. (Lema de Euclides). Sejam $a, b\ e\ n \in \mathbb{Z}$, portanto:

$$mdc\ (a, b) = mdc\ (a, b - na).$$

Demonstração:

Seja $b - na = d$. Logo $b = d + na$. Portanto pelo Teorema 1.5.1, como $a, b\ e\ n \in \mathbb{Z}$, $mdc\ (a, b) = mdc\ (a, d) = mdc\ (a, b - a)$.

Exemplo 1.5.2: Utilizando o Lema de Euclides, calcule o $mdc\ (819, 357)$.

Solução:

$$mdc(819, 357) = mdc\ (819 - 357, 357) = mdc\ (462, 357) =$$

$$= mdc\ (462 - 357, 357) = mdc\ (105, 357) = mdc\ (105, 357 - 2 \cdot 105) =$$

$$= mdc\ (105, 147) = mdc\ (105, 147 - 105) = mdc\ (105, 42) =$$

$$= mdc\,(105 - 2 \cdot 42, 42) = \ mdc\,(21, 42) = mdc\,(21, 42 - 2 \cdot 21) =$$

$$= mdc\,(21, 0) = 21.$$

Exemplo 1.5.3. Dado $n \in \mathbb{Z}$, mostre que:

a) $mdc\,(n,\ 5n + 3) = 3$

b) $mdc\,(n + 2, n^2 + 2n + 2) = 2$

c) $mdc(3n + 1, 10n + 3) = 1$

Solução:

a) Pelo Lema de Euclides temos que:

$$mdc\,(n, 5n + 3) =$$

$$= mdc(n, 5n + 3 - 5n) =$$

$$= mdc\,(n, 3) = 3.$$

b) Pelo Lema de Euclides temos que:

$$mdc\,(n + 2, n^2 + 2n + 2) =$$

$$= mdc\,(n + 2, n^2 + 2n + 2 - (n + 2)^2) =$$

$$= mdc\,(n + 2, n^2 + 2n + 2 - n^2 - 4n - 4) =$$

$$= mdc\,(n + 2, -2n - 2) =$$

$$= mdc\,(n + 3, -2n - 2 + 2 \cdot (n + 2)) =$$

$$= mdc\,(n + 3, -2n - 2 + 2n + 4) =$$

$$= mdc\,(n + 2, 2) = 2$$

c) Pelo Lema de Euclides temos que:

$$mdc(3n+1, 10n+3) =$$

$$= mdc\ (3n+1, 10n+3-3\cdot(3n+1)) =$$

$$= mdc\ (3n+1, 10n+3-9n+3) =$$

$$= mdc\ (3n+1, n) =$$

$$= mdc\ (3n+1-3n, n) =$$

$$= mdc\ (1, n) = 1.$$

1.5.1. Algoritmo de Euclides

O leitor conhece o método para determinar o mdc de dois números utilizando a decomposição deles através de números primos. Mas, todavia, se falarmos de números muito grandes, pode ser um pouco complicado encontrar essa decomposição. O método, chamado de Algoritmo de Euclides, é uma perfeita realização para o ponto de vista computacional e pouco conseguiu aperfeiçoar em mais de milênios, em relação a esse trabalho.

Teorema 1.5.4 (Algoritmo de Euclides) Dado $a, b\ e\ r_j \in \mathbb{Z}, j = \{1,2,3, \dots, n, n+1\}$. Efetuando o Algoritmo da Divisão Euclidiana continuamente de a por b, b por r_1, r_1 por r_2, r_2 por r_3, ..., r_{n-1} por r_n, até $r_{n+1} = 0$, logo abaixo temos $mdc\ (a, b) = r_n$.

$$a = bq_1 + r_1, 0 \leq r_1 < |b|$$

$$b = r_1 q_2 + r_2, 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3, 0 \leq r_3 < r_2$$

$$r_2 = r_3 q_4 + r_4, 0 \leq r_4 < r_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1},\ r_{n+1} = 0.$$

Demonstração:

Por $|b| > r_1 > r_2 > r_3 > r_4 > \cdots$, logo pelo Princípio da Boa Ordenação teremos um número finito de divisões e consequentemente algum $r_{n+1} = 0$.

Pelo Teorema 1.5.1. definimos que

$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = mdc(r_2,r_3) = \cdots = mdc(r_{n-1},r_n) = mdc(r_n,0) = r_n$.

Esse teorema também pode ser demonstrado da seguinte forma, inicialmente efetuando a divisão de $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1
b	a
r_1	

A seguir continuamos efetuando a divisão $a = r_1q_2 + r_2$ e colocamos os números no diagrama

	q_1	q_2
b	a	r_1
r_1	r_2	

Logo prosseguindo, enquanto for possível, teremos

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

Exemplo 1.5.4. Utilizando o Algoritmo de Euclides calcule mdc (960, 725).

Solução: Temos que

$$960 = 725 \cdot 1 + 235$$

$$725 = 235 \cdot 3 + 20$$

$$235 = 20 \cdot 11 + 15$$

$$20 = 15 \cdot 1 + 5$$

$$15 = 5 \cdot 3$$

Logo o $mdc(960{,}725) = 5$.

Exemplo 1.5.5. Calcule o $mdc\ de\ 23732\ e\ 180$ utilizando a segunda maneira apresentada.

	131	1	5	2	3
23732	180	152	28	12	4
152	28	12	4	0	

Observe, nesse exemplo que está acima, O Algoritmo de Euclides nos fornece:

$$4 = 28 - 2 \cdot 12$$

$$12 = 152 - 5 \cdot 28$$

$$28 = 180 - 1 \cdot 152$$

$$152 = 23732 - 131 \cdot 180$$

Portanto, segue que

$$4 = 28 - 2 \cdot 12 = 28 - 2 \cdot (152 - 5 \cdot 28) = 11 \cdot 28 - 2 \cdot 152 =$$

$$11 \cdot (180 - 1 \cdot 152) - 2 \cdot 152 = 11 \cdot 180 - 13 \cdot 152 =$$

$$11 \cdot 180 - 13 \cdot (23732 - 131 \cdot 180) = 1714 \cdot 180 - 13 \cdot 23732.$$

Portanto, temos que

$$mdc\ (23732, 180) = 4 = 1714 \cdot 180 - 13 \cdot 23732.$$

Observe que conseguimos, através do uso do Algoritmo de Euclides, de trás para frente, escrever $4 = mdc\ (23732, 180)$ como múltiplo de 180 menos um múltiplo de 23732.

O Algoritmo de Euclides nos providencia, um meio prático de escrever o mdc de dois números como diferença entre dois múltiplos dos números em questão, esse meio prático é a Identidade de Bezout.

Proposição 1.5.6. Dado $a, b\ e\ c \in \mathbb{Z}$. Se $a \mid bc\ e\ mdc\ (a, b) = 1$, então $a \mid c$.

Demonstração:

Como $a \mid bc$, logo temos que existe um $q \in Z$ tal que $bc = aq$. Pelo fato do $mdc(a, b) = 1$ temos que existem $x\ e\ y\ \in Z$ tal que $ax + by = 1$. Portanto:

$$ax + by = 1$$

$$\Rightarrow cax + cby = c$$

$$\Rightarrow cax + aqy = c$$

$$\Rightarrow a \cdot (cx + qy) = c$$

$$\Rightarrow a \mid c.$$

1.5.2. Números Primos

Um número inteiro $a \neq 0, \pm 1$ tem pelo menos quatro divisores: ± 1 e $\pm a$. Esses divisores são chamados de divisores triviais de a. Alguns números diferentes de 0 e ± 1 só tem os divisores triviais. Um número que tem somente divisores trivia é chamado de **número primo**. Por exemplo, o número 2 seus únicos divisores são ± 1 e ± 2. Um número inteiro diferente de 0 e ± 1 e que tem divisores não triviais é chamado número composto. O 6, por exemplo, cujos divisores são $\pm 1, \pm 2, \pm 3$ e ± 6.

Definição 1.5.7. Um número inteiro p é chamado de número primo se as seguintes condições se verificam:

(i) $p \neq 0$.

(ii) $p \neq \pm 1$.

(iii) Os números divisores de p são $\pm 1, \pm p$.

Corolário 1.5.1. Dado $a, b\ e\ p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, logo $p \mid a$ ou $p \mid b$.

Demonstração:

Se $p \mid a$ não tem o que demonstrar. Se $p \nmid a$, portanto temos que $mdc(a, p) = 1$. Pela Proposição 1.5.6, como $p \mid ab$ e $mdc(a, p) = 1$, logo p $\mid b$.

1.6. Teorema fundamental da Aritmética

Teorema 1.6.1. (Teorema Fundamental da Aritmética). Todo número inteiro maior que 1 é primo ou é escrito de modo único (a menos de ordem dos fatores) como um produto de números primos.

Demonstração:

Usaremos a demonstração por indução por n.

Como o número 2 é primo, logo temos que o teorema é verdadeiro para $n = 2$.

Supondo que o teorema seja valido para $2, 3, \cdots, n-1$, iremos provar que vale para n. Se n for primo não há o que demonstrar. Suponhamos então que n seja composto, portanto existem a e $b \in \mathbb{Z}$ tal que $n = ab$, com $1 < a < n$ e $1 < b < n$. Logo, por hipótese de indução, $a = p_1 p_2 \cdots p_r$ e $b = q_1 q_2 \cdots q_s$, com p_i e q_j primos. Portanto, $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$.

Agora vamos provar a unicidade da escrita. Suponhamos que $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, sendo p_i e q_j números primos, então $p_1 \mid q_1 q_2 \cdots q_s$ assim, $p_1 \mid q_1$ ou $p_1 \mid q_2$ ou $\cdots$ ou $p_1 \mid q_s$ (pelo Corolário 1.5.1) e, portanto, $p_1 = q_1$ ou $p_1 = q_2$ ou $\cdots$ ou $p_1 = q_s$.

Considerando que $p_1 = q_1$. Então $p_2 \cdots p_r = q_2 \cdots q_s < n$ e por hipótese de indução logo temos que $p_2 \cdots p_r = q_2 \cdots q_s$ podemos escrever de uma forma única como um produto de fatores primos, logo necessariamente $r = s$ e $p_i = q_j$ aos pares.

1.7. Aritmética dos Restos

Seja $n \in \mathbb{N}$. Diremos que dois números inteiros a e b são congruentes módulo de n se os restos da divisão euclidiana por n são iguais. Quando os inteiros a e b são congruentes módulo n, escrevemos

$$a \equiv b \ (mod\ n).$$

Quando a relação $a \equiv b \ (mod\ n)$ for falsa, diremos que a e b não são congruentes, ou são incongruentes, módulo n. Nesse caso escreveremos, $a \not\equiv b \ (mod\ n)$.

Pelo fato do resto da divisão de um número inteiro qualquer por 1 é sempre nulo, logo temos que $a \equiv b\ (mod\ 1)$, quaisquer que sejam $a, b \in \mathbb{Z}$. Isso torna desinteressante a aritmética dos restos módulo1. Portanto, daqui para frente, consideremos sempre $n > 1$.

Proposição 1.7.1. Dado $n \in \mathbb{N}$, com $n > 1$. Para todos $a, b, c \in \mathbb{Z}$, temos que:

I. $a \equiv a\ (mod\ n)$. (Reflexiva)
II. $se\ a \equiv b\ (mod\ n), então\ b \equiv a\ (mod\ n)$. (Simétrica)
III. $se\ a \equiv b\ (mod\ n)\ e\ b \equiv c\ (mod\ n), então\ a \equiv c\ (mod\ n)$. (Transitiva)

Nota-se que a demonstração é direta pela definição dos números congruentes.

Para verificar se dois números são congruentes módulo n, não é necessário efetuar a divisão euclidiana de ambos por n para depois comparar os restos. É suficiente aplicar o seguinte resultado:

Proposição 1.7.2 Suponha que $a, b \in \mathbb{Z}$ tais que $b \geq a$ e $n > 1$. Dizemos que $a \equiv b\ (mod\ n)$ se, e somente se, $n \mid b - a$.

Demonstração: Fazendo a divisão euclidiana de a e b por n, logo obtemos então que $a = nq + r$, com $r < n$ e $b = nq' + r'$, com $r' < n$. Logo, temos que:

$$b - a = \begin{cases} (q' - q)n + (r' - r), & se\ r' \geq r \\ (q' - q)n - (r - r'), & se\ r \geq r' \end{cases}$$

No qual $r' - r < n$, ou $r - r' < n$. Portanto, $a \equiv b\ mod\ n$ se, e somente se, $r = r'$, o que é equivalente a dizer que $n \mid b - a$.

Proposição 1.7.3. Dado $a, b, c, n \in \mathbb{Z}$, com $n > 1$.

I. Se $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n)$, então $a + c \equiv b + d\ (mod\ n)$.
II. Se $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n)$, então $ac \equiv bd\ (mod\ n)$.

Demonstração: Supondo que $a \equiv b\ mod\ n$ e $c \equiv d\ mod\ n$. Logo conseguimos, sem perda de generalidade, supor que $b \geq a$ e $d \geq c$. Temos então que $n \mid b - a$ e $n \mid d - c$.

I. Observando que $n \mid (b-a)+(d-c)$ e, portanto, $n \mid (b+d)-(a+c)$, e isso prova essa parte I da propriedade.

II. Nota-se que $bd-ac = d\cdot(b-a)+a\cdot(d-c)$ e concluímos que $n \mid bd-ac$.

Corolário 1.7 Para todos $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, se $a \equiv b\ (mod\ n)$, então $a^m \equiv b^m (mod\ n)$.

Demonstração: A demonstração se faz por indução sobre m, com base na Proposição 1.7.1.3.

Proposição 1.7.4 Sejam $a, b, c, n\ \in \mathbb{Z}$, com $n > 1$. Temos que:

$$a + c \equiv b + c\ (mod\ n)\ \Leftrightarrow a \equiv b\ (mod\ n)$$

Demonstração: Se $a \equiv b\ (mod\ n)$, ocorre imediatamente a Proposição 1.7.1.3 (I) que $a + c \equiv b + c\ (mod\ n)$, pois $c \equiv c\ (mod\ n)$.

Reciprocamente, suponha que $a + c \equiv b + c\ (mod\ n)$. Sem perda de princípios, podemos supor $b + c \geq a + c$. Portanto, $n \mid b + c - (a + c)$, que implica que $n \mid b - a$ e, consequentemente, $a \equiv b\ (mod\ n)$.

Proposição 1.7.5 Dados $a, b, c, n \in \mathbb{Z}$, com $n > 1$ e $c \neq 0$. Temos que

$$\text{ac} \equiv bc\ (\text{mod n})\ \Leftrightarrow a \equiv b\ \left(\text{mod}\frac{n}{mdc(c,n)}\right).$$

Demonstração: Supondo sem perder a generalidade, que $bc \geq ac$. De maneira que $\frac{n}{mdc(c,n)}$ e $\frac{c}{mdc(c,n)}$ são coprimos (significa que são primos entre si), logo temos que

$$\text{ac} \equiv bc\ (\text{mod n})\ \Leftrightarrow\ \text{n} \mid (b-a)\cdot c\ \Leftrightarrow\ \frac{n}{mdc(c,n)} \mid (b-a)\cdot\frac{c}{mdc(c,n)}$$

$$\Leftrightarrow\ \frac{n}{mdc(c,n)} \mid b-\text{a}\ \Leftrightarrow\ \text{a} \equiv b\ \left(\text{mod}\ \frac{n}{mdc(c,n)}\right).$$

Proposição 1.7.6 Sejam $a, b, n, m, n_1, \cdots, n_r \in \mathbb{Z}$, com $n, m, n_1, \cdots, n_r > 1$. Temos que:

i) Se $a \equiv b \; mod \; n$ e $m \mid n$, então $a \equiv b \; mod \; m$;

ii) Se $a \equiv b \; mod \; n$, então $mdc(a,n) = mdc(b,n)$.

Demonstração:

(i) Se $a \equiv b \; mod \; n$, então $n \mid b - a$. Como $m \mid n$, segue que $m \mid b - a$. Portanto, $a \equiv b \; mod \; n$.

(ii) Se $a \equiv b \; mod \; n$, então $n \mid b - a$, isto é, $b - a = n \cdot q \Rightarrow b = a + n \cdot q$, com $q \in \mathbb{Z}$. Portanto, temos que

$$\text{mdc}(a,n) = \text{mdc}(a + tn, n) = \text{mdc}(\text{b}, \text{n})$$

1.7.1 Exemplos

Exemplo 1.7.1 Ache o resto da divisão de 5^{21} por 127.

Demonstração:

Note que $5^3 = 125$ e que $5^3 + 2 \equiv 0 \; (mod \; 127)$. Então $5^3 + 2 \equiv 0 \; (mod \; 127) \Longrightarrow 5^3 + 2 - 2 \equiv 0 - 2 \; (mod \; 127) \Longrightarrow 5^3 \equiv -2 \; mod \; 127$. Pela Proposição 1.7.3, temos que $(5^3)^7 \equiv (-2)^7 \; (mod 127) \Longrightarrow 5^{21} \equiv -128 \; (mod \; 127)$ e na divisão euclidiana de -128 por 127, temos $-128 = 127 \cdot (-1) - 1$, isto é $-128 \equiv -1 \; (mod \; 127)$, portanto$5^{21} \equiv -1 \; (mod \; 127)$. Logo o resto é igual 126.

Exemplo 1.7.2 Para todo $m \in \mathbb{Z}$, mostre que $9^{6n} - 1$ é divisível por 7.

Demonstração: Temos que $9 \equiv 2 \; (mod \; 7)$ e pelo Corolário 1, logo temos que $9^6 \equiv 2^6 \; (mod \; 7)$. Como $2^6 = 64$, isso implica que $64 \equiv 1 \; (mod \; 7)$, então $9^6 \equiv 1 \; (mod \; 7)$, com base ainda no corolário 1.7, temos $(9^6)^n \equiv 1^n \; (\text{mod } 7) \Longrightarrow 9^{6n} \equiv 1 \; (\text{mod } 7)$, portanto $7 \mid 9^{6n} - 1$, para qualquer $n \in \mathbb{Z}$.

CAPÍTULO 2

Nesse capitulo serão apresentados as noções de congruências e as propriedades que utilizamos para a demonstração dos critérios de divisibilidade.

2.1. Critérios de Divisibilidade Comuns e Incomuns

Os critérios de divisibilidade surgiram da necessidade de saber se um certo número m é divisível por um número n sem de fato utilizar o algoritmo da divisão euclidiana. Os critérios são consequências da maneira de como representamos usualmente os números inteiros, com a utilização do sistema decimal.

2.1.1. Critério de divisibilidade por 2

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 2 se, e somente se o último algarismo terminar em 0, 2, 4, 6, 8. Lembrado que o número zero é divisível por todo número diferente dele mesmo.

Para demonstrar esse critério, basta observar que n é um número inteiro escrito na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então temos

$$10^0 \equiv 1 \ (mod\ 2)$$

$$10^1 \equiv 0 \ (mod\ 2)$$

$$10^2 \equiv 0 \ (mod\ 2)$$

$$10^3 \equiv 0 \ (mod\ 2)$$

$$10^4 \equiv 0 \ (mod\ 2)$$

$$\vdots$$

$$10^n \equiv 0 \ (mod\ 2)$$

Ou seja:

$$a_0 10^0 \equiv 1 \cdot a_0 \ (mod\ 2)$$

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

$$a_2 10^2 \equiv 0 \cdot a_2 \ (mod\ 2)$$

$$a_3 10^3 \equiv 0 \cdot a_3 \ (mod\ 2)$$

$$\vdots$$

$$a_r 10^r \equiv 0 \cdot a_r (mod\ 2)$$

Logo, pela Proposição 1.7.3 $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_r \cdot 10^r \equiv a_0\ (mod\ 2) \Longrightarrow a_r a_{r-1} \cdots a_3 a_2 a_1 a_0 \equiv a_0 (mod\ 2)$, ou seja, para que $a_r a_{r-1} \cdots a_3 a_2 a_1 a_0$ ser divisível por 2, tem-se que a_0 deve ser divisível por 2.

Portanto podemos concluir que $(a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 2 se, e somente se o algarismo da unidade for divisível por 2.

Exemplo: Dado um $n = 10574614$ é divisível por 2

Usando o critério de divisibilidade por 2 temos que n termina com um algarismo 4, portanto é divisível por 2, agora se $n = 10574613$ não seria divisível por 2, pois termina com o algarismo 3.

2.1.2 Critério de divisibilidade por 3.

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 3 se, e somente se a soma dos algarismos de n for divisível por 3.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, temos que:

$$10^0 \equiv 1\ (mod\ 3)$$

$$10^1 \equiv 1\ (mod\ 3)$$

$$10^2 \equiv 1\ (mod\ 3)$$

$$10^3 \equiv 1\ (mod\ 3)$$

$$10^4 \equiv 1\ (mod\ 3)$$

$$\vdots$$

$$10^r \equiv 1(mod 3)$$

Ou seja

$$a_0 10^0 \equiv 1 \cdot a_0\ (mod\ 3)$$

$$a_1 10^1 \equiv 1 \cdot a_1\ (mod\ 3)$$

$$a_2 10^2 \equiv 1 \cdot a_2\ (mod\ 3)$$

$$a_3 10^3 \equiv 1 \cdot a_3\ (mod\ 3)$$

$$\vdots$$

$$a_r 10^r \equiv 1 \cdot a_r\ (mod\ 3)$$

Logo, pela Proposição 1.7.3 $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_r\ (mod\ 3)$, isto é, $a_r a_{r-1} \cdots a_3 a_2 a_1 a_0 \equiv 0\ (mod\ 3) \Leftrightarrow a_0 + a_1 + a_2 + a_3 + \cdots + a_r \equiv 0\ (mod\ 3)$. Portanto, se a soma dos algarismos de um número é divisível por 3, então o número também é divisível por 3.

Portanto concluímos assim que $(a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 3 se, e somente se a soma dos algarismos que formam este número resultar em um número que é divisível por 3.

Exemplo: Verifique se $n = 154371$ é divisível por 3.

Aplicando o critério temos que $1 + 5 + 4 + 3 + 7 + 1 = 21$, assim temos que $3 \mid 21$, portanto concluímos que 154371 é divisível por 3.

2.1.3 Critério de divisibilidade por 5

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 5 se, e somente se o último algarismo terminar em 0 ou 5.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 10^1 + a_0 \cdot 10^0.$$

Então, temos que

$$10^0 \equiv 1 \ (mod\ 5)$$

$$10^1 \equiv 0 \ (mod\ 5)$$

$$10^2 \equiv 0 \ (mod\ 5)$$

$$10^3 \equiv 0 \ (mod\ 5)$$

$$10^4 \equiv 0 \ (mod\ 5)$$

$$\vdots$$

$$10^n \equiv 0 \ (mod\ 5)$$

Ou seja:

$$a_0 10^0 \equiv 1 \cdot a_0 \ (mod\ 5)$$

$$a_1 10^1 \equiv 0 \cdot a_1 \ (mod\ 5)$$

$$a_2 10^2 \equiv 0 \cdot a_2 \ (mod\ 5)$$

$$a_3 10^3 \equiv 0 \cdot a_3 \ (mod\ 5)$$

$$\vdots$$

$$a_r 10^r \equiv 0 \cdot a_r \ (mod\ 5)$$

Logo, $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_r \cdot 10^r \equiv a_0 \ (mod\ 5) \Longrightarrow$ $a_r a_{r-1} \cdots a_3 a_2 a_1 a_0 \equiv a_0 (mod\ 5)$, ou seja, para que $a_r a_{r-1} \cdots a_3 a_2 a_1 a_0$ ser divisível por 5, tem-se que $a_0 = 0$ ou $a_0 = 5$.

Portanto concluímos assim que $(a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 5 se, e somente se o último algarismo for 5 ou 0.

Exemplo: Verifique se $n = 9754620$ e $p = 75845$ são divisíveis por 5.

Pelo critério de divisibilidade temos que 9754620 é divisível por 5 pois termina em 0, e 75845 também é divisível por 5 pois termina em 5.

2.1.4 Critério de divisibilidade por 7

Observando que o critério de divisibilidade por 7, não é tão obvio como os por 2,3 e 5, tendo em vista que é mais viável fazer a divisão pelo fato do processo de divisão tornar-se bem mais rápido, más iremos explorar esse critério nesse trabalho.

Vale ressaltar que a maioria dos livros didáticos se quer enunciam esse critério devido sua complexidade de resolução, sendo mais prático simplesmente fazer a divisão.

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)$ é divisível por 7 se, e somente se, o número sem o ultimo algarismo subtraído pelo dobro do último algarismo, resultar em um número divisível por 7.

Demonstração: Por simplicidade, demonstraremos esse resultado sem a utilização da aritmética dos restos.

Supondo que

$$a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_2 \cdot 10^1 + a_1 - 2a_0 = 7\mathrm{q}$$

então,

$$a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 20a_0 = 7(10\mathrm{q})$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 20a_0 + 21a_0 = 7(10\mathrm{q}) + 21a_0$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 7(10\mathrm{q} + 3a_0)$$

$$\Leftrightarrow 7 | a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$\Longrightarrow 7 | (a_r a_{r-1} \cdots a_2 a_1 a_0).$$

■

Exemplo: Verifique se 9275 é divisível por 7.

$$\begin{array}{r} 927/\mathbf{5} \\ -\ 10 \\ \hline 91/\mathbf{7} \\ -14 \\ \hline 77 \end{array}$$

Como 77 é divisível por 7, logo temos que $9275 \equiv 0\ (mod\ 7)$.

2.1.5 Critério de divisibilidade por 11

Assim como o critério de divisibilidade por 7, o critério de divisibilidade por 11 não é tão explorado pelos professores do ensino básico, tendo em vista que é mais viável fazer a divisão pelo fato do processo de divisão tornar-se bem mais rápido, mas iremos explorar esse critério nesse trabalho.

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 11 se, e somente se a soma alternada dos algarismos de ordem par e dos algarismos de ordem impar for divisível por 11.

Se a diferença entre a soma das ordens for menor do que zero, soma-se ao minuendo o menor múltiplo de 11, até que a diferença se torne positiva.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, temos que

$$10^0 \equiv 1\ (mod\ 11)$$

$$10^1 \equiv 10\ (mod\ 11)\ ou\ 10^1 \equiv -1\ (mod\ 11)$$

$$10^2 \equiv 1\ (mod\ 11)\ ou\ 10^2 \equiv -10\ (mod\ 11)$$

$$10^3 \equiv 10\ (mod\ 11)\ ou\ 10^3 \equiv -1\ (mod\ 11)$$

$$10^4 \equiv 1\ (mod\ 11)\ ou\ 10^4 \equiv -10\ (mod\ 11)$$

$$10^5 \equiv 10\ (mod\ 11)\ ou\ 10^5 \equiv -1\ (mod\ 11)$$

$$10^6 \equiv 1\ (mod\ 11)\ ou\ 10^6 \equiv -10\ (mod\ 11)$$

$$\vdots$$

.

Ou seja

$$a_0 10^0 \equiv 1a_0\ (mod\ 11)$$

$$a_1 10^1 \equiv 10 \cdot a_1\ (mod\ 11)\ ou\ a_1 10^1 \equiv -1 \cdot a_1\ (mod\ 11)$$

$$a_2 10^2 \equiv 1 \cdot a_2\ (mod\ 11)\ ou\ a_2 10^2 \equiv -10 \cdot a_2\ (mod\ 11)$$

$$a_3 10^3 \equiv 10 \cdot a_3\ (mod\ 11)\ ou\ a_3 10^3 \equiv -1 \cdot a_3\ (mod\ 11)$$

$$a_4 10^4 \equiv 1 \cdot a_4\ (mod\ 11)\ ou\ a_4 10^4 \equiv -10 \cdot a_4\ (mod\ 11)$$

$$a_5 10^5 \equiv 10 \cdot a_5\ (mod\ 11)\ ou\ a_5 10^5 \equiv -1 \cdot a_5\ (mod\ 11)$$

$$a_6 10^6 \equiv 1 \cdot a_6\ (mod\ 11)\ ou\ a_6 10^6 \equiv -10 \cdot a_6\ (mod\ 11)$$

$$\vdots$$

Portanto, concluímos que $(a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)$ é divisível por 11 se, e somente se

$$n = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \equiv (-1)^r a_r + \cdots - a_3 + a_2 - a_1 + a_0\ mod\ 11,$$

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

Exemplo: Verifique se 4780248 é divisível por 11.

$$Soi = 8 + 2 + 8 + 4 = 22$$

$$Sop = 4 + 0 + 7 = 11$$

$$22 - 11 = 11 > 0$$

$$11 \equiv 0\ (mod\ 11).$$

Portanto o número 4780248 é divisível por 11.

Os critérios de divisibilidade que serão apresentados logo abaixo não são abordados no ensino básico.

2.1.6 Critério de divisibilidade por 13

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 13 se e somente se o número sem o ultimo algarismo é somado à quatro vezes o ultimo algarismo e o resultado nos der um número divisível por 13.

Observação se o número obtido nesse processo for demasiadamente grande, logo o processo deve ser repetido o quanto for necessário.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, suponha que

$$a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_2 \cdot 10^1 + a_1 + 4a_0 = 13\text{q}$$

então,

$$a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 40a_0 = 13(10\text{q})$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 40a_0 - 39a_0 = 13(10\text{q}) - 39a_0$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 13(10\text{q} - 3a_0)$$

$$\Leftrightarrow 13 | a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$\Leftrightarrow 13 | (a_r a_{r-1} \cdots a_2 a_1 a_0).$$

Exemplo: Verifique se 11375 é divisível por 13.

Temos que $5 \cdot 4 = 20 \Longrightarrow 1137 + 20 = 1157 \Longrightarrow 7 \cdot 4 = 28 \Longrightarrow 115 + 28 = 143 \Longrightarrow 3 \cdot 4 = 12 \Longrightarrow 14 + 12 = 26$

Portanto concluímos que 26 é divisível por 13, logo 11375 também é divisível por 13.

2.1.7 Critério de divisibilidade por 17

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 17 se, e somente se a multiplicarmos do último algarismo por 5, subtraindo os números restantes (sem o último número) pelo produto anterior obtivemos um número divisível por 17.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, suponha que

$$a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_2 \cdot 10^1 + a_1 - 5a_0 = 17\text{q}$$

então,

$$a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 50a_0 = 17(10\text{q})$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 - 50a_0 + 51a_0 = 17(10\text{q}) + 51a_0$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 17(10\text{q} + 3a_0)$$

$$\Leftrightarrow 17 | a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$\Leftrightarrow 17 | (a_r a_{r-1} \cdots a_2 a_1 a_0).$$

Exemplo: Verifique se 9384 é divisível por 17.

Temos que $4 \cdot 5 = 20 \Longrightarrow 938 - 20 = 918 \Longrightarrow 8 \cdot 5 = 40 \Longrightarrow 91 - 40 = 51 \Longrightarrow 1 \cdot 5 = 5 \Longrightarrow 5 - 5 = 0.$

Como zero é divisível por 17, portanto temos que 9384 é divisível por 17.

2.1.8 Critério de divisibilidade por 19.

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 19 se, e somente se o dobro do último algarismo somado aos números restantes (sem o último algarismo) for um número divisível por 19.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, suponha que

$$a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_2 \cdot 10^1 + a_1 + 2a_0 = 19\text{q}$$

então,

$$a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 20a_0 = 19(10\text{q})$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 20a_0 - 19a_0 = 19(10\text{q}) - 19a_0$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 19(10\text{q} - a_0)$$

$$\Leftrightarrow 19 | a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$\Leftrightarrow 19 | (a_r a_{r-1} \cdots a_2 a_1 a_0)$$

Exemplo: Verifique se 92815 é divisível por 19.

Temos que $2 \cdot 5 = 10 \Longrightarrow 9281 + 10 = 9291 \Longrightarrow 2 \cdot 1 = 2 \Longrightarrow 929 + 2 = 931 \Longrightarrow 2 \cdot 1 = 2 \Longrightarrow 93 + 2 = 95 \Longrightarrow 2 \cdot 5 = 10 \Longrightarrow 9 + 10 = 19$.

Como 19 é divisível por 19, portanto temos que 92815 é divisível por 19.

2.1.9 Critério de divisibilidade por 23.

Um número inteiro $n = (a_r a_{r-1} \cdots a_3 a_2 a_1 a_0)_{10}$ é divisível por 23 se, e somente se quando multiplicarmos o último algarismo desse número por 7, somando ao número restante (sem o último algarismo), obtemos um número divisível por 23.

Para demonstrar esse critério, basta observar que n é um número inteiro na base decimal da forma:

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Então, suponha que

$$a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_2 \cdot 10^1 + a_1 + 7a_0 = 23\text{q}$$

então,

$$a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 70a_0 = 23(10\text{q})$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + 70a_0 - 69a_0 = 23(10\text{q}) - 69a_0$$

$$\Leftrightarrow a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 23(10\text{q} - 3a_0)$$

$$\Leftrightarrow 23 | a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$\Leftrightarrow 23 | (a_r a_{r-1} \cdots a_2 a_1 a_0).$$

Exemplo: Verifique se 1288 é divisível por 23.

Temos que $8 \cdot 7 = 56 \Longrightarrow 128 + 56 = 184 \Longrightarrow 4 \cdot 7 = 28 \Longrightarrow 18 + 28 = 46.$

Como 46 é divisível por 23, portanto temos que 1288 também é divisível por 23.

2.2. Critério de Divisibilidade Geral

Antes de demonstramos o Teorema de Sebá, seguem alguns esclarecimentos sobre os números primos maiores que cinco.

Seja p o divisor primo em estudo, $p > 5$. Logo o último algarismo de p só poderá ser 1, 3, 7 ou 9. Portanto 1,7, 3 e 9 são respectivamente, os menores números naturais que multiplicados por p fornecem números terminados em 1. Subtraindo 1 de tais produtos, temos necessariamente um múltiplo de 10. Dividindo por 10 esse último resultado, obtém-se o valor de y. Conforme está expresso na tabela abaixo.

Primo terminado em	Fator	Expressão para y
1	1	$y = (p-1)/10$
3	7	$y = (7p-1)/10$
7	3	$y = (3p-1)/10$
9	9	$y = (9p-1)/10$

Para obter uma melhor compreensão do Teorema de Sebá, observe um conhecimento do critério de divisibilidade por 7.

Um número é divisível por 7 se, eliminado seu último algarismo, o número restante subtraído do dobro do algarismo eliminado for divisível por 7.

Exemplo: Verifique se 7063 é divisível por 7 a partir do critério acima.

- Eliminar seu último algarismo: 706~~3~~.
- Número restante:706.
- Subtrair de 706 do dobro do algarismo eliminado: $706 - 2 \cdot 3 = 700$.

Como ainda é um número muito grande a gente repete o processo novamente.

- Eliminar seu último algarismo: 70~~0~~.
- Número restante: 70
- Subtrair de 70 do dobro do algarismo eliminado: $70 - 2 \cdot 0 = 70$.

Como 70 é divisível por 7, conclui-se que 7063 é divisível por 7.

Ao aplicar esse critério de divisibilidade por 7 aos alunos, naturalmente vai surgir a seguinte pergunta: “Por que devemos subtrair o dobro do último algarismo eliminado?”

Com base na tabela acima. Observe que 7 é um número primo maior que 5. Portanto consultando a tabela, tem-se: $y = (3p-1)/10 = (3 \cdot 7 - 1)/10 = 2$, respondendo assim à pergunta.

Teorema 2.2.1. (Teorema de Sebá)*:* Seja n um número inteiro dado. Os passos a seguir constituem um critério para verificar se n é divisível por um número primo $\mathrm{p}, \mathrm{p} > 5$.

1° Passo. Se p terminar em 1, 3, 7 ou 9, multiplique p respectivamente, por 1, 7, 3 e 9 subtraia de 1 e dívida a diferença por 10. Tais coeficientes serão designados por y.

2° Passo. Multiplique y pelo último algarismo de n e subtraia de n sem o último algarismo. Se a diferença for grande, de tal maneira que não seja possível reconhecer facilmente se ele é divisível por p, repete-se o processo até que seja possível reconhecer facilmente a divisão por p.

A demonstração do Teorema de Sebá será dividida em quatro etapas.

- p terminar em 1

1° Passo. Subtraia p de 1 e dívida a diferença por 10. Tal quociente será chamado de y.

2° Passo. Multiplique y pelo último algarismo de n e subtraia de n sem o último algarismo. Se a diferença for grande de tal maneira que não seja possível reconhecer facilmente se ela é divisível por p, repete-se o processo até que seja possível reconhecer facilmente a divisão por p.

Proposição 2.2.1. Considere o número inteiro $n = a_k a_{k-1} \cdots a_0$, com $a_k \neq 0$, e seja p um número inteiro primo que termina em 1, se $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, então $p \mid n$, em que $y = [(p-1)/10]$.

Demonstração: Como $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, isto é:

$$p \mid \left[a_k a_{k-1} \cdots a_1 - \left(\frac{p-1}{10}\right) \cdot a_0\right]$$

Então

$$p \mid [a_k a_{k-1} \cdots a_1 0 - p \cdot a_0 + a_0],$$

isto é,

$$p \mid [a_k a_{k-1} \cdots a_1 a_0 - p \cdot a_0],$$

portanto

$$p \mid (n - p \cdot a_0).$$

Logo

$$p \mid n.$$

- p termina em 3

1° Passo. Se p termina em 3, multiplique p por 7, subtraia 1 e dívida a diferença por 10. Tal quociente será chamado de y.

2º Passo. Multiplique y pelo último algarismo de n e subtraia de n sem o último algarismo. Se a diferença for grande, de tal maneira que não seja possível reconhecer facilmente se ela é divisível por p, repita o processo até que seja possível reconhecer facilmente a divisão por p.

Proposição 2.2.2. Considere o número inteiro n $= a_k a_{k-1} \cdots a_0$, com $a_k \neq 0$ e seja p um número primo que termina em 3. Se $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, então $p \mid n$, em que $y = [(7p-1)/10]$.

Demonstração: Como $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, isto é,

$$p \mid \left[a_k a_{k-1} \cdots a_1 - \left(\frac{7p-1}{10}\right) \cdot a_0\right]$$

Então

$$p \mid [a_k a_{k-1} \cdots a_1 0 - 7p \cdot a_0 + a_0],$$

isto é,

$$p \mid [a_k a_{k-1} \cdots a_0 - 7p \cdot a_0],$$

portanto

$$\mathrm{p} \mid (n - 7p \cdot a_0).$$

Logo

$$p \mid n.$$

- p terminado em 7

1° Passo. Se p termina em 7, multiplique p por 3, subtraia de 1 e dívida a diferença por 10. Tal quociente será chamado de y.

2° Passo. Multiplique y pelo último algarismo de n e subtraia de n sem o último algarismo. Se a diferença for grande, de tal maneira que não seja possível reconhecer facilmente se ela é divisível por p, repita o processo até que seja possível reconhecer facilmente a divisão por p.

Proposição 2.2.3. Considere o número inteiro n $= a_k a_{k-1} \cdots a_0$, com $a_k \neq 0$ e seja p um número primo que termina em 7. Se $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, então $p \mid n$, em que $y = [(3p-1)/10]$.

Demonstração: Como $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, isto é,

$$p \mid \left[a_k a_{k-1} \cdots a_1 - \left(\frac{3p-1}{10}\right) \cdot a_0\right],$$

Então

$$p \mid [a_k a_{k-1} \cdots a_1 0 - 3p \cdot a_0 + a_0],$$

isto é,

$$p \mid [a_k a_{k-1} \cdots a_0 - 3p \cdot a_0],$$

portanto

$$\mathrm{p} \mid (n - 3p \cdot a_0).$$

Logo

$$p \mid n.$$

- p terminado em 9.

1° Passo. Se p terminar em 9, multiplique p por 9, subtraia de 1 e dívida a diferença por 10. Tal quociente será chamado de y.

2° Passo. Multiplique y pelo último algarismo de n e subtraia de n sem o último algarismo. Se a diferença for grande, de tal forma que não seja possível reconhecer facilmente se ela é divisível por p, repete o processo até que seja facilmente reconhecer facilmente a divisão por p.

Proposição 2.3.4. Considere o número inteiro n $= a_k a_{k-1} \cdots a_0$, com $a_k \neq 0$ e seja p um número primo terminado em 9. Se $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, então $p \mid n$, em que $y = [(9p-1)/10]$.

Demonstração: Como $p \mid (a_k a_{k-1} \cdots a_1 - y \cdot a_0)$, isto é,

$$p \mid \left[a_k a_{k-1} \cdots a_1 - \left(\frac{9p-1}{10}\right) \cdot a_0\right],$$

Então

$$p \mid [a_k a_{k-1} \cdots a_1 0 - 9p \cdot a_0 + a_0],$$

isto é,

$$p \mid [a_k a_{k-1} \cdots a_0 - 9p \cdot a_0],$$

portanto

$$\mathrm{p} \mid (n - 9p \cdot a_0).$$

Logo

$$p \mid n.$$

Logo abaixo são apresentados alguns exemplos utilizando o Teorema de Sebá.

Exemplo 1) Verifique se $n = 898865$ é divisível por $p = 11$.

1° Passo.

$$y = \frac{p-1}{10} = \frac{11-1}{10} = 1.$$

2° Passo.

$$\begin{array}{r} 89886/\mathbf{5} \\ -5 \\ \hline 8988/\mathbf{1} \\ -1 \\ \hline \end{array}$$

$$\begin{array}{r}
898/\mathbf{7} \\
-7 \\
\hline
89/\mathbf{1} \\
-1 \\
\hline
8/\mathbf{8} \\
-8 \\
\hline
0
\end{array}$$

Como a diferença (0) é divisível por 11, conclui-se que 898865 é divisível por 11.

Exemplo 2) Verifique se $n = 78421$ é divisível por $p = 17$.

1° Passo.

$$y = \frac{3p - 1}{10} = \frac{3 \cdot 17 - 1}{10} = 5.$$

2° Passo.

$$\begin{array}{r}
7842/\mathbf{1} \\
-5 \\
\hline
783/\mathbf{7} \\
-35 \\
\hline
74/\mathbf{8} \\
-40 \\
\hline
3/\mathbf{4} \\
-20 \\
\hline
-17
\end{array}$$

Como a diferença (-17) é divisível por 17, conclui-se que 78421 é divisível por 17.

Exemplo 3) Verifique se $n = 13851$ é divisível por $p = 19$.

1° Passo.

$$y = \frac{9p - 1}{10} = \frac{9 \cdot 19 - 1}{10} = 17$$

2° Passo.

$$\begin{array}{r} 1385/\mathbf{1} \\ -17 \\ \hline 136/\mathbf{8} \\ -136 \\ \hline 0 \end{array}$$

Como a diferença (0) é divisível por 19, conclui-se que 13851 é divisível por 19.

Exemplo 4) Verifique se $n = 96968$ é divisível por $p = 23$.

1° Passo.

$$y = \frac{7p - 1}{10} = \frac{7 \cdot 23 - 1}{10} = 16.$$

2° Passo.

$$\begin{array}{r} 9696/\mathbf{8} \\ -128 \\ \hline 956/\mathbf{8} \\ -128 \\ \hline 82/\mathbf{8} \\ -128 \\ \hline -46 \end{array}$$

Como a diferença (-46) é divisível por 23, conclui-se que 96968 é divisível por 23.

Considerações Finais

Nesse trabalho apresentamos os Critérios de Divisibilidade de alguns números primos, e ao desenvolvermos a pesquisa foi necessário fazer uma abordagem considerável de conceitos e definições, como pré-requisito para o desenvolvimento do tema. Os resultados alcançados através das aplicações são simples, embora seja observado que a construção desses critérios não é tão simples quanto ao que se estuda no ensino básico. Além disso, observou-se que a criação desses critérios pode ser expandida para a divisibilidade de quaisquer números primos maiores que cinco, por meio de um teorema conhecido como Teorema de Sebá.

Concluiu-se inicialmente após uma breve revisão histórica, que a divisibilidade está presente nas atividades humanas desde o Período Paleolítico.

Observou-se que para uma compreensão mais precisa sobre o tema de pesquisa, é necessária uma compreensão de alguns conceitos de Teorias dos números, como Sistema de Numeração na Base Decimal, Algoritmos de Euclides, Máximo Divisor Comum e Aritmética dos Restos.

Ficou evidenciado que a eficiência dos Critérios de Divisibilidade reside no fato de que o método empregado pode ser aplicado de forma sucessiva até que se tenha que observar apenas a divisibilidade entre dois números relativamente pequenos.

Para concluir, as ideias sobre os critérios de divisibilidade apresentados nesse trabalho, pode tornar-se um material útil e fonte de inspiração para professores que queiram agregar os conceitos aqui desenvolvidos em suas práticas de ensino e no direcionamento de atividades que estimulem a descoberta aos estudantes interessados e curiosos.

Referências

[1] BOYER, C. B., **História da Matemática.** 2 ed. São Paulo, Editora Edgard Blucher, 1996.

[2] HEFEZ, A., **Aritmética.** 2 ed. Rio de Janeiro, Editora da SBM, 2016.

[3] HEFEZ, A., **Curso de Álgebra.** Rio de Janeiro, Associação Instituto de Matemática Pura e Aplicada, 2002.

[4] HEFEZ, A., **Elementos de Aritmética.** Rio de Janeiro, Editora da SBM, 2005.

[5] NASCIMENTO, S. VIEIRA, **Critério de Divisibilidade por Qualquer Número Primo Maior que Onze.** O Baricentro da Mente: Porque o Conhecimento é Infinito, 2012. Disponível em: https://www.obaricentrodamente.com/2012/03/criterios-de-divisibilidade-por.html. Acesso em: 23 de junho de 2020.

[6] TORRES, G. Z. **Divisibilidade por 3, 7, 9, 11, 13, 17,....** Revista do Professor de Matemática, Rio de Janeiro, n. 58.