UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

CRITÉRIOS DE DIVISIBILIDADE

LUÍS CARLOS DE SOUZA JUNQUEIRA

Trabalho de Conclusão de Curso apresentado para obtenção do grau de licenciado em Matemática.
Orientadora: Profª Carmem Suzane Comitre Gimenez

Florianópolis, julho de 2001.

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÂO DE CURSO** no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designados pela Portaria n.º 04/SC/99.

Profª Carmem Suzane Comitre Gimenez
Professora da disciplina

Banca Examinadora:

Profª Carmem Suzane Comitre Gimenez
Orientadora

Prof° Antônio Vladimir Martins

Profª Jane de Oliveira Gippa

À meu pai, Junqueira

AGRADECIMENTOS

Á meus pais, pelo apoio e incentivo de todos estes anos.

À Dorlete, minha amada, pela compreensão, amor e apoio incansável, e pelos fins de semana abdicados em virtude do meu trabalho.

À minha família.

À minha orientadora, professora Carmem, por sua atenção e todo tempo dedicado a realização deste trabalho.

À banca examinadora, pelas críticas e sugestões deste trabalho.

ÍNDICE

INTRODUÇÃO

A matemática é fascinante para muitas pessoas pelas oportunidades que oferece para a criação e a descoberta assim como pela sua utilidade. É contínuo e rápido o seu crescimento no sentido de satisfazer tanto a curiosidade quanto às necessidades de aplicação. Os estudantes podem desenvolver processos sistemáticos para tratar problemas, sejam ou não, de rotina ou de soluções imediatamente determináveis.

Para achar os fatores de um determinado número podemos sempre tentar, mas será muito mais fácil se pudermos dizer simplesmente olhando para o número se ele tem ou não um dado fator.

Foi pensando em resolver este problema que resolvi fazer meu trabalho de conclusão de curso.

O objetivo deste trabalho é servir como um material de pesquisa para estudantes e alunos interessados em desvendar os mistérios da teoria dos números. A apresentação é feita de tal forma que a matéria pode ser rapidamente compreendida pelos leitores.

No capítulo 1 falamos despretensiosamente um pouco da história da aritmética e dos grandes gênios da matemática.

No capítulo 2 encontramos os fundamentos necessários para o desenvolvimento da teoria da divisibilidade.

No capítulo 3, objeto central do texto, construímos ao fim a teoria completa da divisibilidade.

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

CAPÍTULO 1

Histórico

O conceito de número e o processo de contar desenvolveram-se tão antes dos primeiros registros históricos que a maneira como ocorreram é largamente conjetural. Não é difícil, porém, imaginar como isso provavelmente se deu. É razoável admitir que a espécie humana, mesmo nas épocas mais primitivas, tinha algum senso numérico, pelo menos ao ponto de reconhecer mais e menos quando se acrescentavam ou retiravam alguns objetos de uma coleção pequena, pois há estudos que mostram que alguns animais são dotados desse senso. Com a evolução gradual da sociedade, tornaram-se inevitáveis contagens simples. Uma tribo tinha que saber quantos eram seus membros e quantos eram seus inimigos e tornava-se necessário a um homem saber se seu rebanho de carneiros estava diminuindo. É provável que a maneira mais antiga de contar se baseasse em algum método de registro simples, empregando o princípio da correspondência biunívoca. Para uma contagem de carneiros, por exemplo, poderia se dobrar um dedo para cada animal. Podia-se também contar fazendo-se ranhuras no barro ou numa pedra, produzindo-se entalhes num pedaço de madeira ou fazendo-se nós em uma corda. Então talvez mais tarde, desenvolveu-se um arranjo de sons vocais para registrar verbalmente o número de objetos de um grupo pequeno. E mais tarde ainda, com o aprimoramento da escrita, foram surgindo arranjos de símbolos para representar esses números. Esse desenvolvimento hipotético encontra respaldo em relatórios de antropólogos que estudaram povos primitivos em nossa época.

Bases

Quando se tornou necessário efetuar contagens mais extensas, o processo de contar teve de ser sistematizado. Isso foi feito dispondo-se os números em grupos básicos convenientes, sendo a ordem de grandeza desses grupos determinadas em grande parte pelo processo de correspondência empregado. Esquematizando-se as idéias, o método consistia em escolher um certo número **b** como base e atribuir nomes aos números 1, 2,...,b. Para os números maiores do que **b** os nomes eram essencialmente combinações dos nomes dos números já escolhidos.

Como os dedos do homem constituíam um dispositivo de correspondência conveniente, não é de estranhar que o 10 acabasse sendo escolhido freqüentemente como o número **b** da base.

Há evidências de que 2, 3 e 4 serviam como bases primitivas. Por exemplo, há nativos de Queensland que contam "um, dois, dois e um, dois e dois, muito". Uma outra tribo da Terra do Fogo compõe seus primeiros e poucos nomes de números na base 3 e algumas da América do Sul usam de maneira análoga o 4.

Como seria de esperar, o sistema quinário, ou sistema de numeração de base 5 , foi o primeiro a ser usado extensivamente. Até hoje algumas tribos da América do Sul contam com as mãos; os Yulraghirs da Sibéria usam uma escala mista para contar. Ainda no século XIX se encontravam calendários de camponeses germânicos baseados no sistema quinário.

Há evidências de que o 12 pode ter sido usado como base em épocas pré-históricas, principalmente em relação a medidas. Essa base pode ter sido sugerida pelo número aproximado de lunações de um ano ou, talvez, pelo fato de 12 ter vários divisores inteiros.

O sistema vigesimal (base 20) também foi amplamente utilizado, e remonta aos dias em que o homem andava descalço. Esse sistema foi usado por índios Americanos, sendo mais conhecido pelo bem desenvolvido sistema de numeração Maia. Também se encontravam traços no gaélio, no dinamarquês e no inglês. Em inglês há a palavra score (uma vintena), freqüentemente usada.

O sistema sexagesimal (base 60) foi usado pelos babilônios, sendo ainda empregado na medida de tempo e de ângulos em minutos e segundos.

Números digitais e números escritos

Além dos números falados, uma certa época usavam-se largamente os números digitais (representados por meio de dedos). Com efeito, a expressão de números por meio de várias posições dos dedos e das mãos talvez preceda os símbolos numéricos ou os nomes dos números. Assim, os símbolos escritos primitivos para 1, 2, 3 e 4 eram invariavelmente o número conveniente de riscos verticais ou horizontais, representando o número correspondente de dedos levantados ou estendidos, remontando a palavra dígito (isto é "dedo"), para indicar os algarismos de 1 a 9, à mesma origem.

Com o tempo, os números digitais foram estendidos de modo a abranger os números maiores que ocorriam nas transações comerciais; perto da Idade Média eles tinham se tornado internacional.

Embora os números digitais tivessem se originado em épocas muito remotas, ainda são usados hoje por alguns povos primitivos da África. Nas Américas do Sul e do Norte, alguns indígenas e algumas tribos de esquimós ainda usam os dedos. Os números digitais tinham a vantagem de transcender diferenças de linguagem mas, como os números vocais, deixavam a desejar quanto a permanência e não eram convenientes para a realização de cálculos. Já mencionamos o uso de marcas e entalhes como maneiras primitivas de registrar números. Esses expedientes provavelmente representam as primeiras tentativas por parte do homem de escrever. De qualquer maneira, desses primeiros esforços no sentido de fazer registros permanentes de números resultaram vários sistemas de numeração escritos. Voltaremos nossa atenção para o sistema de numeração posicional.

Sistemas de numeração posicionais

Nosso próprio sistema de numeração é um exemplo de um sistema de numeração posicional. Para esse sistema, depois de se escolher uma base **b**, adotam-se símbolos para 0, 1, 2,..., b-1.

Assim, há no sistema **b** símbolos básicos, que no caso de nosso sistema chamamos dígitos ou algarismos. Qualquer número **N** pode ser escrito de maneira única na forma

$$\mathbf{N} = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_2 b^2 + a_1 b + a_0,$$

onde $0 \leq a_i < b$, i = 0, 1,..., n. Por isso então representamos o número **N** na base **b** pela seqüência de símbolos:

$$(a_n a_{n-1} \ldots a_2 a_1 a_0)_b$$

Assim, um símbolo básico em qualquer numeral dado representa um múltiplo de alguma potência da base, potência essa que depende da posição ocupada pelo símbolo básico. Em nosso próprio sistema de numeração indo-arábico, 2 em 206 representa 2.10^2 ou 200. Deve-se notar que para clareza completa necessita-se de um símbolo para o zero, a fim de indicar a ausência possível de alguma potência da base. Um sistema de numeração posicional é uma conseqüência lógica, embora não necessariamente histórica, de um sistema de agrupamentos multiplicativo.

Os babilônios antigos desenvolveram, em algum momento entre 3000 e 2000 a.C., um sistema sexagesimal que empregava o princípio posicional. O sistema de numeração babilônico é, porém, misto, na medida em que, embora os números superiores a 60 fossem escritos de acordo com o princípio posicional, os 60 números correspondentes ao grupo básico eram escritos nos moldes de um sistema de agrupamento simples e decimal. Esse sistema de numeração posicional ressentiu-se, até depois do ano 300 a.C., da falta de um símbolo para o zero que representasse as potências ausentes de 60, levando assim a possíveis mal-entendidos na expressão de um número dado. Finalmente introduziu-se um símbolo, consistindo em duas cunhas pequenas, inclinadas, mas esse símbolo só era usado para indicar uma potência ausente de 60 dentro de um número, nunca quando ele ocorresse no seu final. Esse símbolo era, portanto, apenas um zero parcial, pois um zero verdadeiro serve para indicar as potências ausentes da base tanto no meio como no final dos números, como é o caso dos nossos 304 e 340.

Muito interessante é o sistema de numeração maia. De origem remota e desconhecida, foi descoberto pelas expedições espanholas no início do século XVI. Esse sistema é essencialmente vigesimal, mas seu segundo grupo vale 18.20 = 360 em vez de $20^2 = 400$. Os grupos de ordem superior são da forma 18.20". A explicação para essa discrepância reside no fato de o ano maia consistir em 360 dias. O símbolo para o zero era usado consistentemente. Esse sistema de base mista era usado pela classe sacerdotal. Há relatos de um sistema vigesimal puro usado pelo povo, mas que não sobreviveu em forma escrita.

O sistema de numeração Indo-arábico

O sistema de numeração Indo-arábico tem esse nome devido aos hindus, que o inventaram, e devido aos árabes que o transmitiram para a Europa Ocidental. As primeiras amostras datadas de 250 a.C., não contêm zero e não utilizam a notação posicional. Contudo, a idéia de valor posicional e um zero devem ter sido introduzidos na Índia algum tempo antes do ano 800 d.C., pois o matemático persa al- Khowârizmê descreveu de maneira completa o sistema hindu num livro do ano 825 d.C.

Como e quando os novos símbolos numerais entraram na Europa são questões ainda não decididas. Muito provavelmente eles foram levados por comerciantes e viajantes pelas costas do Mediterrâneo. Esses símbolos se encontram num manuscrito espanhol do século X, sendo possível que tenham sido introduzidos na Espanha pelos árabes que invadiram a península ibérica no ano 711 d.C, onde permaneceram até 1492 d.C. Mas foi uma tradução latina do tratado de al-khowârizmê, feita no século XII, seguida de alguns trabalhos europeus sobre o assunto, o que fez com que o sistema de disseminasse mais amplamente.

Os quatro séculos seguintes assistiram a uma verdadeira batalha entre abacistas e algoristas, como eram chamados os defensores do novo sistema, mas em torno do ano 1500 as atuais regras de computação acabaram se impondo. Mais um século e os abacistas haviam sido quase esquecidos, sendo que perto do século XVIII não restava mais nenhum traço do ábaco na Europa Ocidental.

Até que os símbolos dos numerais indo-arábicos se estabilizassem, com a invenção da imprensa de tipos móveis, muitas modificações em sua grafia se verificaram. Nossa palavra zero provavelmente provém da forma latinizada zephirum derivada de sifr que é uma tradução para o árabe de sunya, que em hindu significa "vazio" ou "vácuo". A palavra árabe sifr foi introduzida na Alemanha no século XIII, por Nemorarius, como Cifra, que em português significa, entre outras coisas, zero.

Aritmética pitagórica

Os gregos antigos faziam distinção entre o estudo das relações abstratas envolvendo os números e a arte prática de calcular com os números. Esta era conhecida como logística e aquela como aritmética. Essa distinção atravessou a Idade Média chegando até por volta do final do século XV, quando surgiram textos que tratavam as facetas teóricas e práticas da abordagem dos números sob a designação única de aritmética. É interessante que hoje aritmética tenha seu significado original na Europa Continental, ao passo que na Inglaterra e nos Estados Unidos o significado popular de aritmética corresponde à logística grega. Nos dois países citados usa-se a expressão teoria dos números para designar a faceta abstrata do estudo dos números.

Admite-se geralmente que os primeiros passos no sentido do desenvolvimento da teoria dos números e, ao mesmo tempo, do lançamento das bases do futuro misticismo numérico, foram dados por Pitágoras e seus seguidores movidos pela filosofia da fraternidade. Assim é que Jâmblico, um influente filósofo neoplatônico que viveu por volta de 320 d.C., atribui a Pitágoras a descoberta dos números amigáveis. Dois números se dizem amigáveis se cada um deles é igual à soma dos divisores próprios do outro. Por exemplo, 284 e 220, que constituem o par atribuído a Pitágoras, são amigáveis porque os divisores próprios de 220 são 1, 2, 4, 5, 10 ,11 ,20 ,44 ,55 e 110 cuja soma é 284, ao passo que os divisores próprios de 284 são 1, 2, 4, 71 e 142 cuja soma é 220. Esse par de números alcançou uma aura mística, e rezava a superstição posterior que dois talismãs com esses números selariam uma amizade perfeita entre os que os usassem. Os dois números vieram a ter um papel importante na magia, na feitiçaria, na astrologia e na determinação de horóscopos. Todos os números amigáveis inferiores a um bilhão já foram encontrados.

Também se atribuem aos pitagóricos os números perfeitos, deficientes e abundantes, que apresentam ligações místicas essenciais a especulações numerológicas. Um número se diz perfeito se é igual à soma de seus divisores próprios, deficiente se excede a soma de seus divisores próprios e abundante se é menor que a soma de seus divisores próprios. Assim Deus criou o mundo em seis dias, um número perfeito pois 1+2+3 = 6. Por outro lado , toda raça humana descende das oito almas da arca de Noé, sendo essa criação imperfeita porque 8 é deficiente, já que 1+2+4 < 8. Atualmente são conhecidos trinta números perfeitos.

O conteúdo dos "Elementos" de Euclides

Contrariando a impressão muito difundida, os Elementos de Euclides não tratam apenas de geometria, contém também teoria dos números e álgebra elementar.

Os Livros VII, VIII e IX, que no total têm cento e duas proposições, tratam da teoria elementar dos números. O Livro VII começa com o processo, hoje conhecido como algoritmo euclidiano, para achar o máximo divisor comum de dois ou mais números inteiros e o usa para verificar se dois inteiros são primos entre si. Estabelecem-se ainda nesse Livro muitas propriedades numéricas básicas.

No Livro IX encontram-se muitos teoremas significativos. Entre eles o importante teorema fundamental da aritmética, a saber, que todo natural maior que 1 pode se expressar como produto de primos de uma e, salvo quanto à ordem dos fatores, uma só maneira.

Fermat

Dentre as variadas contribuições de Fermat à matemática, a mais importante é a fundação da moderna teoria dos números. Neste campo a intuição e o talento de Fermat eram extraordinários. Sua atenção para a teoria dos números provavelmente foi despertada pela tradução latina da Aritmética de Diofanto, feita por Bachet de Méziriac em 1621. Muitas das contribuições de Fermat ao assunto se deram na forma de enunciados e notas escritas nas margens do exemplar que tinha do trabalho de Bachet.

Em 1670, cinco anos após sua morte esse material foi incorporado numa nova, mas infelizmente muito mal impressa, edição da Aritmética, publicada por um dos filhos de Fermat, Clément – Samuel. Muitos dos teoremas enunciados por Fermat mostraram-se depois verdadeiros. O exemplo seguinte ilustra o caráter das investigações de Fermat:

"Se p é primo e a é primo com p, então $a^{p-1}-1$ é divisível por p". Por exemplo se p = 5 e a = 2, então $a^{p-1}-1$ = 15 = 5.3. Esse teorema, conhecido como pequeno teorema de Fermat, foi apenas enunciado por Fermat numa carta de 18 de outubro de 1640 a Frénicle de Bessy. A primeira demonstração pública desse teorema data de 1736 e é devida a Euler.

Os números primos

Os números primos ostentam uma longa história, desde os dias dos gregos antigos até o presente. Como algumas das mais importantes descobertas sobre primos foram feitas no século XIX, parece apropriado discutir-se aqui esses interessantes números. O teorema fundamental da aritmética diz que os números primos são tijolos de construção a partir dos quais os outros inteiros são formados multiplicativamente. Por conseguinte, os números primos foram muito estudados e se fizeram esforços consideráveis no sentido de determinar a natureza de sua distribuição na seqüência dos inteiros positivos. Os principais resultados obtidos na antigüidade foram a prova da infinitude dos primos e o crivo de Eratóstenes para determinar os primos inferiores a um inteiro dado n.

Eratóstenes tornou-se célebre em aritmética devido a um dispositivo conhecido como crivo, usado para se acharem todos os números primos menores que um número n dado. Adotam-se, em ordem e começando por 3 , todos os números ímpares menores que n. Eliminam-se os números compostos da seqüência riscando-se, a partir do 3 (exclusive) todos os terceiros números que se seguem, depois a partir de 5 (exclusive) todos os quintos números que se seguem e assim por diante. Nesse procedimento riscam-se alguns números mais do que uma vez. Todos os números não-riscados, mais o número 2, formam a lista dos primos menores que n.

A partir do crivo de Eratóstenes pode-se obter uma fórmula para determinar o número de primos inferiores a n, quando se conhecem os primos inferiores a $\sqrt{n}$.

Não há, porém nenhum procedimento prático para testar se um número grande é primo e o esforço feito na verificação de alguns números particulares foi enorme.

Um sonho dos especialistas em teoria dos números é encontrar uma função f(n) que, para inteiros positivos n, forneça apenas números primos, uma infinidade desses números.

Assim $f(n) = n^2 - n + 41$ fornece primos para todo $n < 41$, mas $f(41) = 41^2$ é um número composto. O polinômio quadrático $f(n) = n^2 - 79n + 1601$ fornece primos para $n < 80$. Pode-se encontrar funções polinomiais que forneçam sucessivamente tantos primos quanto se deseje, mas nenhum deles fornecerá sempre números primos.

Em 1640 Pierre de Fermat conjeturou que $f(n) = 2^{2^n} + 1$ é primo para todos os inteiros não negativos n mas isso não é verdadeiro.

Um resultado recente e interessante, nessa linha, é a demonstração, feita em 1947 por W. H. Mills, da existência de um número real A tal que o maior inteiro que não excede A^{3^n} é primo, para todo inteiro positivo n. Nada se mostrou sobre o valor real nem mesmo sobre a ordem de grandeza por alto do número A.

Uma generalização notável do teorema de Euclides da infinitude dos primos foi estabelecida por Lejeune – Dirichlet (1805-1859) ao conseguir mostrar que toda a progressão aritmética a, a+d, a+2d, a+3d,..., onde a e d são primos entre si, contém infinitos números primos. A prova desse resultado está muito longe de ser fácil.

Talvez o mais surpreendente dos resultados já encontrados referente a distribuição dos primos seja o chamado teorema dos números primos. Indiquemos por A_n o número de primos abaixo de n. O teorema dos números primos assegura que $\frac{A_n \log_e n}{n}$ se aproxima de 1 conforme n cresce indefinidamente. Em outras palavras, $\frac{A_n}{n}$ chamada densidade dos primos entre os primeiros n inteiros, aproxima-se de $\frac{1}{\log_e n}$, tanto mais quanto maior for n. Esse teorema, que fora conjeturado por Gauss após o exame de uma grande tábua de números primos, foi provado independentemente em 1896 pelo francês J. Hodamard e pelo belga C. J. de la Vallée Poussim.

Nas pesquisas sobre números primos calcularam-se tábuas extensas de fatores. Com o advento dos computadores o trabalho de verificar se um número é primo e de construir tábuas de primos especiais se intensificou grandemente.

Há muitas conjeturas em aberto com relação aos números primos. Uma delas aponta para a existência de infinitos pares de primos gêmeos da forma p e p+2, como 3 e 5, 11 e 13 e 29 e 31. Outra é a conjetura feita por Christian Goldbach (1690-1764) em 1742 numa carta a Euler. Goldbach observou que todo inteiro par, exceto o 2, parecia ser exprimível como a soma de dois primos. Por exemplo, 4 = 2+2, 6 = 3+3, 8 = 5+3,...,16 = 13+3, 18 = 11+7,...,48 = 29+19,...,100 =

97+3 e assim por diante. Já se comprovou a hipótese de Goldbach para os números até 100 milhões.

As seguintes questões (nas quais n representa um inteiro positivo) sobre primos ainda não foram respondidas: há uma infinidade de primos da forma $n^2 + 1$? Sempre há um primo entre n^2 e $(n + 1)^2$? É um n qualquer, de um certo ponto em diante, ou um quadrado ou a soma de um primo e um quadrado? Há uma infinidade de números primos de Fermat (primos na forma $2^{2^n} + 1$) ?

Números negativos: origens

Coube também aos hindus a introdução na matemática dos números negativos. O objetivo era indicar débitos. O primeiro registro do uso de números negativos de que se tem notícia foi feito pelo matemático e astrônomo hindu Brahmagupta (598-?), que já conhecia inclusive as regras para as quatro operações com números negativos. Bhaskara (séc. XII), outro matemático e astrônomo hindu, assinalou que todo número positivo tem duas raízes quadradas, uma negativa e outra positiva, e salientou também a impossibilidade de se extrair a raiz quadrada de um número negativo.

Ao introduzirem os números negativos, os hindus não tinham nenhuma preocupação de ordem teórica. Na verdade, os progressos matemáticos verificados na Índia, por essa época, ocorreram quase que por acaso e em boa parte devido ao descompromisso com o rigor e a formalidade.

Mas a aceitação e o entendimento pleno dos números negativos foi um processo longo. Basta ver algumas designações que receberam: Stifel (1486-1567) os chamava de números absurdos; Cardano (1501-1576), de números fictícios. Descartes (1596-1650) chamava de falsas as raízes negativas de uma equação. Outros, como F. Viete (1540-1603), importante matemático francês, simplesmente rejeitava os números negativos.

A emergência de estruturas algébricas

As operações usuais como adição e multiplicação efetuadas no conjunto dos inteiros positivos são operações binárias: a cada par de inteiros positivos a e b associam-se univocamente inteiros c e d, chamados, respectivamente, soma de a e b e produto de a por b, e denotados pelos símbolos:

$c = a + b$ e $d = a \times b$.

Essas operações no conjunto dos inteiros têm algumas propriedades ou leis básicas. Por exemplo, se a, b, e c indicam inteiros positivos arbitrários, temos:

1. a + b = b + a (propriedade comutativa da adição)
2. a x b = b x a (propriedade comutativa da multiplicação)
3. (a+b) + c = a + (b+c) (propriedade associativa da adição)
4. (a x b) x c = a x (b x c) (propriedade associativa da multiplicação)
5. a x (b + c) = (a x b) + (a x c) (propriedade distributiva da multiplicação em relação à adição)

No início do século XIX a álgebra era considerada simplesmente como aritmética simbólica. Em outras palavras, em vez de trabalhar com números específicos, como fazemos em aritmética, em álgebra empregamos letras que representam esses números. As cinco propriedades acima são, portanto, afirmações sempre válidas na álgebra dos inteiros positivos. Mas como se trata de afirmações simbólicas, é imaginável que elas possam se aplicar a outros conjuntos de elementos, que não os inteiros positivos, desde que ofereçamos definições adequadas para as duas operações envolvidas. De fato, é isso o que ocorre.

Segue-se que as cinco propriedades básicas dos inteiros positivos há pouco listadas podem também ser considerados como propriedades de outros sistemas de elementos, inteiramente diferentes. As conseqüências das cinco propriedades precedentes constituem uma estrutura aplicável aos inteiros positivos, bem como outros sistemas, isto é, existe uma estrutura algébrica (as cinco propriedades básicas e suas conseqüências) comum ligada a muitos sistemas diferentes. As cinco propriedades básicas podem ser consideradas como postulados de um tipo particular de estrutura algébrica, e qualquer teorema que decorra formalmente desses postulados será aplicável a qualquer interpretação que ajuste às cinco propriedades básicas. Vistas as coisas assim, cortam-se os laços da álgebra com a aritmética, tornando-se aquela um campo de estudos puramente hipotético-dedutivo formal.

Os primeiros vislumbres dessa visão moderna da álgebra surgiram por volta de 1830 na Inglaterra, com o trabalho de Georg Peacock (1791-1858), um ex-aluno e professor da Universidade de Cambridge. Peacock foi um dos primeiros a estudar seriamente os princípios fundamentais da álgebra, e em 1830 publicou seu Treatise on Álgebra, no qual procurou dar à álgebra um tratamento lógico equiparável ao dos Elementos de Euclides, com o que ganhou o epíteto de "o Euclides da Álgebra". Peacock distinguia entre o que chamava "álgebra aritmética" e "álgebra simbólica". A primeira era considerada por ele como o estudo resultante do uso de símbolos para denotar os números decimais, como o de adição e o de multiplicação, aos quais podem-se sujeitar esses números. Assim, na "álgebra aritmética", certas operações são limitadas por sua aplicabilidade. Numa subtração a - b, por exemplo, devemos ter, a > b. A "álgebra simbólica" de Peacock, adota as operações da "álgebra aritmética" mas ignora suas restrições. Por exemplo, a subtração na "álgebra simbólica" difere da mesma operação na "álgebra aritmética" pelo fato de que na primeira ela sempre tem sentido. A justificativa dessas regras de extensão da "álgebra aritmética" para a "álgebra simbólica" era chamado por Peacock de princípio da permanência das formas equivalentes. A "álgebra simbólica" de Peacock é uma "álgebra aritmética" universal cujas operações são determinadas pelas da "álgebra aritmética", enquanto as duas álgebras caminham juntas, e pelo princípio da permanência das formas equivalentes em todos os outros casos.

O princípio da permanência das formas equivalentes foi considerado um conceito de grande alcance em matemática, e teve um papel histórico significativo em questões como o desenvolvimento inicial da aritmética do sistema de números complexos e a extensão das leis de potenciação, no caso de expoentes inteiros positivos para outros mais gerais. Por exemplo, se **a** é um número racional positivo e **n** é um inteiro positivo, então a^n é, por definição, o produto de **n** fatores iguais a **a**. Dessa definição decorre que, para quaisquer inteiros positivos **m** e **n**, $a^m a^n = a^{m+n}$. Pelo princípio da permanência das formas equivalentes, afirmava Peacock que na "álgebra simbólica" se tem então $a^m a^n = a^{m+n}$, não importa de que natureza possam ser a base **a** e os expoentes **m** e **n**. O nebuloso principio da permanência das formas equivalentes hoje está na lata do lixo da matemática, mas muitas vezes, quando tentamos estender uma definição, orientamo-nos de maneira que a definição mais geral preserve algumas das propriedades daquela que pretendemos generalizar.

Alguns contemporâneos britânicos de Peacock levaram avante seus estudos e empurraram a noção de álgebra para mais perto da maneira como modernamente se entende essa matéria. Assim, num artigo de Duncan Farquharson Gregory (1813-1844), publicado em 1840, as leis comutativa e distributiva da álgebra foram trazidas à luz. Augusto de Morgan (1806-1871), outro membro da escola Britânica de algebristas, deu algumas contribuições adicionais ao esclarecimento dos fundamentos da álgebra. No trabalho algo tateante da escola britânica, pode-se divisar a emergência da idéia de estrutura algébrica e a preparação para o programa postulacional no desenvolvimento da álgebra. Logo as idéias da escola britânica se espalharam pelo continente europeu, onde, em 1867, mereceram cuidadosa atenção de Hermann Hankel (1839-1873), um historiador de matemática alemão. Porém, antes ainda de surgir o tratamento de Hankel, o matemático Irlandês William Rowan Hamilton (1805-1865) e o matemático alemão Hermann Güinther Grassmann (1809-1877) tinham publicado resultados de grande alcance, resultados esses que levaram à libertação da álgebra, da mesma maneira que as descobertas de Lobachevsky e Bolyai levaram à libertação da geometria, e que abriram as comportas da álgebra abstrata.

CAPÍTULO 2

Neste capítulo faremos um estudo dos fundamentos necessários para o desenvolvimento da teoria da divisibilidade.

Números inteiros

Os números inteiros ou apenas inteiros são os nossos conhecidos:

..., -3, -2, -1, 0, 1, 2, 3,...

cujo conjunto representa-se pela letra Z, isto é:

$Z = \{..., -3, -2, -1, 0, 1, 2, 3,...\}$

Neste conjunto Z destacam-se os seguintes subconjuntos:

(1) Conjunto Z^* dos inteiros não nulos;

$Z^* = \{ x \in Z \mid x \neq 0 \} = \{ \pm 1, \pm 2, \pm 3,... \}$

(2) Conjunto Z_+ dos inteiros não negativos;

$Z_+ = \{ x \in Z \mid x \geq 0 \} = \{ 0, 1, 2, 3, ... \}$

(3) Conjunto Z_- dos inteiros não positivos;

$Z_- = \{ x \in Z \mid x \leq 0 \} = \{ 0, -1, -2, -3, ... \}$

(4) Conjunto (Z_+^*) dos inteiros positivos;

$Z_+^* = \{ x \in Z \mid x > 0 \} = \{ 1, 2, 3,... \}$

(5) Conjunto Z_-^* dos inteiros negativos;

$Z_-^* = \{ x \in Z \mid x < 0 \} = \{ -1, -2, -3,... \}$

Obs: O conjunto dos números inteiros não negativos é o conjunto dos números naturais.

Propriedades dos inteiros

O conjunto Z dos números inteiros munido das operações de adição (+) e multiplicação (.) possui as propriedades fundamentais que a seguir enumeramos, onde a, b e c são inteiros quaisquer, isto é, elementos de Z:

1. $a + b = b + a$ e $ab = ba$
2. $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$
3. $0 + a = a$ e $1.a = a$
4. $-a = (-1)a$ e $a - a = a + (-a) = 0$
5. $a(b + c) = ab + ac$
6. $0.a = 0$, e se $ab = 0$, então $a = 0$ ou $b = 0$.

Também existe uma "relação de ordem" entre os inteiros , representada pelo sinal " $\leq$ " (menor que), que possui as seguintes propriedades:

1. $a \leq a$ (reflexiva)
2. Se $a \leq b$ e $b \leq a$ então $a = b$ (anti-simétrica)
3. Se $a \leq b$ e $b \leq c$ então $a \leq c$ (transitiva)
4. Se $a \leq b$ então $a + c \leq b + c$ (compatibilidade com a adição)
5. Se $a \leq b$ e $c \geq 0$ então $ac \leq bc$ e se $a \leq b$ e $c \leq 0$ então $bc \leq ac$

Podemos ainda definir a relação "$<$ ", como sendo: $a < b \Leftrightarrow a \leq b$ e $a \neq b$, que satisfaz as propriedades 3, 4 e 5.

Elemento mínimo de um conjunto de inteiros

2.1. Definição - Seja A um conjunto de inteiros. Chama-se elemento mínimo de A um elemento $a \in A$ tal que $a \leq x$ para todo $x \in A$.

Representa-se pela notação "minA" , que se lê : " mínimo de A" .

2.2. Teorema - Se a é elemento mínimo de um conjunto $A \subset Z$, então este elemento é único.

Demonstração: Seja a = minA, se existisse um outro elemento mínimo b de A , teríamos :

(i) $a \leq b$, porque a = minA

(ii) $b \leq a$, porque b = minA

Logo , pela propriedade anti – simétrica da relação de ordem natural " $\leq$ " em Z , temos a = b.

O elemento mínimo de $A \subset Z$, se existe , denomina-se também primeiro elemento de A ou menor elemento de A .

2.3. Teorema (Principio da Boa Ordenação): Todo conjunto não vazio A de inteiros não negativos possui o elemento mínimo.

Em outros termos, todo subconjunto não vazio A do conjunto $Z_+ = \{ 0, 1, 2, 3,... \}$, possui o elemento mínimo.

2.4. Teorema (Princípio da indução finita): Seja S um subconjunto do conjunto N dos inteiros não negativos, que satisfaz as duas seguintes condições:

(1) 0 pertence a S;

(2) para todo inteiro não negativo k , se $k \in S$, então $k + 1 \in S$.

Nestas condições, S é o conjunto N dos inteiros não negativos.

Demonstração: Suponhamos, por absurdo, que S não é o conjunto N dos inteiros positivos e seja X o conjunto de todos os inteiros positivos que não pertencem a S , isto é :

$$X = \{ x \mid x \in N \text{ e } x \notin S \} = N - S$$

Então, X é um subconjunto não vazio de N e, pelo " Princípio da boa ordenação", existe o elemento mínimo x_0 de X.

Pela condição (1), $0 \in S$, de modo que $x_0 > 1$ e, portanto, $x_0 - 1$ é um inteiro positivo que não pertence a X. Logo, $x_0 - 1 \in S$ e , pela condição (2) , segue-se que $(x_0 - 1) + 1 = x_0 \in S$, o que é uma contradição, pois , $x_0 \in X = N - S$, isto é, $x_0 \notin S$. Assim sendo, $X = \varnothing$ e $S = N$.

Consoante este " Princípio da boa indução finita " , o único subconjunto de N que satisfaz às condições (1) e (2) é o próprio N.

2.5. Teorema: Seja P (n) uma proposição associada a cada inteiro positivo $n \geq a$ e que satisfaz às duas seguintes condições:

(1) P (a) é verdadeira ;

(2) para um inteiro positivo $k > a$, se P (k) é verdadeira, então P (k + 1) também é verdadeira.

Nestas condições, a proposição P (n) é verdadeira para todo inteiro positivo $n \geq a$

Demonstração: Seja S o conjunto de todos os inteiros positivos n para os quais a proposição P (n) é verdadeira, isto é:

$$S = \{ n \in N \mid P (n) \text{ é verdadeira} \}$$

Pela condição (1), P (1) é verdadeira e , portanto, $1 \in S$. Pela condição (2), para todo inteiro positivo k, se $k \in S$, então $k + 1 \in S$. Logo, o conjunto S satisfaz às condições (1) e (2) do " *Princípio de indução finita*" e , portanto, S = N , isto é , a proposição P (N) é verdadeira para todo inteiro positivo n .

NOTA. A demonstração de uma proposição usando-se este teorema chama-se " demonstração por indução" ou "demonstração por indução sobre n " .

Na demonstração por indução de uma dada proposição P (n) é obrigatório verificar que as condições (1) e (2) são ambas satisfeitas. A verificação da condição (2) implica em demonstrar o teorema auxiliar cuja hipótese é :

H : proposição P (k) é verdadeira, $k \geq a$,denominada " hipótese de indução ", e cuja tese ou conclusão é :

T: proposição P (k + 1) é verdadeira.

Relação de divisibilidade em Z

2.6. Definição: Sejam a e b dois inteiros. Diz –se que a divide b se e somente se existe um inteiro q tal que b = aq.

Se a divide b também se diz que a é um divisor de b , que b é múltiplo de a, que a é um fator de b ou que b é divisível por a.

Com a notação "$a \mid b$" indica-se que $a \neq 0$ divide b e , portanto, a notação " $a \nmid b$" significa que $a \neq 0$ não divide b.

A relação $a \mid b$ denomina-se relação de divisibilidade em Z .

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

2.7. Teorema: Quaisquer que sejam os inteiros a, b e c, tem-se:

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

(2) Se $a \mid 1$, então $a = \pm 1$

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

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

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

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

(7) Se $a \mid b$ e se $a \mid c$, então $a \mid (bx + cy)$, $\forall x,y \in Z$

Demonstração:

(1) Com efeito:

$0 = a.0$, $a = 1 . a$, $a = a . 1$

(2) Com efeito , se $a \mid 1$, então $1 = aq$, com $q \in Z$, o que implica $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, isto é : $a = \pm 1$.

(3) Com efeito:

$a \mid b \Rightarrow b = aq$, com $q \in Z$ e
$c \mid d \Rightarrow d = cq$, com $q_1 \in Z$

Portanto :

$bd = (ac)(qq_1) \Rightarrow ac \mid bd$

(4) Com efeito :

$a \mid b \Rightarrow b = aq$, com $q \in Z$ e $b \mid c \Rightarrow c = bq_1$, com $q_1 \in Z$

Portanto:

$c = a(qq_1) \Rightarrow a \mid c$

(5) Com efeito :

$a \mid b \Rightarrow b = aq$, com $q \in Z$ e $b \mid a \Rightarrow a = bq_1$, com $q_1 \in Z$

Portanto:

$a = a(qq_1) \Rightarrow qq_1 = 1 \Rightarrow q_1 \mid 1$ e $\Rightarrow q_1 = \pm 1 \Rightarrow a = \pm b$

(6) Com efeito :

$a \mid b$, $b \neq 0 \Rightarrow b = aq$, $q \neq 0$ e $|b| = |a| \, |q|$
Como $q \neq 0$, segue-se que $|q| \geq 1$ e , portanto $|b| \geq |a|$

(7) Com efeito :

$a \mid b \Rightarrow b = aq$, com $q \in Z$ e $a \mid c \Rightarrow c = aq_1$, com $q_1 \in Z$

Portanto, quaisquer que sejam os inteiros x e y :

$bx + cy = aqx + aq_1y = a(qx + q_1y) \Rightarrow a \mid (bx + cy)$

Esta propriedade (7) admite uma óbvia generalização; isto é , se

$a \mid b_k$, para $k = 1, 2, \ldots, n$

então quaisquer que sejam os inteiros $x_1, x_2, \ldots, x_n$:

$a \mid (b_1x_1 + b_2x_2 + \ldots + b_nx_n)$

NOTA.O conjunto de todos os divisores de um inteiro qualquer a indica-se por D(a).

Algoritmo da divisão

2.8. Teorema: Se a e b são dois inteiros , com $b \neq 0$, então existem e são únicos os inteiros q e r que satisfazem às condições:

$a = bq + r \quad e \quad 0 \leq r < |b|$

Demonstração:

1) Para $b > 0$

Seja S o conjunto de todos os inteiros não negativos que são da forma $a - bx$, com $x \in Z$, isto é :

$S = \{ a - bx \mid x \in Z, a - bx \geq 0 \}$

Este conjunto S não é vazio, porque, sendo $b > 0$, temos $b \geq 1$ e, portanto, para $x = |a|$, resulta:

$a - bx = a + b|a| \geq a + |a| \geq 0$

Assim sendo, pelo "Princípio da boa ordenação", existe o elemento mínimo r de S tal que;

$r \geq 0$ e $r = a - ba$ ou $a = bq + r$, com $q \in Z$

Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos:

$0 \leq r - b = a - bq - b = a - b(q + 1) < r$

isto é, r não seria o elemento mínimo de S.

Para demonstrar a unicidade de q e r, suponhamos que existem dois outros inteiros q_1 e r_1 tais que

$a = bq_1 + r_1 \quad e \quad 0 \leq r_1 < b$

Então, teremos:

$bq_1 + r_1 = bq + r \Rightarrow r_1 - r = (q - q_1)\, b \Rightarrow b \mid (r_1 - r)$

Por outro lado, temos:

$-b < -r \leq 0$ e $0 \leq r_1 < b$

o que implica:

$-b < r_1 - r < b$, isto é: $\mid r_1 - r \mid < b$

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

2) Para $b < 0$

Se $b < 0$, então $\mid b \mid > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r tais que

$a = \mid b \mid q_1 + r$ e $0 \leq r < \mid b \mid$

ou seja, por ser $\mid b \mid = -b$:

$a = b(-q_1) + r$ e $0 \leq r < \mid b \mid$

Portanto, existem e são únicos os inteiros $q = -q$ e r tais que;

$a = bq + r$ e $0 \leq r < \mid b \mid$

Os inteiros q e r chamam-se respectivamente o quociente e o resto na divisão de a por b.

Observa-se que b é divisor de a se e somente se $r = 0$. Neste caso, temos $a=bq$ e o quociente q na divisão exata de a por b indica-se também por $\frac{a}{b}$.

2.9. Definição: Resto por deficiência

Uma vez obtido o maior múltiplo do divisor(D) , contido no dividendo(d) , se a divisão não é exata, depois de restado o dividendo este múltiplo cria uma diferença, que se chama resto por deficiência, e o designaremos por r .

De um modo geral : $r = d - Dc$, de onde $D = dc + r$.

2.10. Definição: Resto por excesso

D está compreendido entre dois múltiplos de d , que são dc e $d(c + 1)$. Do mesmo modo que temos chamado resto por deficiência a diferença entre D e o

múltiplo menor, chamaremos resto por excesso, r' , a diferença entre o múltiplo maior e D , ou seja r' = d (c + 1) – D.

Quando não se especificar a classe de resto se subentende que se trata de resto por deficiência.

Somando as expressões que definem os restos, teremos: r + r' = d, ou seja , a soma dos restos por deficiência e por excesso é igual ao divisor. Logo, os restos por excesso e por deficiência são ambos menores que o divisor.

Máximo divisor comum de dois inteiros

2.11. Definição: Sejam a e b dois números inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d ($d > 0$) que satisfaz às condições:

(1) $d \mid a$ e $d \mid b$

(2) se $c \mid a$ e se $c \mid b$, então $c \mid d$.

Observa-se que, pela condição (1), d é um divisor comum de a e b, e pela condição (2), d é o maior dentre todos os divisores comuns de a e b.

O máximo divisor comum de a e b indica-se pela notação mdc (a, b).

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

(i) o mdc (a, 1) = 1
(ii) se $a \neq 0$, então o mdc (a, 0) = $\mid a \mid$
(iii)se $a \mid b$, então o mdc (a, b) = $\mid a \mid$

Existência e unicidade do mdc

2.12. Teorema: Se a e b são dois inteiros não conjuntamente nulos, então existe e é único o mdc (a, b); além disso, existem inteiros x e y tais que
mdc (a, b) = ax + by

Demonstração: Seja S o conjunto de todos os inteiros positivos da forma au + bv, com $u,v \in Z$, isto é:

$S = \{ au + bv \mid au + bv > 0 \text{ e } u,v \in Z \}$

Este conjunto S não é vazio, porque, p.ex., se $a \neq 0$, então um dos dois inteiros:

$a = a.1 + b.0$ ou $-a = a.(-1) + b.0$

é positivo e pertence a S. Logo, pelo " Princípio da boa ordenação ", existe e é único o elemento mínimo d de S : minS = d > 0. E, consoante a definição de S, existem inteiros x e y tais que d = ax + by.

Posto isto, vamos mostrar que d = mdc (a, b). Com efeito, pelo algoritimo da divisão, temos:

$a = dq + r$, com $0 \leq r < d$

o que dá:

$r = a - dq = a - (ax + by) q = a (1 - qx) + b (-qy)$

isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S, segue-se que r = 0 e a = dq, isto é, $d \mid a$.

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

Finalmente, se c é um divisor comum positivo qualquer de a e b ($c \mid a$ e $c \mid a$, $c > 0$), então:

$c \mid (ax + by) \Rightarrow c \mid d$

isto é, d é o maior divisor comum positivo de a e b, ou seja:

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

e o teorema fica demonstrado.

NOTA. A demonstração do teorema 4.1 deixa ver que o mdc (a, b) é menor inteiro positivo da forma ax + by, isto é, que pode ser expresso como combinação linear de a e b . Mas esta representação do mdc (a,b) como combinação linear de a e b não é única, pois, temos:

$mdc (a,b) = d = a (x + bt) + b (y - at)$

qualquer que seja o inteiro t.

Importa ainda notar que, se d = ar + bs, para algum par de inteiros r e s, então d não é necessariamente o mdc (a, b). Assim, p.ex., se :

mdc (a,b) = ax + by, então t.mdc (a, b) = atx + bty para todo inteiro t, isto é:

d = ar + bs

onde d = t. mdc (a, b), r = tx e s = ty

2.13. Teorema: Se a e b são dois inteiros não conjuntamente nulos, então o conjunto de todos os múltiplos do mdc (a, b) = d é

$T = \{ ax + by / x,y \in Z \}$

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

Por outro lado, existem inteiros x_0 e y_0 tais que

$d = ax_0 + bx_0$, pelo teorema anterior.

Assim, todo múltiplo kd de d é da forma:

$kd = k (ax_0 + bx_0) = a (kx_0) + b (ky_0)$

Isto é, kd é uma combinação linear de a e b e, portanto, kd é elemento do conjunto T.

Inteiros primos entre si

2.14. Definição: Sejam a e b dois inteiros não conjuntamente nulos.
Diz-se que a e b são primos entre si se e somente o mdc (a,b) = 1.

Dois inteiros a e b primos entre si admitem como únicos divisores comuns 1 e –1.

2.15. Teorema: Dois inteiros a e b , não conjuntamente nulos, são primos entre si se e somente se existem inteiros x e y tais que ax + by = 1.

Demonstração:

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

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

2.16. Corolário: Se o mdc(a,b) = d, então o mdc($\frac{a}{d}, \frac{b}{d}$) = 1.

Demonstração: Preliminarmente, observe-se $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, porque d é um divisor de a e b.
Posto isto, se o mdc (a, b) = d, então existem inteiros x e y tais que ax + by = d, ou seja, dividindo ambos os membros desta igualdade por d:

$$\frac{a}{d}x+\frac{b}{d}x=1$$

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

Assim, p.ex.:
mdc(-12, 30) = 6 e mdc (-12/6, 30/6) = mdc (-2,5) =1

2.17. Colorário: Se a, b, c $\in$ Z, a $|$ b e mdc(b,c) = 1 , então o mdc(a,c) = 1.

Demonstração: Com efeito;

a $|$ b $\Rightarrow$ b = aq, com q $\in$ Z, mdc (b,c) = 1 $\Rightarrow$ bx + cy = 1, com x,y $\in$ Z

Portanto:

a (qx) + cy = 1 $\Rightarrow$ mdc (a,c) = 1

2.18. Corolário: Se a $|$ c, b $|$ c e mdc (a,b) = 1, então ab $|$ c.

Demonstração: Com efeito:

a $|$ c $\Rightarrow$ c= aq_1, com $q_1 \in Z$
b $|$ c $\Rightarrow$ c= bq_2, com $q_2 \in Z$
mdc (a,b) = 1 $\Rightarrow$ ax + by = 1, com x,y $\in$ Z $\Rightarrow$ acx +bcy = c

Portanto:

c = a(bq_2)x + b(aq_1)y = ab(q_2x + q_1y) $\Rightarrow$ ab $|$ c

Observa-se que somente as condições a$|$ c e b $|$ c não implicam ab $|$ c.

2.19. Corolário: Se mdc (a, b) = 1 = mdc (a, c), então o mdc (a, bc) = 1.

Demonstração: Com efeito:

mdc (a,b) = 1 $\Rightarrow$ ax + by = 1, com x,y $\in$ Z
mdc (a,c) = 1 $\Rightarrow$ az + ct = 1, com z,t $\in$ Z

Portanto multiplicando temos:

1 = (ax + by) (az + ct) = ax . az + ax.ct+by.az+by.ct = $\underline{a}$(xaz+xct+byz) + (bc).(yt), que indica mdc(a, bc) = 1.

2.20. Corolário: Se o mdc (a,bc) = 1, então mdc (a,b) = 1 = mdc (a,c).

Demonstração: Com efeito:

mdc (a,bc) = 1 $\Rightarrow$ ax + (bc)y = 1, com x,y $\in$ Z

Portanto:

ax + b(cy) = 1 $\Rightarrow$ mdc (a,b) = 1
ax + c(by) = 1 $\Rightarrow$ mdc (a,c) = 1

Nota-se que esta proposição é a recíproca da anterior.

2.21. Teorema: (de EUCLIDES) Se a | bc e se o mdc (a,b) = 1, então a | c.

Demostração: Com efeito,

a | bc $\Rightarrow$ bc = aq, com q $\in$ Z
mdc (a,b) = 1 $\Rightarrow$ ax + by = 1, com x,y $\in$ Z $\Rightarrow$ acx + bcy = c

Portanto:

c = acx + aqy = a(cx + qy) $\Rightarrow$ a | c

Nota-se que somente a condição a | bc não implica que a | c. Assim, p.ex., 12 | 9.8, mas 12 ł 9 e 12 ł 8, mdc (12,9) $\neq$ 1 e mdc (12,8) $\neq$ 1).

Números primos e compostos

2.22. Definição: Diz-se que um inteiro p é um número primo ou apenas primo se e somente se:

i. $p \neq 0$, $p \neq 1$, $p \neq -1$
ii. os únicos divisores de p são ± 1 e $\pm p$

Um inteiro a, $a \neq 0$, $a \neq 1$ e $a \neq -1$ que não é primo diz-se composto.

Assim, p.ex., os inteiros 2, 3, -5 e 7 são todos primos e os inteiros 4, 6, 8 e -10 são todos compostos.

Os inteiros 0, 1 e -1 não são nem primos nem composto, e por conseguinte se a é um inteiro qualquer, então a é primo, ou a é composto ou a = 1ou a = -1 ou a=0.

Obs 1: 2 e -2 são os únicos inteiros pares que são primos.

Obs 2: Um inteiro p é primo se e somente se | p | é primo.

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

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

2.24. Corolário: Se p é um primo tal que $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração: Se $p \mid a$, nada há para demonstrar, e se, ao invés, p não divide a, então, pelo teorema anterior, o mdc (p,a) = 1. Logo, pelo teorema 2.21(de EUCLIDES), $p \mid b$.

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

Demonstração: Usando o "Segundo Princípio da Indução", a proposição é verdadeira para n=1 (imediato) e para n = 2 (pelo Corolário 2.24). Suponhamos, pois, n > 2 e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (hipótese de indução).

Pelo corolário 2.23, se $p \mid a_1 a_2 \ldots a_n$, então $p \mid a_n$ ou $p \mid a_1 a_2 \ldots a_{n-1}$

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

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

Demonstração: Com efeito, pelo corolário 2.25, existe um índice k, com $1 \leq k \leq n$, tal que $p \mid q_k$, e como os únicos divisores positivos de q_k são 1 e q_k, porque $\pm q_k$ é primo, segue-se que p = 1 ou $p = \pm q_k$. Mas p > 1, porque p é primo. Logo, $p = \pm q_k$.

2.27. Teorema: Todo inteiro composto possui um divisor primo.

Demonstração: Seja a um inteiro composto. Consideremos o conjunto A de todos os divisores positivos de a, exceto os divisores triviais 1 e a, isto é:

$\{ x \in Z_+$ tal que $x \mid a$ e $1 < x < a \}$

Pelo Princípio da Boa Ordenação existe o elemento mínimo p de A, que vamos mostrar ser primo. Com efeito, se p fosse composto admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d \mid p$ e $p \mid a$, o que implica $d \mid a$, isto é, p não seria o elemento mínimo de A. Logo, p é primo.

Teorema fundamental da aritmética

Todo inteiro positivo $n > 1$ é igual a um produto de fatores primos.

Demonstração: Com efeito, se n é primo, nada há que demonstrar, e se n é composto, então, pelo teorema 2.27, possui um divisor primo p_1, e temos

$$n = p_1 n_1, \quad 1 < n_1 < n$$

Se n_1 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_1 é composto, então, pelo teorema 2.27, possui um divisor primo p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_2, \quad 1 < n_2 < n_1$$

Se n_2 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_2 é composto, então, pelo mesmo teorema 2.27, possui um divisor primo p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3, \quad 1 < n_3 < n_2$$

e assim por diante.

Assim sendo, temos a seqüência decrescente:

$$n > n_1 > n_2 > n_3 > \ldots > 1$$

e como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k que é um primo p_k ($n_k = p_k$), e por conseguinte teremos:

$$n = p_1 p_2 p_3 \ldots p_k$$

Esta igualdade representa o inteiro positivo $n > 1$ como produto de fatores primos.

2.28. Corolário: A decomposição de um inteiro positivo $n > 1$ como produto de fatores primos é única, a menos da ordem dos fatores.

Demonstração: Suponhamos que n admite duas decomposições como produto de fatores primos, isto é:

$n = p_1 p_2 p_3 \ldots p_r = q_1 q_2 q_3 \ldots q_s, \quad r \leq s$

onde os p_i e os q_j são todos inteiros primos e tais que;

$p_1 \leq p_2 \leq p_3 \ldots \leq p_r, \; q_1 \leq q_2 \leq q_3 \leq \ldots \leq q_s$

Como $p_1 \mid q_1 q_2 q_3 \ldots q_s$, existe um índice k, com $1 \leq k \leq s$, tal eu $p_1 = q_k$ (Corolário 2.24), de modo que $p_1 \geq q_1$. Analogamente, $q_1 = p_h$, com $1 \leq h \leq r$, de modo que $q_1 \geq p_1$. Portanto, temos $p_1 = q_1$, o que implica:

$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$

Com o mesmo raciocínio conclui-se que $p_2 = q_2$, o que implica:

$p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s$

e assim por diante.

Assim sendo, se subsiste a desigualdade $r < s$, então se chega necessariamente a igualdade:

$1 = q_{r+1} q_{r+2} \ldots q_s$

o que é absurdo, porque cada $q_j > 1$. Logo, r = s e temos:

$p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$

isto é, as duas decomposições do inteiro positivo n > 1 como produto de fatores primos são idênticas, ou seja, n admite uma única decomposição como produto de fatores primos.

2.29. Corolário: Todo inteiro positivo m > 1 admite uma única decomposição da forma:

$n = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_r^{\alpha_r}$

onde, para i = 1,2, ... , r, cada α_i é um inteiro positivo e cada p_i é um primo positivo, com $p_1 < p_2 < \ldots < p_r$, denominada decomposição canônica do inteiro positivo
n > 1.

2.30. Teorema:(de EUCLIDES) O conjunto dos números primos é infinito.

Demonstração: Suponhamos que existe um primo p_n maior que todos os demais primos $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ... , e consideremos o inteiro positivo:

$a = p_1 p_2 p_3 \ldots p_n + 1$

Como a > 1, o Teorema Fundamental da Aritmética permite afirmar que a tem pelo menos um divisor primo p. Mas, $p_1, p_2, p_3, \ldots, p_n$ são os únicos primos, de modo que p deve, necessariamente, ser igual a um desses n primos. Assim sendo:

$p \mid a \quad e \quad p \mid p_1 p_2 p_3 \ldots p_n$

o que implica:

$p \mid a - p_1 p_2 p_3 \ldots p_n$ ou $p \mid 1$

o que é absurdo, porque p > 1 e o único divisor positivo de 1 é o próprio 1. Logo, qualquer que seja o primo p_n existe um primo maior que p_n, isto é, o conjunto

{ 2, 3, 5, 7, 11, 13,... }

é infinito.

2.31. Teorema: Se um inteiro positivo a > 1 é composto, então a possui um divisor primo $p \leq \sqrt{a}$.

Demonstração: Com efeito, se o inteiro positivo a > 1 é composto, então:

a = bc, com 1 < b < a e 1 < c < a

Portanto, supondo $b \leq c$, teremos:

$b^2 \leq bc = a \Rightarrow b \leq \sqrt{a}$

Por ser b > 1, o Teorema Fundamental da Aritmética assegura que b tem pelo menos um divisor primo p, de modo que $p \leq b \leq \sqrt{a}$. Como $p \mid b$ e $b \mid a$, segue-se que $p \mid a$, isto é, o inteiro primo $p \leq \sqrt{a}$ é divisor de a .

Nota. O teorema anterior fornece um processo que permite reconhecer se um dado inteiro a > 1 é primo ou é composto: basta dividir a sucessivamente pelos primos que não excedem a $\sqrt{a}$.

Este processo, como logo se vê, é muito trabalhoso e, portanto, pouco prático, sendo até de aplicação impossível para inteiros muitos grandes.

Inteiros congruentes

2.32. Definição: Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se e somente se m divide a diferença a – b.

Em outros termos, a é congruente a b módulo m se e somente se existe um inteiro k tal que a – b = km.

Com a notação
$a \equiv b$ (mod.m)

indica-se que a é congruente a b módulo m. Portanto, simbolicamente:

$a \equiv b$ (mod.m) $\Leftrightarrow m \mid (a - b)$

ou seja :

$a \equiv b$ (mod.m) $\Leftrightarrow \exists\, k \in Z \mid a - b = km$

Se m não divide a diferença a - b, então diz-se que a é incongruente a b módulo m, o que se indica pela notação:

$a \not\equiv b$ (mod.m)

Nota-se que dois inteiros quaisquer são congruentes módulo 1, enquanto que dois inteiros são congruentes módulo 2 se ambos são pares ou se ambos impares.

Em particular, $a \equiv 0$ (mod.m) se e somente se $m \mid a$.

Caracterização de inteiros congruentes

2.33. Teorema: Dois inteiros a e b congruentes módulo m deixam o mesmo resto quando divididos por m.

Demonstração:

($\Rightarrow$) Suponhamos que $a \equiv b$ (mod.m). Então, por definição:

$a - b = km$, com $k \in Z$

Seja r o resto da divisão de b por m; então, pelo algoritmo da divisão:

$b = mq + r$, onde $0 \leq r < m$
Portanto:
$a = km + b = km + mq + r = (k + q)\, m + r$

E isto significa que r é o resto da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo resto r.

($\Leftarrow$) Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever:

$a = mq_1 + r$ e $b = mq_2 + r$, onde $0 \leq r < m$

e, portanto:

$a - b = (q_1 - q_2)m \Rightarrow m \mid (a-b) \Rightarrow a \equiv b \ (\text{mod.}m)$

Propriedades das congruências

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

(1) $a \equiv a$ (mod.m)
(2) Se $a \equiv b$ (mod.m), então $b \equiv a$ (mod.m)
(3) Se $a \equiv b$ (mod.m) e se $b \equiv c$ (mod.m), então $a \equiv c$ (mod.m)

Demonstração:

(1) Com efeito:

$m \mid 0$ ou $m \mid (a - a) \Rightarrow a \equiv a$ (mod.m)

(2) Com efeito, se $a \equiv b$ (mod.m), então $a - b = km$, com $k \in Z$.

Portanto:

$b - a = -(km) = (-k)m \Rightarrow b \equiv a$ (mod.m)

(3) Com efeito, se $a \equiv b$ (mod.m) e se $b \equiv c$ (mod.m), então existem inteiros h e k tais que

$a - b = hm$ e $b - c = km$

Portanto:

$a - c = (a - b) + (b - c) = hm + km = (h + k)m$

e isto significa que $a \equiv c$ (mod.m).

NOTA. Consoante este teorema, a relação R no conjunto Z dos inteiros definida por $aRb \Leftrightarrow a \equiv b$ (mod.m)

é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em Z.

Esta relação de equivalência R em Z é denominada "congruencia módulo m".

2.35. Teorema: Seja m um inteiro positivo fixo (m > 0) e sejam a e b dois inteiros quaisquer. Valem as seguintes propriedades:

1. Se $a \equiv b$ (mod.m) e se $n \mid m$, com $n > 0$, então $a \equiv b$ (mod.n)
2. Se $a \equiv b$ (mod.m) e se $c > 0$, então $ac \equiv bc$ (mod.mc).

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

Demonstração:

(1) Com efeito:

a ≡ b (mod.m) ⇒ a – b = km e n | m ⇒ m = nq onde k e q > 0 são inteiros.

Portanto:

a – b = (kq)n ⇒ a ≡ b (mod.n)

(2) Com efeito:

a ≡ b (mod.m) ⇒ a – b = km ⇒ ac – bc = k(mc) ⇒ ac ≡ bc (mod.mc)

(3) Com efeito

a ≡ b (mod.m) ⇒ a – b = km ⇒ $\frac{a}{d} - \frac{b}{d} = k(\frac{m}{d})$

⇒ $\frac{a}{d} \equiv \frac{b}{d}$ (mod. $\frac{m}{d}$)

Assim, p.ex.:

- 15 ≡ 9 (mod.8) ⇒ - 15 ≡ 9 (mod.4)
7 ≡ - 8 (mod.3) ⇒ 35 ≡ -40 (mod.15)
36 ≡ - 24 (mod.8) ⇒ 9 ≡ - 6 (mod.3)

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

(1) Se a≡ b (mod.m) e se c ≡ d (mod.m), então
a + c≡ b + d (mod.m) e ac ≡ bd (mod.m)

(2) Se a≡ b (mod.m), então a + c ≡ b + c (mod.m) e
ac ≡ bc (mod.m)

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

Demonstração:

(1) Com efeito, se a ≡ b (mod.m) e se c ≡d (mod.m), então existem inteiros h e k tais que a – b = hm e c – d = km. Portanto:

(a + c) – (b + d) = (a – b) + (c – d) = hm + km = (h + k)m e
ac – bd = (b + hm) (d + km) – bd = (bk + dh + hkm)m

o que implica:

$a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$

(2) Com efeito, se $a \equiv b \pmod{m}$, como $c \equiv c \pmod{m}$, temos, pela propriedade anterior:

$a + c \equiv b + c \pmod{m}$ e $ac \equiv bc \pmod{m}$

(3) Usando o Princípio de Indução, a proposição é verdadeira para n = 1, e suposta verdadeira para um inteiro positivo k, temos:

$a^k \equiv b^k \pmod{m}$ e $a \equiv b \pmod{m}$

Portanto, pela propriedade (1):

$a^k . a \equiv b^k . b \pmod{m}$ ou $b^{k+1} \equiv b^{k+1} \pmod{m}$

isto é, a proposição é verdadeira para o inteiro positivo k + 1. Logo, a proposição é verdadeira para todo inteiro positivo n.

2.37. Teorema: Se $ac \equiv bc \pmod{m}$ e se o mdc (c, m) = d, então $a \equiv b \pmod{\frac{m}{d}}$.

Demonstração: Com efeito, se $ac \equiv bc \pmod{m}$, então:

$ac - bc = (a - b)c = km$, com $k \in Z$

Se o mdc (c, m) = d, existem inteiros r e s tais que c = dr e m = ds, onde r e s são primos entre si.Portanto:

$(a - b)dr = kds$ ou $(a - b)r = ks$

o que implica que $s \mid (a - b)r$, com o mdc (r,s) = 1. Logo, pelo teorema 2.30 (de EUCLIDES) : $s \mid (a - b)$ e $a \equiv b \pmod{s}$ ou, por ser $s = \frac{m}{d}$, $a \equiv b \pmod{\frac{m}{d}}$.

2.38. Corolário: Se $ac \equiv bc \pmod{m}$ e se o mdc (c,m) = 1, então $a \equiv b \pmod{m}$.

Esta propriedade mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são relativamente primos com o módulo.

2.39. Corolário: Se $ac \equiv bc \pmod{p}$, com p primo, e se p não divide c, então $a \equiv b \pmod{p}$.

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

Representação dos inteiros em outras bases

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

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

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

Demonstração: Pelo algoritmo da divisão aplicado aos inteiros n e b, temos:

$$n = bq_1 + a_0, \quad 0 \leq a_0 < b \qquad (0)$$

Aplicando, agora, o algoritmo da divisão ao quociente q_1 e ao inteiro b, temos:

$$q_1 = bq_2 + a_1, \quad 0 \leq a_1 < b \qquad (1)$$

Analogamente,continuando a aplicar o algoritmo da divisão aos quocientes obtidos q_i e ao inteiro b, temos:

$$q_2 = bq_3 + a_2, \quad 0 \leq a_2 < b \qquad (2)$$

$$q_3 = bq_4 + a_3, \quad 0 \leq a_3 < b \qquad (3)$$

e assim por diante.

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

$$q_{m-1} = bq_m + a_{m-1}, \quad 0 \leq a_{m-1} < b \qquad (m\text{-}1)$$

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

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

$$\begin{array}{ll}
n = bq_1 + a_0, & 0 \leq a_0 < b \\
bq_1 = b^2q_2 + a_1b, & 0 \leq a_1 < b \\
b^2q_2 = b^3q_3 + a_2b^2, & 0 \leq a_2 < b \\
b^3q_3 1 = b^4q_4 + a_3b^3, & 0 \leq a_3 < b \\
\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\
b^{m+1}q_{m-1} = b^m a_m + a_{m-1}b^{m-1} & 0 \leq a_{m-1} < b
\end{array}$$

Somando ordenadamente todas essas m igualdades, teremos,

$$n + (bq_1 + b^2 q_2 + ... + b^{m-1} q_{m-1}) =$$
$$= (bq_1 + b^2 q_2 + ... + b^{m-1} q_{m-1}) +$$
$$+ (a_0 + a_1 b + a_2 b^2 + ... + a_{m-1} b^{m-1} + a_m b^m)$$

ou, finalmente:

$$n = a_m b^m + a_{m-1} b^{m-1} + ... + a_2 b^2 + a_1 b + a_0$$

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

$0 \leq a_i < b$ (i = 0,1,2,...,m), sendo $a_m \neq 0$

Este polinômio representa-se, de modo abreviado, pela notação:

$$n = (a_m a_{m-1} \ldots a_2 a_1 a_0)_b$$

em que os coeficientes a_i são indicados pela ordem respectiva, figurando o inteiro b como um índice.

A unicidade desta representação é uma conseqüência imediata do teorema 2.13.

O inteiro b chama-se base e é costume dizer que n está escrito em base b.

Critérios de divisibilidade

Chama-se de critério de divisibilidade todo conjunto de condições que permitem reconhecer se um inteiro dado é divisível por outro.

Assim, p.ex., um inteiro n é divisível por 2 se n é par. E como n é par se o algarismo das unidades de n é par, segue-se que o critério da divisibilidade por 2 é que o algarismo das unidades do inteiro dado seja 0, 2, 4, 6 ou 8.

Todo inteiro positivo n pode ser expresso sob a forma 10k + r, onde r é um inteiro tal que $0 \leq r < 10$, de modo que n é divisível por 5 se 10k + r é divisível por 5, isto é, se r = 0 ou r = 5. E como r representa o algarismo das unidades de n, segue-se que o critério de divisibilidade por 5 é que o algarismo das unidades do inteiro dado seja 0 ou 5.

As propriedades da relação da congruência permitem estabelecer critérios especiais de divisibilidade de um inteiro dado por outro, mas muitos deles são de difícil aplicação e, portanto, carecem de utilidade prática.

2.41. Lema: Se $a \equiv b \pmod{m}$ e se

$$P(x) = \sum_{k=0}^{n} c_k x^k = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$$

é um polinômio em x com coeficiente c_k inteiros, então:

$P(a) \equiv P(b) \pmod{m}$

Demonstração: Por ser $a \equiv b \pmod{m}$, temos (Teorema 2.30):

$a^k \equiv b^k \pmod{m}$, para $k = 0, 1, 2, \ldots, n$

E, portanto:

$c_k a^k \equiv c_k b^k \pmod{m}$, para $k = 0, 1, 2, \ldots, n$

Somando ordenadamente todas essas n + 1 congruências, obtemos:

$$\sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod{m}$$

ou seja:

$P(a) \equiv P(b) \pmod{m}$

Se $P(a) \equiv 0 \pmod{m}$, diz-se que a é uma solução da congruência $P(x) \equiv 0 \pmod{m}$.

2.42. Corolário: Se a é uma solução da congruência $P(x) \equiv 0 \pmod{m}$ e se $a \equiv b \pmod{m}$, então b também é uma solução desta congruência.

Demonstração: Com efeito, pela proposição anterior, temos

$P(a) \equiv P(b) \pmod{m}$.

Portanto, se a é uma solução de $P(x) \equiv 0 \pmod{m}$, então:

$P(b) \equiv P(a) \equiv 0 \pmod{m}$

De modo que b também é uma solução de $P(x) \equiv 0 \pmod{m}$.

Critério de divisibilidade por 9

2.43. Teorema: Seja

$$n = a_m . 10^m + a_{m-1} . 10^{m-1} + \ldots + a_1 . 10 + a_0$$

a representação no sistema decimal (base 10) do inteiro positivo n, onde cada a_k é um inteiro tal que $0 \leq a_k < 10$, e seja S a soma dos seus algarismo:

$$S = a_0 + a_1 + \ldots + a_{m-1} + a_m$$

Então, o inteiro positivo n é divisível por 9 se e somente se S é divisível por 9.

Demonstração: Consideremos o polinômio em x com coeficientes inteiros:

$$P(x) = \sum_{K=0}^{m} a_k x^k$$

Por ser $10 \equiv 1 \pmod{9}$, temos (lema 2.41):

$$P(10) \equiv P(1) \pmod{9}$$

Como P(10) = n e P(1) = S, segue-se que $n \equiv S \pmod{9}$. Assim sendo $n \equiv 0 \pmod{9}$ se e somente se $S \equiv 0 \pmod{9}$, isto é, $9 \mid n$ se e somente se $9 \mid S$.

Assim, p.ex., o inteiro n = 26356734 é divisível por 9, porque a soma sos seus algarismos é

$$S = 2 + 6 + 3 + 5 + 6 + 7 + 3 + 4 = 36$$

e 36 é divisível por 9. Realmente:

$$26356734 = 9 \times 2928526.$$

Exemplo 1: Determinar os algarismos x e y do inteiro n = 75 x 4y de modo que n seja divisível por 5 e por 9.

Pelo critério de divisibilidade por 5 só podemos ter y = 0 ou y = 5, e pelo critério de divisibilidade por 9 devemos ter:

$$7 + 5 + x + 4 + y \equiv 0 \pmod{9}$$

ou

$$x + y \equiv -16 \equiv 2 \pmod{9}$$

Como x e y são ambos menores que 10, só podemos ter:
$x + y = 2$ ou $x + y = 11$

Se y = 0, então x = 2 ou x = 11 (impossível), o que dá o inteiro 75240. Se y = 5, então x = -3 (impossível) ou x = 6, o que dá inteiro 75645, isto é, o problema admite duas soluções.

Critério de divisibilidade por 11

2.44. Teorema: Seja

$n = a_m.10^m + a_{m-1}.10^{m-1} + ... + a_1.10 + a_0$

a representação no sistema decimal (base10) do inteiro positivo n, onde cada a_k é um inteiro tal que $0 \leq a_k < 10$, e seja

$$T = a_0 - a_1 + a_2 - ... + (-1)^m a_m$$

Então, o inteiro positivo n é divisível por 11 somente se T é divisível por 11.

Demonstração: Consideremos o polinômio em x com coeficientes inteiros:

$$P(x) = \sum_{k=0}^{m} a_k x^k$$

Por ser $10 \equiv -1 \pmod{11}$, temos (Lema 2.41)

$P(10) \equiv P(-1) \pmod{11}$

Como P(10) = n e P(-1) = T, segue-se que $n \equiv T \pmod{11}$. Portanto, $n \equiv 0 \pmod{11}$ se e somente se $T \equiv 0 \pmod{11}$, isto é, $11 \mid n$ se e somente se $11 \mid T$.

Assim, p.ex., o inteiro n = 1571724 é divisível por 11, porque a soma alternada:

$$T = 4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

é divisível por 11.

Note-se que este inteiro também é divisível por 9, porque a soma sos seus algarismos é 27 e 27 é divisível por 9.

CAPÍTULO 3

Neste capítulo encontramos a teoria completa da divisibilidade numérica, abrangendo todos os divisores inteiros, em todas as bases inteiras.

O homem não tem o poder ou a capacidade de pensar diretamente a quantidade contínua. Para estudá-la em profundidade, tem que medi-la, que transformá-la em uma união de partes hipotéticas, que reduzi-la mentalmente a grupos, conjuntos e sistemas de números. É operando desta forma que chegamos a compreender adequadamente a natureza e o modo de proceder nas operações fundamentais da aritmética.

Portanto, a aritmética é a fonte original e a base sobre que se assentam nossos conhecimentos matemáticos.

Algarismática

Definição: É a ciência das propriedades e das relações que os números abstratos adquirem, ou perdem, quando escrevemos em cada um dos sistemas de numeração possíveis.

Os números não apresentam todas as propriedades individuais que nós supomos, pelo contrário, o modo de escrever os números (o sistema de numeração adotado) lhes dá, ou lhes tira algumas propriedades, passando-as de um número para outro.

Ou seja, quando um número muda de sistema, sofre mudanças de propriedades. Por vezes uma só e mesma propriedade do número **x** no sistema de base **A** pode passar para o número **y** no sistema de base **B**. Por fim, predeterminando-se uma propriedade ou uma relação absurda no sistema de base **C** pode haver um sistema de base **D** em que o absurdo cesse, apresentando-se números que a possuam.

A aritmética em si é o conhecimento dos números e de suas propriedades essenciais. A teoria dos números varia com os modos de numeração adotados, por exemplo:

Na aritmética de base 8 um número é divisível por 8 quando termina pelo algarismo zero.

Na aritmética de base 9 um número é divisível por oito quando a soma de seus algarismos é múltipla de oito.

Há tantas aritméticas equivalentes quantos forem os sistemas de numeração possíveis, por conseguinte, devemos procurar e adotar a aritmética mais cômoda; aquela em que os teoremas se reduzem a um conteúdo e a um enunciado simples.

Cada nova aritmética empresta algumas qualidades novas e individuais a cada número e tira-lhe algumas propriedades antigas.

Podemos distribuir **n** algarismos, formando com eles igualdades absurdas e arbitrárias. Por via de regra, há sempre uma aritmética humana, de base **B**, capaz de fornecer números que verifiquem a igualdade predeterminada.

Uma igualdade arbitrariamente escrita, e absurda, na aritmética de base **X**, pode ser verdadeira ou evidente na aritmética de base **Y**. Por exemplo, predeterminando-se $\frac{50}{13} = \sqrt{14}$, verificamos que é uma igualdade errada, absurda, no sistema de base 10, porém é verdadeiro na base 12.

Portanto, a cada igualdade predeterminada com algarismos relacionados arbitrariamente, pode corresponder uma aritmética em que um ou alguns números a satisfaçam, isto é, em que a igualdade seja verdadeira. Este é o princípio fundamental do que se chama "algarismática".

Pesquisa dos critérios de divisibilidade em base 10

Todo número de **n** algarismos da forma $a_{n-1}a_{n-2}...a_2a_1a_0$ pode decompor-se em uma soma de tantas parcelas quantos são seus algarismos, a saber:

N = $a_0 + 10a_1 + 10^2a_2 + ... + 10^{n-1}a_{n-1}$, constando cada parcela de um algarismo multiplicado por uma potência de 10. O algarismo correspondente à parcela 10^{n-1} possui ordem **n** a começar da direita.

Ora, dividindo-se as parcelas e a soma por um só e mesmo número **D**, o resto da soma é igual a soma dos restos das parcelas módulo **D**. Portanto o resto da divisão de **N** por **D** é côngruo ao resto da divisão de a_0 por **D**, mais o resto da divisão de $10a_1$ por **D**, mais o resto da divisão de 10^2a_2 por **D** e assim por diante Mód **D**.

Acontece que o resto da divisão de um produto de dois fatores por um número **D** é côngruo ao produto do primeiro fator pelo resto da divisão do segundo fator por **D**, módulo **D**, logo:

Resto de $\frac{N}{D} \equiv a_0$ x Resto de $\frac{1}{D}$ + a_1 x resto de $\frac{10}{D}$+...+ a_{n-1} x resto de $\frac{10^{n-1}}{D}$ (Mód D).

Observando-se a congruência acima, vê-se que tanto faz efetuar separadamente as divisões $\frac{1}{D}, \frac{10}{D}, ..., \frac{10^{n-1}}{D}$, como efetuar uma divisão só $\frac{10^{n-1}}{D}$, em que os restos aparecem em cada passo do algoritmo.

Exemplo 1: divisão por 7.

	1000000	7
$r_0 \rightarrow$	10	0142857
$r_1 \rightarrow$	30	
$r_2 \rightarrow$	20	
$r_3 \rightarrow$	60	
$r_4 \rightarrow$	40	
$r_5 \rightarrow$	50	
$r_6 \rightarrow$	1	

Daí o seguinte;

Resultado 1: Para D $\in N^*$, N = $a_{n-1}10^{n-1}+...+a_1 10+a_0$ e r_1, r_2,..., r_{n-1} os restos de 10 por D, 10^2 por D,..., 10^{n-1} por D, respectivamente, temos:
D | N $\Leftrightarrow$ D | $(1.a_0+r_1.a_1+r_2.a_2+...+r_{n-1}a_{n-1})$

A cada um dos restos 1, r_1, r_2,..., r_{n-1}, denominamos **coeficiente de divisibilidade.**

Demonstração:
$\Rightarrow$
Hipótese : D | N
Tese: D | $(1.a_o +...+ r_{n-1}a_{n-1})$

Por Hipótese, N = D.X , X $\in$ N

$a_{n-1}.10^{n-1} +...+ a_1.10 + a_0 = D.X$
$10^{n-1} = Dq_{n-1} + r_{n-1} \Rightarrow r_{n-1} = 10^{n-1} - D.q_{n-1}$
$\vdots$
$10^2 = D.q_2 + r_2 \Rightarrow r_2 = 10^2 - D.q_2$
$10 = Dq_1 + r_1 \Rightarrow r_1 = 10 - D.q_1$
$1 = D.0 + 1, r_0 = 1$

$1.a_0 + r_1a_1 +...+ r_{n-1}a_{n-1} =$
$= 1.a_0 +(10-Dq_1)a_1 +...+ (10^{n-1} - Dq_{n-1}).a_{n-1} =$
$= 1.a_0 + 10a_1 - Dq_1a_1 +...+ 10^{n-1}a_{n-1} - Dq_{n-1}a_{n-1} =$
$= (1.a_0 + 10a_1 +...+ 10^{n-1}a_{n-1}) - D(q_1a_1 +...+ q_{n-1}a_{n-1} =$
$= D.X - D(q_1a_1 +...+q_{n-1}a_{n-1})$ que é múltiplo de D. Logo,
D | $(1.a_0 + r_1a_1 +...+ r_{n-1}a_{n-1})$
$\Leftarrow$
Hipótese : D | $(1.a_0 +...+ r_{n-1}a_{n-1})$

Tese: D | N

Por Hipótese, $a_0 + a_1 r_1 + ... + a_{n-1} r_{n-1} = D.y$, $y \in N$

$N = a_{n-1} 10^{n-1} + ... + a_1 .10 + a_0 =$

$= a_{n-1} .(Dq_{n-1} + r_{n-1}) + ... + a_1 (Dq_1 + r_1) + a_0 =$

$= a_{n-1} .Dq_{n-1} + a_{n-1} .r_{n-1} + ... + a_1 .Dq_1 + a_1 r_1 + a_0 =$

$= D (a_{n-1} q_{n-1} + ... + a_1 q_1) + (a_0 + a_1 r_1 + ... + a_{n-1} r_{n-1}) =$

$= D (a_{n-1} q_{n-1} + ... + a_1 q_1) + Dy$ que é múltiplo de D.

Logo, D | N

Exemplo 2: divisão por 3

	1000000	3
$r_0 \rightarrow$	10	0333333
$r_1 \rightarrow$	10	
$r_2 \rightarrow$	10	
$r_3 \rightarrow$	10	
$r_4 \rightarrow$	10	
$r_5 \rightarrow$	10	
$r_6 \rightarrow$	1	

Exemplo 3: quando D | 10, os restos que aparecem em cada passo da divisão serão zero, com exceção do primeiro resto que será $r_0 = 1$. Assim sendo, a divisibilidade dependerá apenas do algarismo de primeira ordem a_0.

	1000000	10
$r_0 \rightarrow$	10	0100000
$r_1 \rightarrow$	00	
$r_2 \rightarrow$	00	
$r_3 \rightarrow$	00	
$r_4 \rightarrow$	00	
$r_5 \rightarrow$	00	
$r_6 \rightarrow$	0	

Quando dividimos 1, 10, ..., 10^{n-2}, 10^{n-1} pelo divisor D, podemos tomar o quociente aumentado de 1. Neste caso, teremos o resto por deficiência.

No exemplo da divisão por 7.

1000 = 7 x 142 + **6** ou 1000 = 7 x 143 + (**-1**)

Assim,

6 ≡ **-1** (Mód 7); -1 = 6 - 7

10000 = 7 x 1428 + **4** ou 10000 = 7 x 1429 + (**-3**)

Assim,
4 ≡ **-3** (Mód 7); -3 = 4 - 7

100000 = 7 x 14285 + **5** ou 100000 = 7 x 14286 + (**-2**)
Assim,
5 ≡ **-2**(Mód 7); -2 = 5 - 7

Resultado 2: Sejam N ∈ N^*, D ∈ N^*, D > 1. Então, sendo N = Dq + r, q, r ∈ N e r < D, teremos r ≡ (r – D) (Mód D)
Demonstração: r – (r – D) = D e D | D logo, **r ≡ (r – D) (Mód D)**

Exemplo 4: Verificar se 703.101 é divisível por 7.
Sabemos que D | N ⇔ D | $(1.a_0 + r_1.a_1 + r_2.a_2 + ... + r_{n-1}a_{n-1})$, logo
7 | 703.101 ⇔ 7 | (1.1 + 0.3 + 1.2 - 3.1 - 0.3 - 7.2) = 3 - 17 = -14
Como 7 | -14, temos que 703.101 é divisível por 7.

Portanto, na aritmética de base dez, um número é divisível por 7, quando, dividido em grupos de três algarismos a partir da direita e multiplicadas as unidades de cada grupo por 1, as dezenas por 3 e as centenas por 2, a soma dos resultados dos grupos de lugar ímpar menos a soma dos resultados dos grupos de lugar par, resulta um múltiplo de sete.

Generalizando os critérios de divisibilidade por D numa base B.

Sempre é bom lembrar que se um número N é divisível por D em base B, ele será divisível por D qualquer que seja sua representação em outra base.

Em um sistema de base B um número se escreve como:
N = $a_{n-1}B^{n-1} + a_{n-2}B^{n-2} + ... + a_2B^2 + a_1B^1 + a_0$
Onde $a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0$ são os algarismos na base B, $0 \leq a_{n-1}, ..., a_2, a_1, a_0 \leq$ B –1.

Anotaremos as potências de base B da seguinte forma:
$B^{n-1} = 1.\underbrace{0.0...0}_{n-1 zeros}$
$B^2 = 1.0.0$
$B = 1.0$

Esta notação se justifica pois o próprio B em base B se escreve 1.0.

Exemplo 5:
978 em base 8 se escreve como:
$978 = 1.8^3 + 7.8^2 + 2.8 + 2$
8 em base 8 se escreve1.0, então:
978 = 1 . 1.0.0.0 + 7 . 1.0.0 + 2 . 1.0 + 2

Análogo ao que foi feito em base 10, com a nova notação para as potências da base B, verificamos que não precisamos efetuar cada divisão $\frac{1}{D}, \frac{1.0}{D}, ...$, etc. pois

os restos destas divisões aparecerão na seqüência da divisão da maior potência de B envolvida, por D.

Exemplo 6: Em base 11, a divisibilidade por 7, de um número de 4 algarismos, depende dos restos das divisões(em base 11):

1	7	,	1.0	7	,	1.0.0	7	,	1.0.0.0	7	,
1	0		**4**	1		40	16		40	163	
↓			↓			**2**			2 0		
r_0			r_1			↓			**1**		
						r_2			↓		
									r_3		

ou, com uma única divisão:

	1.0.0.0.0.0.0	7
$r_0 \rightarrow$	**10**	0163
$r_1 \rightarrow$	**40**	
$r_2 \rightarrow$	**20**	
$r_3 \rightarrow$	**1**	

Observe que em base 11, os restos da divisão das potências de 11 por 7 se repetem em grupos de 3: 1, 4, 2.

Assim, o critério pode ser colocado da seguinte maneira:

$7 \mid (a_{n-1}a_{n-2}...a_2a_1a_0) \Leftrightarrow 7 \mid (1.a_0 + 4.a_1 + 2a_2 + 1a_3 + 4a_4 + 2a_5 + ... + ka_{n-1})$, onde k=1, 4 ou 2, dependendo do número de algarismos do número.

Podemos, então, dizer que:

D | N $\Leftrightarrow$ D | $(1.a_0 + r_1.a_1 + ... + r_{n-1}.a_{n-1})$, onde:

1 é o resto da divisão de B^0 por D
r_1 é o resto da divisão de B por D
r_2 é o resto da divisão de B^2 por D
⋮
r_{n-1} é o resto da divisão de B^{n-1} por D

Se N = Dq + r,
$r \equiv (1.a_0 + r_1.a_1 + r_2.a_2 + ... + r_{n-1}a_{n-1})$ (mód D)

Os restos $r_0, r_1, r_2, ..., r_{n-1}$ são também chamados de **coeficientes de divisibilidade.**

Exemplo 7: $(1722)_8$ é divisível por 3?

$(1722)_8 = 1.8^3 + 7.8^2 + 2.8 + 2$

D = 3

$8^3 = 512 = 170 \times 3 + \mathbf{2}$

$8^2 = 64 = 21 \times 3 + \mathbf{1}$

$8 = 2 \times 3 + \mathbf{2}$

$1 = 0 \times 3 + \mathbf{1}$

$3 \mid N \Leftrightarrow 3 \mid (\mathbf{1}.2 + \mathbf{2}.2 + \mathbf{1}.7 + \mathbf{2}.1)$

como $3 \mid 15$, temos que $3 \mid N$ e $(1722)_8$ é divisível por 3.

Exemplo 8: $(347)_{12}$ é divisível por 11?

$(347)_{12} = 3.(12)^2 + 4.12 + 7$

Temos D = 11, vemos que;

$12^2 = 144 = 13 \times 11 + \mathbf{1}$

$12 = 1 \times 11 + \mathbf{1}$

$1 = 0 \times 11 + \mathbf{1}$

$11 \mid N \Leftrightarrow 11 \mid (\mathbf{1}.7 + \mathbf{1}.4 + \mathbf{1}.3)$

como $11 \nmid 14$, temos que $11 \nmid N$ e $(347)_{12}$ não é divisível por 11.

Os resultados anteriores permitem descobrir os critérios de divisibilidade em toda e qualquer base. Exige-se, porém, que se façam contas variadas. Vamos estabelecer, no entanto para evitar este inconveniente, um resultado mais simples, para isso vamos:

1º) Empregar um modo (tipo) de conta invariável para todos os casos;

2º) Descobrir imediatamente os critérios de divisibilidade, por qualquer número, em toda e qualquer base, operando apenas com a aritmética a que estamos habituados.

Resultado 3:

Em base B, os coeficientes de divisibilidade por D são côngruos módulo D a:
$(B-D)^0, (B-D)^1, (B-D)^2, \ldots$ ou, chamando B – D = n, $n^0, n^1, n^2, \ldots$
onde n = B - D é chamado coeficiente fundamental.

Demonstração: Os coeficientes de divisibilidade são os restos das divisões das potências da base B pelo divisor D. De acordo com o teorema de D'Alembert, o resto da divisão de uma potência de B por B - n se obtém substituindo B por n.

$N = B^{n-1}.a_{n-1} + \ldots + Ba_1 + a_0$

Coeficiente de Divisibilidade

$$B^{n-1} = Dq_{n-1} + r_{n-1}$$
$$B^{n-2} = Dq_{n-2} + r_{n-2}$$
$$\vdots$$
$$B^2 = Dq_2 + r_2$$
$$B = Dq_1 + r_1$$
$$1 = D.0 + 1$$

Seja B – D = n

Sabemos que dividir uma potência B^k por D, é como dividir um polinômio por D. Como D = B – n, estamos dividindo B^k por B – n.

Sabemos do Teorema de D'Alembert, que:

$B^k = (B - n)\,Q + R$

$R = B^k - (B - n)Q$

Substituindo B por n

$R = n^k - (n - n).Q$

$R = n^k$.

Assim, os restos das divisões das potências da base B por D serão dados pelas potências de **n**.

Usando a notação já estabelecida para as potências da base B temos:

Resto da divisão de $(1.0)^0$ por D = B – n : $n^0 = 1$;
Resto da divisão de 1.0 por D = B – n : n ;
Resto da divisão de 1.0.0 por D = B - n : n^2 ;
Resto da divisão de 1.0.0.0...0.0.0 ou B^m por D = B – n : n^m

Resumindo: Os restos das divisões das potências de B por B – n são: n^0, n^1, n^2, n^3,...,n^m.

Esta lei dá imediatamente os coeficientes de divisibilidade em toda e qualquer base e o número n = B – D (onde B é a base e D o número pelo qual estamos dividindo) é chamado **coeficiente fundamental**.

Exemplo 9: Quais os coeficientes de divisibilidade por 7, no sistema de base 10?

Solução: Vimos que podemos fazer D = B – n ou 7 = 10 – n. Logo n = 3 é o coeficiente fundamental em base 10, quando da divisibilidade por 7.

Fazendo $3^m \equiv r$ (Mód 7), obtemos os valores da tabela para m = 0, 1, 2, ...

m	a_m	3^m	r	r - 7
0	a_0	1	**1**	-6
1	a_1	3	**3**	-4
2	a_2	9	**2**	-5
3	a_3	27	6	**-1**
4	a_4	81	4	**-3**
5	a_5	243	5	**-2**
6	a_6	729	**1**	-6
7	a_7	2187	**3**	-4
⋮	⋮	⋮	⋮	⋮

Quando for conveniente, usaremos os coeficientes também da coluna r – 7, como assinalado.

Observe que a partir de m = 6 os valores de r (coeficiente de divisibilidade) se repetem. Podemos então trabalhar somente com 6 valores dos coeficientes, nesta seqüência: 1, 3, 2, -1, -3, -2.

Para um número com mais de 6 algarismos a seqüência dos coeficientes de divisibilidade se repete.

Logo, em base 10, um número é divisível por sete quando, selecionado em grupos de 3 algarismos, a contar da direita, e multiplicadas as unidades de cada grupo por 1, as dezenas por 3 e as centenas por 2, a soma dos resultados dos grupos de lugar ímpar menos a soma dos resultados dos grupos de lugar par, resulta um múltiplo de sete.

Assim, para sabermos, por exemplo, se o número 9.789.131é múltiplo de 7 devemos:

1º) Separar o número em grupos de 3 algarismos, a contar da direita:

$$\underbrace{009}_{3°\,grupo}\ ,\ \underbrace{789}_{2°\,grupo}\ ,\ \underbrace{131}_{1°\,grupo}$$

2º) Sempre contando a partir da direita, identificamos:

1º algarismo do 1º grupo: 1 = a_0
2º algarismo do 1º grupo: 3 = a_1
3º algarismo do 1º grupo: 1 = a_2

1º algarismo do 2º grupo: 9 = a_3
2º algarismo do 2º grupo: 8 = a_4
3º algarismo do 2º grupo: 7 = a_5

1º algarismo do 3º grupo: 9 = a_6

$$7 \mid 9.789.131 \Leftrightarrow 7 \mid a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 \qquad (1)$$

Observemos então que a expressão (1) pode ser escrita como:

$$\underbrace{1.1 + 3.3 + 2.1}_{grupo.de.lugar.impar} - \underbrace{1.9 + 3.8 + 2.7}_{grupo.de.lugar.par} + \underbrace{1.9}_{grupo.de.lugar.impar}$$

Esta soma resulta -26, que não é múltiplo de 7. Logo, 9.789.131 não é múltiplo de 7.

Exemplo 10: Quais são os coeficientes de divisibilidade por 11, no sistema de base 10?

Solução: D = B – n ou 11 = 10 – n. Logo n = -1 é o coeficiente fundamental em base 10, quando da divisibilidade por 11.

Fazendo $(-1)^m \equiv r$ (Mód 11), obtemos os valores da tabela para m = 0, 1, 2, ...

m	a_m	$(-1)^m$	r	r - 11
0	a_0	1	1	-10
1	a_1	-1	-1	10
2	a_2	1	1	-10
3	a_3	-1	-1	10
4	a_4	1	1	-10
5	a_5	-1	-1	10
6	a_6	1	1	-10
7	a_7	-1	-1	10
⋮	⋮	⋮	⋮	⋮

Como vemos, os coeficientes da coluna r – 11 não são convenientes.

Observe que a partir de m = 2 os valores de r (coeficiente de divisibilidade) se repetem. Podemos então trabalhar somente com 2 valores dos coeficientes, nesta seqüência: 1, -1.

Para um número com mais de 2 algarismos a seqüência dos coeficientes de divisibilidade se repete.

Logo, em base 10, um número é divisível por 11 quando, a soma de seus algarismos de ordem ímpar (a contar da direita) menos a soma de seus algarismos de ordem par, resulta um múltiplo de 11.

Exemplo 11: Quais os critérios de divisibilidade por 16, no sistema de base 12?

Solução: D = B – n ou 16 = 12 – n. Logo n = -4 é o coeficiente fundamental em base 12, quando da divisibilidade por 16.

Fazendo $(-4)^m \equiv r$ (Mód 16), obtemos os valores da tabela para m = 0, 1, 2, ...

m	a_m	$(-4)^m$	r	r - 16
0	a_0	1	1	-15
1	a_1	-4	4	-12
2	a_2	16	0	-16
3	a_3	-64	0	-16
4	a_4	256	0	-16
5	a_5	-1024	0	-16
6	a_6	4096	0	-16
7	a_7	-16384	0	-16
⋮	⋮	⋮	⋮	⋮

Como vemos, os coeficientes da coluna r – 16 não são convenientes.

Observe que a partir de m = 2 os valores de r (coeficiente de divisibilidade) se repetem e são iguais a zero. Podemos então trabalhar somente com 2 valores dos coeficientes, nesta seqüência: 1, 4.

Para um número com mais de 2 algarismos a seqüência dos coeficientes de divisibilidade se anulam.

Logo, em base 12, um número é divisível por 16, quando suas unidades da primeira ordem, (quando seu último algarismo) menos o quádruplo de suas unidades de segunda ordem (menos o quádruplo de seu penúltimo algarismo) dá múltiplo de 16.

Resultado 4: Em base B, os coeficientes de divisibilidade por B – 1, B – 2, B – 3, B – 4, B – 5, B – 6, B – 7,..., B – (B – 2), se obtêm escrevendo a seguinte série de coeficientes fundamentais:

	Divisibilidade por:				
Algarismo	B – 1	B - 2	B - 3	...	B – (B – 2) = 2
a_0	1^0	2^0	3^0	...	$(B-2)^0$
a_1	1^1	2^1	3^1	...	$(B-2)^1$
a_2	1^2	2^2	3^2	...	$(B-2)^2$
⋮	⋮	⋮	⋮		⋮

Exemplo 12: Em base 10, os coeficientes de divisibilidade por 9, 8, 7, 6, 5, 4, 3 e 2, são:

	Divisibilidade por:							
Alg.	**10-1=9**	**10-2=8**	**10-3=7**	**10-4=6**	**10-5=5**	**10-6=4**	**10-7=3**	**10-8=2**
a_0	1^0	2^0	3^0	4^0	5^0	6^0	7^0	8^0
a_1	1^1	2^1	3^1	4^1	5^1	6^1	7^1	8^1
a_2	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2
a_3	1^3	2^3	3^3	4^3	5^3	6^3	7^3	8^3
a_4	1^4	2^4	3^4	4^4	5^4	6^4	7^4	8^4
a_5	1^5	2^5	3^5	4^5	5^5	6^5	7^5	8^5
a_6	1^6	2^6	3^6	4^6	5^6	6^6	7^6	8^6
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Ou:

	Divisibilidade por:							
Alg.	**10-1=9**	**10-2=8**	**10-3=7**	**10-4=6**	**10-5=5**	**10-6=4**	**10-7=3**	**10-8=2**
a_0	1	1	1	1	1	1	1	1
a_1	1	2	3	4	5	6	7	8
a_2	1	4	9	16	25	36	49	64
a_3	1	8	27	64	125	216	343	512
a_4	1	16	81	256	625	1296	2401	4096
a_5	1	32	243	1024	3125	7776	16807	32768
a_6	1	64	729	4096	15625	46656	117649	262144
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Fazendo as congruências e tomando os coeficientes mais convenientes obtemos:

	Divisibilidade por:							
Alg.	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**
a_0	1	1	1	1	1	1	1	1
a_1	1	2	3	-2	0	2	1	0
a_2	1	4	2	-2	0	0	1	0
a_3	1	0	-1	-2	0	0	1	0
a_4	1	0	-3	-2	0	0	1	0
a_5	1	0	-2	-2	0	0	1	0
a_6	1	0	1	-2	0	0	1	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Assim, em base 10, podemos enunciar os critérios:

a) Um número é divisível por 9 quando a soma de seus algarismos resulta um múltiplo de 9;

b) Um número é divisível por 8 quando o primeiro algarismo da direita mais o dobro do segundo mais o quádruplo do terceiro, resulta um múltiplo de 8;

c) Um número é divisível por 7 quando selecionado em grupos de três algarismos, a contar da direita, e multiplicadas (em cada grupo) as unidades de primeira ordem por 1, as de segunda por 3 e as de terceira por 2, a soma dos resultados dos grupos de lugar impar menos a soma dos resultados dos grupos de lugar par, resulta um múltiplo de 7;

d) Um número é divisível por 6 quando o primeiro algarismo da direita menos o dobro da soma dos demais algarismos, resulta um múltiplo de 6;

e) Um número é divisível por 5 quando termina em 0 ou 5;

f) Um número é divisível por 4 quando o primeiro algarismo da direita mais o dobro do segundo algarismo, resulta um múltiplo de 4;

g) Um número é divisível por 3 quando a soma de seus algarismos resulta um múltiplo de 3;

h) Um número é divisível por 2 quando termina em 0, 2, 4, 6 ou 8.

Exemplo 13: Em base 12, considerando a = 10 e b = 11, os coeficientes fundamentais de divisibilidade por b, a, 9, 8, 7, 6, 5, 4, 3 e 2, são:

	Divisibilidade por:				
Alg.	**12-1=11**	**12-2=10**	**12-3=9**	**12-4=8**	**12-5=7**
a_0	1^0	2^0	3^0	4^0	5^0
a_1	1^1	2^1	3^1	4^1	5^1
a_2	1^2	2^2	3^2	4^2	5^2
a_3	1^3	2^3	3^3	4^3	5^3
a_4	1^4	2^4	3^4	4^4	5^4
⋮	⋮	⋮	⋮	⋮	⋮

	Divisibilidade por:				
Alg.	**12-6=6**	**12-7=5**	**12-8=4**	**12-9=3**	**12-10=2**
a_0	6^0	7^0	8^0	9^0	10^0
a_1	6^1	7^1	8^1	9^1	10^1
a_2	6^2	7^2	8^2	9^2	10^2
a_3	6^3	7^3	8^3	9^3	10^3
a_4	6^4	7^4	8^4	9^4	10^4
⋮	⋮	⋮	⋮	⋮	⋮

Ou:

	Divisibilidade por:				
Alg.	**12-1=11**	**12-2=10**	**12-3=9**	**12-4=8**	**12-5=7**
a_0	1	1	1	1	1
a_1	1	2	3	4	5
a_2	1	4	9	16	25
a_3	1	8	27	64	125
a_4	1	16	81	256	625
⋮	⋮	⋮	⋮	⋮	⋮

	Divisibilidade por:				
Alg.	**12-6=6**	**12-7=5**	**12-8=4**	**12-9=3**	**12-10=2**
a_0	1	1	1	1	1
a_1	6	7	8	9	10
a_2	36	49	64	81	100
a_3	216	343	512	729	1000
a_4	1296	2401	4096	6561	10000
⋮	⋮	⋮	⋮	⋮	⋮

Fazendo as congruências e tomando os coeficientes mais convenientes obtemos:

	Divisibilidade por:									
Alg.	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**
a_0	1	1	1	1	1	1	1	1	1	1
a_1	1	2	3	4	-2	0	2	0	0	0
a_2	1	4	0	0	-3	0	-1	0	0	0
a_3	1	-2	0	0	-1	0	-2	0	0	0
a_4	1	-4	0	0	2	0	1	0	0	0
a_5	1	2	0	0	3	0	2	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Assim, em base 12, podemos enunciar os critérios:

i) Um número é divisível por 11 quando, a soma de seus algarismos resulta um múltiplo de 11;

j) Um número é divisível por 10 quando, selecionado em grupos de dois algarismos a contar do segundo da direita, e multiplicados o primeiro algarismo de cada grupo por 2 e o segundo por 4, a soma dos resultados dos grupos de

lugar ímpar, menos a soma dos resultados dos grupos de lugar par, mais o primeiro algarismo da direita, resulta um múltiplo de 10;

k) Um número é divisível por 9 quando, o primeiro algarismo da direita mais o triplo do segundo, resulta um múltiplo de 9;

l) Um número é divisível por 8 quando, o primeiro algarismo da direita mais o quádruplo do segundo algarismo, resulta um múltiplo de 8;

m) Um número é divisível por 7 quando, selecionado em grupos de três algarismos a contar do segundo da direita e multiplicadas (em cada grupo) as unidades de primeira ordem por 2, as de segunda por 3 e as de terceira por 1, a soma dos resultados dos grupos de lugar par menos a soma dos resultados dos grupos de lugar ímpar, mais o primeiro algarismo da direita, resulta um múltiplo de 7;

n) Um número é divisível por 6 quando termina em 0 ou 6;

o) Um número é divisível por 5 quando, selecionado em grupos de dois algarismos, a contar da direita, e multiplicados o 1º algarismo de cada grupo por 1 e o segundo por 2, a soma dos resultados dos grupos de lugar ímpar, menos a soma dos resultados dos grupos de lugar par, resulta um múltiplo de 5;

p) Um número é divisível por 4 quando termina em 0, 4 ou 8;

q) Um número é divisível por 3 quando termina em 0, 3, 6 ou 9;

r) Um número é divisível por 2 quando termina em 0, 2, 4, 6, 8 ou a.

Resultado 5: Sejam B e D números naturais maiores que 1. Os coeficientes de divisibilidade por D em base B são iguais aos coeficientes de divisibilidade por D em base B + Dy, $\forall\, y \in N^*$, ou seja:

se $s_{n-1}, s_{n-2}, \ldots, s_1, s_0$ são coeficientes de divisibilidade por D em base B, então são também coeficientes de divisibilidade por D em base Dy + B, $y \in N^*$

Demonstração:

$$N = a_{n-1}B^{n-1} + \ldots + a_1 B + a_0$$
$$B^{n-1} = D.q_{n-1} + s_{n-1}$$
$$B^{n-2} = D.q_{n-2} + s_{n-2}$$
$$\vdots \qquad\qquad 0 \leq s_i < D$$
$$B^2 = Dq_2 + s_2$$
$$B^1 = Dq_1 + s_1$$
$$1 = Dq_0 + s_0$$

Também,

$$N = b_{n-1}(Dy + B)^{n-1} + \ldots + b_1 (Dy + B) + b_0$$

$$(Dy + B)^{n-1} = D.P_{n-1} + r_{n-1}$$
$$\vdots \qquad\qquad 0 \leq r_i < D$$
$$(Dy + B)^2 = D.P_2 + r_2$$
$$Dy + B = D.P_1 + r_1$$
$$1 = D.P_0 + r_0$$

Faremos por indução sobre a quantidade **n** de algarismos do número N.

$n = 1 : N = a_0, N = b_0$

$1 = Dq_0 + s_0$
$1 = Dp_0 + r_0$

$D(q_0 - p_0) = r_0 - s_0$
$D \mid r_0 - s_0, 0 \leq r_0, s_0 < D$
$\therefore r_0 - s_0 = 0 \Rightarrow r_0 = s_0$

Suponhamos $r_k = s_k$ e provemos para k + 1
$B^k = D.q_k + s_k$
$B^{k+1} = Dq_{k+1} + s_{k+1}$

$(Dy + B)^{k+1} = Dp_{k+1} + r_{k+1}$
$(Dy + B)^k . (Dy + B) = Dp_{k+1} + r_{k+1}$
H.I.
$(Dp_k + s_k).(Dy + B) = Dp_{k+1} + r_{k+1}$
$(Dp_k + B^k - Dq_k)(Dy + B) = Dp_{k+1} + r_{k+1}$
$D^2 p_k y + Dp_k B + B^k Dy + B^{k+1} - D^2 q_k y - D^2 q_k B = Dp_{k+1} + r_{k+1}$
$D[Dp_k y + p_k B + B^k y - Dq_k y - Dq_k B] + B^{k+1} = Dp_{k+1} + r_{k+1}$
$D.M + Dq_{k+1} + s_{k+1} = Dp_{k+1} + r_{k+1}$
$D(M + q_{k+1} + P_{k+1}) = r_{k+1} - s_{k+1}$

Portanto $D \mid r_{k+1} - s_{k+1}$ e $s_{k+1} = r_{k+1}$

Observemos que, como já foram estudados os critérios de divisibilidade para bases menores que B, o resultado 5 faz o estudo dos critérios para bases maiores que B. No entanto, o resultado continua válido para bases do tipo $B' = B - Dy$, para $y \in Z$. Neste caso, só devemos lembrar que a base é sempre um número positivo maior que 1.

Exemplo 14: Estudar a divisibilidade de 32109 por 3 em base B = 4.

Solução: Sabemos que $B' = B - Dy$ e fazendo y = -2 temos que $B' = 4 - 3.(-2) = 10$.

D = B - n ou 3 = 4 - n e 3 = 10 - n. Logo, n = 1 e n = 7 são os coeficientes fundamentais em base 4 e 10 respectivamente, quando da divisibilidade por 3.

Fazendo $1^m \equiv r'$ (Mód 3) e $7^m \equiv r''$ (Mód 3), obtemos os valores da tabela para m = 0, 1, 2, 3 e 4.

m	a_m	1^m	r'	7^m	r''
0	a_0	1	**1**	1	**1**
1	a_1	1	**1**	7	**1**
2	a_2	1	**1**	49	**1**
3	a_3	1	**1**	343	**1**
4	a_4	1	**1**	2401	**1**

Observamos que os coeficientes de divisibilidade por 3 em base 4 são os mesmos coeficientes de divisibilidade por 3 em base 4 + 3.2 = 10.

Portanto, $1a_0 + 1a_1 + 1a_2 + 1a_3 + 1a_4 = 1.9 + 1.0 + 1.1 + 1.2 + 1.3 = 15$. Como 15 é múltiplo de 3, então 32109 é divisível por 3 em base 4 e 10 respectivamente.

Resultado 6: (Corolário do resultado 5)

Seja D > 1 e considere a relação de equivalência em Z, n ≡ r (Mód D).

Esta relação determina D classes de equivalência, disjuntas, cuja união é Z.

$\overline{0} = \{ Dx / x \in Z \}$
$\overline{1} = \{ Dx + 1 / x \in Z \}$
$\overline{2} = \{ Dx + 2 / x \in Z \}$
⋮

$\overline{D - 1} = \{ Dx + (D - 1) / x \in Z \}$

Assim, qualquer número B pertence a um e somente um destes conjuntos.

Como os coeficientes de divisibilidade por D em base B são os mesmos para a base B + Dm, $\forall$ m $\in \mathbb{N}^*$, teremos então D listas de coeficientes de divisibilidade por D, que atenderão a todas as possíveis bases.

	Base						
a_n	**Dx**	**Dx + 1**	**Dx + 2**	**Dx + 3**		**Dx + (D – 2)**	**Dx + (D – 1)**
a_0	D^0	1^0	2^0	3^0	...	$(D-2)^0$	$(D-1)^0$
a_1	D^1	1^1	2^1	3^1	...	$(D-2)^1$	$(D-1)^1$
a_2	D^2	1^2	2^2	3^2	...	$(D-2)^2$	$(D-1)^2$
a_3	D^3	1^3	2^3	3^3	...	$(D-2)^3$	$(D-1)^3$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tomando as congruências, módulo D, obtemos os coeficientes mais convenientes.

Exemplo 15: Divisibilidade por 5 (5 classes de equivalência)

$\overline{0} = \{ 5x / x \in Z \} = \{..., -10, -5, 0, 5, 10,...\}$
$\overline{1} = \{ 5x + 1 / x \in Z \} = \{..., -9, -4, 1, 6, 11,...\}$
$\overline{2} = \{ 5x + 2 / x \in Z \} = \{..., -8, -3, 2, 7, 12,...\}$
$\overline{3} = \{ 5x + 3 / x \in Z \} = \{..., -7, -2, 3, 8, 13,...\}$
$\overline{4} = \{ 5x + 4 / x \in Z \} = \{..., -6, -1, 4, 9, 14,...\}$

Para bases do tipo B = 5x, teremos os coeficientes de divisibilidade por 5 em base 5 (ou base 10):

a_m	
a_0	1
a_1	0
a_2	0
⋮	⋮

Para bases do tipo B = 5x + 1, teremos os coeficientes de divisibilidade por 5 em base 6:

a_m	6 - 5 = 1
a_0	1
a_1	1
a_2	1
⋮	⋮

Para bases do tipo B = 5x + 2, teremos os coeficientes de divisibilidade por 5 em base 7 (ou base 2):

a_m	7 - 5 = 2
a_0	$2^0 = 1$
a_1	$2^1 = 2$
a_2	$2^2 = 4$ ou -1
a_3	$2^3 = 8$ ou -2
⋮	⋮

Para bases do tipo B = 5x + 3, teremos os coeficientes de divisibilidade por 5 em base 8 (ou base 3):

a_m	8 - 5 = 3
a_0	$3^0 = 1$
a_1	$3^1 = 3$ ou -2
a_2	$3^2 = 9$ ou -1
a_3	$3^3 = 27$ ou 2
⋮	⋮

Para bases do tipo B = 5x + 4, teremos os coeficientes de divisibilidade por 5 em base 9 (ou base 4):

a_m	9 - 5 = 4
a_0	$4^0 = 1$
a_1	$4^1 = 4$ ou -1
a_2	$4^2 = 16$ ou 1
a_3	$4^3 = 64$ ou -1
a_4	$4^4 = 256$ ou 1
⋮	⋮

Exemplo 16:Para D = 7 e já tomando as congruências, temos:

	Base						
a_n	7x	7x + 1	7x + 2	7x + 3	7x + 4	7x + 5	7x + 6
a_0	1	1	1	1	1	1	1
a_1	0	1	2	3	-3	-2	-1
a_2	0	1	-3	2	2	-3	1
a_3	0	1	1	-1	1	-1	-1
a_4	0	1	2	-3	-3	2	1
a_5	0	1	-3	-2	2	3	-1
a_6	0	1	1	1	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Todas as aritméticas de base inteira estão aqui representadas.

Logo, as listas de coeficientes de divisibilidade por sete, em todas as aritméticas de base inteira, são apenas sete.

Exemplo 17: As listas de coeficientes de divisibilidade por onze, em todas as aritméticas de base inteira são respectivamente:

1	10^0	1	1	1	1
0	10^1	2	3	4	5
0	10^2	4	9	16	125
	10^3	8	27	64	625
	10^4	16	81	256	3125
	10^5	32	243	1024	15625
	10^6	64	729	4096	
	10^7	128	2187	16384	
⋮	⋮	⋮	⋮	⋮	⋮

1	1	1	1	1
6	7	8	9	10
36	49	64	81	100
216	343	512	729	1000
1296	2401	4096	6561	10000
7776	16807	32768	59049	100000
46656	117649	262144	531441	1000000
⋮	⋮	⋮	⋮	⋮

Fazendo as congruências e tomando os coeficientes mais convenientes obtemos:

	Base										
a_n	**11x**	**11x+1**	**11x+2**	**11x+3**	**11x+4**	**11x+5**	**11x+6**	**11x+7**	**11x+8**	**11x+9**	**11x+10**
a_0	1	1	1	1	1	1	1	1	1	1	**1**
a_1	0	1	2	3	4	5	-5	-4	-3	-2	**-1**
a_2	0	1	4	-2	5	3	3	5	-2	4	**1**
a_3	0	1	-3	5	-2	4	-4	2	-5	3	**-1**
a_4	0	1	5	4	3	-2	-2	3	4	5	**1**
a_5	0	1	-1	1	1	1	-1	-1	-1	1	**-1**
a_6	0	1	-2	3	4	5	5	4	3	-2	**1**
a_7	0	1	-4	-2	5	3	-3	-5	2	4	**-1**
a_8	0	1	3	5	-2	4	4	-2	5	3	**1**
a_9	0	1	-5	4	3	-2	2	-3	-4	5	**-1**
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Como utilizar a tabela?

Queremos saber o critério de divisibilidade por 11 em base 13;

1º) descobrimos o resto da divisão de 13 por 11: 13 = 11.1 + 2, r = 2
2º) a base 13 corresponde ao tipo 11x+2, estando os coeficientes de divisibilidade na 3ª coluna da tabela.

CONCLUSÃO

Ao término deste trabalho, convém salientar que ao propor a realização do mesmo, passou-se por vários obstáculos. O principal foi relativo ao capítulo 3, centro das atenções deste trabalho, que exigiu um processo de discussão com a professora orientadora e um período de amadurecimento do texto escrito.

Notamos que o assunto abordado neste trabalho é pouco utilizado nos colégios, fica quase esquecido. Foi pensando em mudar esse comportamento que decidimos mostrar através deste trabalho, o quanto é interessante o conhecimento de alguns critérios de divisibilidade.

A importância deste trabalho se deve ao fato de podermos mostrar facilmente, através dos restos sucessivos de uma divisão de uma potência da base por um divisor D, de onde vem os critérios de divisibilidade e ao mesmo tempo podermos construir estes critérios na hora que for conveniente e sem cálculos complicados.

Convém ressaltar que há possibilidades de continuidade do trabalho visto que foram observadas as seguintes conclusões, não demonstradas:

- Se D um divisor primo, a lista dos coeficientes de divisibilidade em base B contém no máximo $\frac{D-1}{2}$ coeficientes que se repetem em valor absoluto;

- A tabela geral para os critérios de divisibilidade apresenta uma simetria em relação ao seu eixo vertical, o que facilita a construção de outras tabelas, com outros divisores;

Gostaria de salientar ainda que quanto maior o divisor primo, tanto maior será a quantidade de coeficientes de divisibilidade, o que tornaria o trabalho inviável, mas se predeterminarmos um número com uma quantidade x de algarismos, não haveria necessidade de montarmos uma tabela completa, visto que a quantidade de coeficientes de divisibilidade estariam em função da quantidade de algarismos do número dado.

BIBLIOGRAFIA

BOYER,Carl Benjamin. **História da matemática**. Trad. Elza F. Gomide São Paulo: Edgard Blucher, 1974.

CENTURIÓN, Marília. **Números e operações**. São Paulo: Scipione, 1994.

DANTE, L. R. **RPM** 10, p. 33, 1987.

DOMINGUES, Hygino H. **Fundamentos de aritmética**. São Paulo: Atual, 1991.

FILHO, Edgard. **Teoria elementar dos números**. São Paulo: Nobel, 1985.

FOMIN, S. **Sistemas de numeração**. São Paulo: Atual, 1995.

MELLO, Lydio Machado. **A matemática do universo e a matemática dos homens**. São Paulo: Manuscrito, 1959.

NIVEN, J. **Introdución a la teoria de los números**. Buenos Aires: Limusa, 1976.

TÁBOAS, C. M. G. & Ribeiro, H. S. **RPM** 6, p. 21, 1985.