INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

MESTRADO PROFISSIONAL EM MATEMÁTICA

AUTOR: CARLOS WILSON VIEIRA DA SILVA

A ARITMÉTICA NO ENSINO MÉDIO.

RIO DE JANEIRO

2015

INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

MESTRADO PROFISSIONAL EM MATEMÁTICA

AUTOR: CARLOS WILSON VIEIRA DA SILVA

A ARITMÉTICA NO ENSINO MÉDIO.

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Instituto Nacional de Matemática Pura e Aplicada, como requisito parcial para obtenção do título de Mestre Profissional em Matemática.

Sob a orientação do Prof. Dr. **Carlos Gustavo T. de A. Moreira**
Área de Concentração: Ensino de Matemática na Educação Básica

RIO DE JANEIRO

2015

AUTOR: CARLOS WILSON VIEIRA DA SILVA

A ARITMÉTICA NO ENSINO MÉDIO.

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Instituto Nacional de Matemática Pura e Aplica, como requisito parcial para obtenção do título de Mestre Profissional em Matemática.

Área de Concentração: Ensino de Matemática na Educação Básica

DATA DA DEFESA: 25/02/2015

RESULTADO:_____

BANCA EXAMINADORA:

Prof. Dr. Carlos Gustavo Tamm de Araújo Moreira - IMPA

Prof. Dr. Luiz Amâncio Machado de Sousa Junior - UNIRIO

Prof. Dr. Moacyr Alvim Horta Barbosa da Silva - FGV

“Tudo o que um sonho precisa para ser realizado é alguém que acredite que ele possa ser realizado.”
Roberto Shinyashiki

AGRADECIMENTOS

Ao término deste trabalho, deixo primeiramente meus agradecimentos ao ser de inteligência suprema, causa primeira de todas as coisas, o Grande Arquiteto do Universo, que é Deus, que me proporcionou escolher este caminho me dando saúde e sabedoria para prossegui-lo.

À minha mãezinha em especial que com muito suor, amor, carinho e determinação me conduziram até o seu passamento, sendo exemplo de vida e dedicação aos filhos e familiares.

À minha esposa Joana Ribeiro de Castro que com muita paciência soube suportar a ausência momentânea em várias noites de sono em busca de um propósito maior.

Aos meus filhos Bárbara de Castro Pontes, Carlos Wilson Vieira da Silva Junior e Guilherme Pietro Vieira da Silva que suportaram dias sem a atenção e a dedicação que deveria ter dado a eles e pela compreensão da ausência.

A minha irmã Janaina Vieira da Silva que de uma forma ou de outra contribuiu me incentivando para que eu desse mais esse passo rumo ao meu crescimento individual e espiritual.

Aos meus companheiros de turma, que de uma forma direta ou indiretamente, contribuíram para minha formação, em especial ao amigo Professor Silvio Freitas com quem compartilhei parte deste trabalho.

A todos meus professores, em especial aos de Matemática que tive em minha condução até o término deste trabalho, Prof. Magalhães e Prof. Jorge - Curso Tamandaré, Prof. André - Curso Impacto – Duque de Caxias, Profª Carmem Especotti, Prof. Geraldo Magela, Prof. Amâncio Cezar, Profª Maria Luiza, Prof. João Cataldo, Prof. João Jorge (J.J.) - UERJ, Prof. Augusto C. Morgado (in memoria - PAPMEM), Prof Dr. Elon Lages Lima, Prof. Dr. Paulo Cezar Carvalho, Prof. Eduardo Wagner– PAPMEM e PROFMAT, Prof. Dr. Carlos Gustavo Tamm, Prof Dr. Roberto Imbuzeiro, Prof. Dr. Marcelo Vianna, Prof. Dr. Moacyr Alvim – PROFMAT e Profª Drª. Rúbia – PROFMAT (UFPA), que com muita paciência, transformaram minha visão do saber matemático, contribuindo assim, para um propósito de melhorar a educação dos jovens e adultos do nosso país.

E por fim aos amigos que sempre me incentivaram para que eu seguisse sem desistir, apesar de todas as adversidades do dia a dia.

RESUMO

O objetivo principal deste trabalho é o desenvolvimento de uma sugestão didática que pudesse auxiliar professores e alunos no processo de ensino-aprendizagem de conceitos de Aritmética básica no Ensino Médio. Em continuação e complementação ao trabalho do Prof. Silvio Freitas, serão abordados, de forma aprofundada, os tópicos de Indução, Teorema Fundamental da Aritmética e Congruência Modular. Os assuntos aqui sugeridos são importantes ferramentas da Teoria dos Números e podem ser encontrados em inúmeras aplicações no nosso dia-a-dia, nomeadamente, nos sistemas de identificação utilizados nos números de identificação pessoais, nos códigos de barras e em Criptografia.

Palavras-chaves: Teoria dos Números, Indução Matemática, Aritmética Modular e Teorema Fundamental da Aritmética.

ABSTRACT

The main objective of this work is the development of a teaching suggestion , which could help teachers and students in the teaching- learning process of basic arithmetic concepts in high school . In continuation and complement the work of Prof. Silvio Freitas, will be addressed in depth, topics Induction, Fundamental Theorem of Arithmetic and Congruence Modular. The topics suggested here are important tools of number theory and can be found in numerous applications in our day-to- day, particularly in the identification systems used in personal identification numbers in barcodes and Encryption.

Keywords : Number Theory , Mathematical Induction , Modular Arithmetic and Fundamental Theorem of Arithmetic.

Sumário

1. INTRODUÇÃO

Refletindo sobre o ensino da aritmética durante curso ministrado no Mestrado Profissional em Matemática (IMPA - 2º semestre de 2012), verifiquei que muitos dos assuntos ali apresentados eram de pouco ou nenhum conhecimento de meus alunos do ensino médio e, mesmo os assuntos já vistos no ensino fundamental, estes não estavam bem fundamentados. Surgia ali a semente dessa proposta que mais tarde foi sugerida pelo professor Doutor Carlos Gustavo Tamm Moreira ("Gugu"). Inicialmente foi feita uma pesquisa com professores que trabalham no ensino médio e no fundamental nos Estados do Rio de Janeiro (especificamente a maior parte na Região Metropolitana) e no Pará (cidades de Belém, Anindeua e Castanhal). Os resultados dessa pesquisa, apresentados em anexo a esse trabalho, mostram que a totalidade dos professores foi a favor de que alguns assuntos fossem revistos.

Ao analisar os resultados podemos verificar também que alguns assuntos ficaram em maior evidência. De posse dessas informações e seguindo as sugestões de nosso orientador faremos as propostas de introduzir alguns conteúdos de Aritmética no Ensino Médio. Os assuntos escolhidos foram divididos em dois trabalhos: no primeiro, realizado pelo Professor Sílvio Freitas, são abordados Divisibilidade, MMC e MDC; no segundo, produzido por mim, são tratados Indução Matemática, Teorema Fundamental da Aritmética e Congruências.

Verificamos que os assuntos de Razão e Proporção também foram citados em grande quantidade na pesquisa feita no estado do Rio de Janeiro e que não aconteceu no estado do Pará que apontou como os mais importantes nesta ordem: Indução Matemática, MMC, MDC, Divisibilidade e Congruências. No entanto Razão e Proporção são assuntos que já fazem parte de revisões e já são bem vistos no ensino fundamental.

Sabedores que o processo de criação matemático é em si conflituoso: concreto *versus* abstrato, particular *versus* geral, formal *versus* informal. Tais conflitos também estão presentes no processo de ensino-aprendizagem desta disciplina. Nesse sentido é fundamental que o ensino de Matemática desempenhe seu papel no desenvolvimento da formação de capacidades intelectuais, na criação e agilidade do raciocínio dedutivo e sua aplicação na resolução de problemas. Sob este ponto de vista, os PCNs, dizem que:

> "... é fundamental não subestimar a capacidade dos alunos, reconhecendo que resolvem problemas, mesmo que razoavelmente complexos, lançando mão de seus conhecimentos sobre o assunto e buscando estabelecer relações entre o já conhecido e o novo. (BRASIL , 1997, p.29)"

Para isso é fundamental que o professor compreenda um problema matemático em seus diversos aspectos, concebendo-o como uma situação que exige a realização de uma sequência de ações ou operações com o objetivo de chegar a um resultado. Desta forma, o professor deve ter a consciência de que a solução desse problema não está disponível no início, mas é possível construí-la.

O tema central deste trabalho é uma proposta do ensino de Indução Matemática, do conceito do Teorema Fundamental da Aritmética e Congruência para o Ensino Médio, de forma construtiva e intuitiva. Nesse aspecto, ao longo do trabalho busca-se justificar a importância da presença dos tópicos acima mencionados no ensino de Matemática, deixando claro que estes fiquem como assuntos complementares para o currículo de Matemática e postos em momentos adequados. Lins lança uma crítica muito forte sobre o ensino de Aritmética, a qual é uma justificativa pertinente a este trabalho acadêmico por ser, de fato, o problema aqui abordado.

> "O desenvolvimento habitual do ensino-aprendizagem da Aritmética nas salas de aula deixa de lado muitos pontos importantes." (LINS , 1997, p.34)

Assim que encontramos o tema deste trabalho e o problema abordado (o ensino de Aritmética no Ensino Básico deixam de lado muitos pontos importantes), era necessário estabelecer a metodologia usada para o desenvolvimento. O primeiro foi uma pesquisa bibliográfica sobre os tópicos aritméticos abordados (Divisão Euclidiana, Algoritmo de Euclides, congruência módulo n e equações diofantinas lineares). Uma segunda etapa do trabalho foi uma analise de textos didáticos que abordam assuntos como: divisão nos naturais, máximo divisor comum para, desta forma, compreender quais pontos iniciais são necessários para o aprofundamento em sala de aula. Em seguida, fizemos uma pesquisa em trabalhos acadêmicos que abordam a mesma temática: o ensino da Aritmética dos restos e congruência. O que percebemos foi que propostas de ensino sobre as equações diofantinas eram vastas. E por fim propomos a elaboração de sequências didáticas, visando ser esse o produto final do trabalho dissertativo. Não são abordados, visando o entendimento mais

aprimorado, os conteúdos de: indução matemática, congruências e teorema fundamental da aritmética. Esses capítulos são o produto deste trabalho dissertativo, que visa uma orientação para o professor que deseja ensinar algum desses tópicos de Aritmética. Também são apresentadas aplicações de congruência na Trigonometria, nos Números Complexos e com Polinômios, mostrando assim que a congruência pode ser um bom recurso de apoio para o desenvolvimento de conteúdos tradicionalmente vistos no Ensino Básico, satisfazendo assim um objetivo presente nos PCNs: "estabelecer conexões entre temas matemáticos de diferentes campos." (BRASIL , 1997,p.37).

Apresentamos algumas situações-problema, em sua maioria da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), especificamente para desenvolver um significado mais elaborado do resto de uma divisão euclidiana, já que os PCNs trazem a seguinte orientação.

> resolver situações-problema envolvendo números naturais, inteiros, racionais e a partir delas ampliar e construir novos significados da adição, subtração, multiplicação, divisão, potenciação e radiciação(BRASIL , 1998,p.64)

2. ARITIMÉTICA E O ENSINO BÁSICO

2.1 - UM POUCO DE HISTÓRIA

Desde a antiguidade, os gregos se dedicavam à Matemática e, dada a atitude filosófica e especulativa que os mesmos tinham face à vida, deram a esta ciência um caráter científico.

Pitágoras de Samos (580 - 500 a.C) e a sua escola, chamada escola Pitagórica, difundiram a Matemática pela Grécia e suas colônias. Os mesmos atribuíram aos números um poder místico, adotando a *Aritmética* como fundamento de seu sistema filosófico. O filosofo Platão (429 - 348 a.C), apesar de não ser matemático, tinha preferência pelos aspectos mais teóricos e conceituais, e fazia uma clara diferenciação entre a ciência dos números, que ele chamava *Aritmética*, e a arte de calcular, que ele chamava *Logística*, a qual desprezava por ser "infantil e vulgar".

Tratada de maneira tão significativa pelos Gregos, a Matemática, em especial a *Aritmética*, ganha ainda mais notoriedade, com o surgimento de um importante tratado "Os Elementos de Euclides". Foi Euclides que estabeleceu um padrão de apresentação e rigor na Matemática, que passou a ser seguido nos milênios que se sucederam. A obra de Euclides é composta por treze livros, sendo que três desses, os Livros VII, VIII e IX, eram dedicados à *Aritmética*. Neles, encontram-se temas relacionados a: Divisibilidade, Divisão com Resto, Máximo Divisor Comum, Números Primos, Progressões Geométricas, dentre outros.

Após Euclides, a *Aritmética* passou por um longo período de estagnação (cerca de 500 anos) até ressurgir com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 d.C. Diofanto escreveu uma obra em treze volumes, chamada **Aritmética**.

Entre os séculos XVI e XVII, vários matemáticos se dedicaram à *Aritmética*, destacando-se Pierre de Fermat e Leonhard Euler, que foram fundamentais no desenvolvimento da Teoria dos Números.

Entre os séculos XVIII e XIX, surge um dos maiores matemáticos de todos os tempos, o Alemão Carl Frederich Gauss (1777 - 1855), que de forma precoce, aos 17 anos de idade, decidiu incursionar na Aritmética, com o propósito de esclarecer, completar e desenvolver o que os seus predecessores haviam realizado. Aos 21 anos, Gauss produz uma das obras primas de toda a matemática, o livro *Disquisitiones Arithmeticae*, trazendo

a noção de congruência modular e aritmética dos restos, sendo de grande aplicação no cotidiano - como exemplo, podemos citar os sistemas de criptografa e segurança de dados.

Diante de notória importância da *Aritmética* ao longo da história e, observando a carência dos alunos do ensino básico bem como a dos livros didáticos nessa importante área do conhecimento, o presente trabalho tem como objetivo, de forma gradativa e numa linguagem acessível ao aluno, revisar os vários tópicos relacionados à teoria dos números, a fim de construir os conceitos de indução, números primos, teorema fundamental da aritmética, congruência modular e as aplicações.

2.2 - O ENSINO E APRENDIZAGEM DE ARITMÉTICA

Conforme consta na apresentação nos Parâmetros Curriculares Nacionais para matemática no Ensino Fundamental verificamos que:

"O ensino de Matemática costuma provocar duas sensações contraditórias, tanto por parte de quem ensina como por parte de quem aprende: de um lado, a constatação de que se trata de uma área de conhecimento importante; de outro, a insatisfação diante dos resultados negativos obtidos, com muita frequência, em relação à sua aprendizagem.

A constatação da sua importância se apoia no fato de que a Matemática desempenha papel decisivo, pois permite resolver problemas da vida cotidiana, tem muitas aplicações no mundo do trabalho e funciona como instrumento essencial para a construção de conhecimentos em outras áreas curriculares. Do mesmo modo, interfere fortemente na formação de capacidades intelectuais, na estruturação do pensamento e na agilização do raciocínio dedutivo do aluno.

A insatisfação revela que há problemas a serem enfrentados, tais como a necessidade de reverter um ensino centrado em procedimentos mecânicos, desprovidos de significados para o aluno. Há urgência em reformular objetivos, rever conteúdos e buscar metodologias compatíveis com a formação que hoje a sociedade reclama.

No entanto, cada professor sabe que enfrentar esses desafios não é tarefa simples, nem para ser feita solitariamente. O documento de Matemática é um instrumento que pretende estimular a busca coletiva de soluções para o ensino dessa área. Soluções

que precisam transformar-se em ações cotidianas que efetivamente tornem os conhecimentos matemáticos acessíveis a todos os alunos.

Os Parâmetros Curriculares Nacionais para a área de Matemática no ensino fundamental estão pautados por princípios decorrentes de estudos, pesquisas, práticas e debates desenvolvidos nos últimos anos. São eles:

- A Matemática é componente importante na construção da cidadania, na medida em que a sociedade se utiliza, cada vez mais, de conhecimentos científicos e recursos tecnológicos, dos quais os cidadãos devem se apropriar.

- A Matemática precisa estar ao alcance de todos e a democratização do seu ensino deve ser meta prioritária do trabalho docente.

- A atividade matemática escolar não é "olhar para coisas prontas e definitivas", mas a construção e a apropriação de um conhecimento pelo aluno, que se servirá dele para compreender e transformar sua realidade.

- No ensino da Matemática, destacam-se dois aspectos básicos: um consiste relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo, a comunicação tem grande importância e deve ser estimulada, levando-se o aluno a "falar" e a "escrever" sobre Matemática, a trabalhar com representações gráficas, desenhos, construções, a aprender como organizar e tratar dados.

- A aprendizagem em Matemática está ligada à compreensão, isto é, à apreensão do significado; apreender o significado de um objeto ou acontecimento pressupõe vê-lo em suas relações com outros objetos e acontecimentos. Assim, o tratamento dos conteúdos em compartimentos estanques e numa rígida sucessão linear deve dar lugar a uma abordagem em que as conexões sejam favorecidas e destacadas. O significado da Matemática para o aluno resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele estabelece entre os diferentes temas matemáticos.

- A seleção e organização de conteúdos não deve ter como critério único a lógica interna da Matemática. Deve-se levar em conta sua relevância social e a contribuição para o desenvolvimento intelectual do aluno. Trata-se de um processo permanente de construção.

- O conhecimento matemático deve ser apresentado aos alunos como historicamente construído e em permanente evolução. O contexto histórico possibilita ver a Matemática em sua prática filosófica, científica e social e contribui para a compreensão do lugar que ela tem no mundo.

- Recursos didáticos como jogos, livros, vídeos, calculadoras, computadores e outros materiais têm um papel importante no processo de ensino e aprendizagem. Contudo, eles precisam estar integrados a situações que levem ao exercício da análise e da reflexão, em última instância, a base da atividade matemática.

- A avaliação é parte do processo de ensino e aprendizagem. Ela incide sobre uma grande variedade de aspectos relativos ao desempenho dos alunos, como aquisição de conceitos, domínio de procedimentos e desenvolvimento de atitudes. Mas também devem ser avaliados aspectos como seleção e dimensionamento dos conteúdos, práticas pedagógicas, condições em que se processa o trabalho escolar e as próprias formas de avaliação. (BRASIL, 1997, p.15 - 19).

A aritmética é uma ciência de todos os tempos, provêm do vocábulo ARITHMOS, que significa número (GROENWALD et tal, 2006). Os números naturais foram se formando pouco a pouco pela prática diária de contagens (ROSA et al, 2007). Isto é, o homem primitivo conhecia de forma intuitiva uma série de conceitos que aplicava em sua vida prática, e desta forma chegou a formalizar a representação de quantidades.

Na escolarização básica a aritmética é desenvolvida desde os primeiros anos, o trabalho com números e operações juntamente com o ensino do espaço e das formas, integram os primeiros conteúdos vistos pela criança. Além disso, é preciso lembrar que quando esta chega à escola já existe nela certa noção de número, construída a partir de atitudes naturais de agrupamento e seriação. Mas, o que é a aritmética e o que o seu ensino deve proporcionar aos alunos?

Parece fácil responder a essa pergunta, pois se pode dizer, sem medo de errar, que aritmética são os números e suas operações: somar, subtrair, multiplicar, dividir e

outras. Mas, segundo Lins e Gimenez (1996), a educação aritmética é muito mais que isso, ela inclui também representações e significações diversas, pontos de referencias e núcleos, que ampliam a ideia simples do manipulativo (técnicas e algoritmos). Eles são importantes, mas precisam ser revestidos de significados que justifiquem o seu uso e torne esse uso adequado e racional.

Dessa maneira o ensino da aritmética deve proporcionar aos alunos o desenvolvimento de um sentido numérico através de um processo extenso em que se trabalhe o raciocínio figurativo e intuitivo (conservação de quantidades), pensamento relativo e absoluto (percepção de quantidade), raciocínio estruturado aditivo (mudança de estado, combinação) e pensamento proporcional (comparação em forma multiplicativa), de forma que todo esse trabalho dê ao aluno condições de produzir afirmações aritméticas com significados, sendo capazes de construir justificações.

3. INDUÇÃO MATEMÁTICA

3.1 INTRODUÇÃO

- O que é Indução?

Dizemos que a ***indução*** é um processo de raciocínio, que faz a passagem de conhecimentos particulares (ou hipóteses) para conclusões gerais.

As ciências naturais se utilizam daquilo que denominamos *indução empírica*. Este tipo de indução se utiliza para formular leis que devem reger determinados fenômenos a partir de um grande número de observações particulares, selecionadas adequadamente. Este tipo de procedimento, embora não seja logicamente correto, é frequentemente satisfatório: por exemplo, ninguém duvidaria de que quando um corpo é liberado ao seu próprio peso, no vácuo, na superfície da Terra, ele cai segundo a vertical local.

Nas ciências naturais, em geral, um raciocínio desse tipo é plenamente aceito, como no seguinte exemplo, *"Todo homem é mortal"*, esta afirmação se verifica como certa, dado o número enorme de confirmações através do tempo desde o inicio da humanidade até os dias de hoje.

No entanto tal raciocínio não se aplica as afirmações e teoremas demonstrados através de raciocínio puramente matemáticos.

Pode-se dizer, então, que na matemática a indução não se aplica como raciocínio válido, pois está ciência não se satisfaz com os "graus de confiança" obtidos na indução empírica.

Podemos "definir" a indução matemática da seguinte forma:

Indução matemática é um método de prova matemática usado para demonstrar a verdade de um número infinito de proposições.

A forma mais simples e mais comum de indução matemática prova que um enunciado vale para todos os números naturais n e consiste de dois passos:

1º) **A base**: mostrar que o enunciado vale para $n = 1$

2º) **O passo indutivo**: mostrar que, se o enunciado vale para $n = k$, então o mesmo enunciado vale para $n = k + 1$.

Esse método funciona provando que o enunciado é verdadeiro para um valor inicial, e então provando que o processo usado para ir de um valor para o próximo. Se ambas as coisas são provadas, então qualquer valor pode ser obtido através da repetição desse processo. Para entender por que os dois passos são suficientes, é útil pensar no efeito dominó: se você tem uma longa fila de dominós em pé e você puder assegurar que:

1. O primeiro dominó cairá.
2. Sempre que um dominó cair, seu próximo vizinho também cairá.

Então se pode concluir que *todos* os dominós cairão.

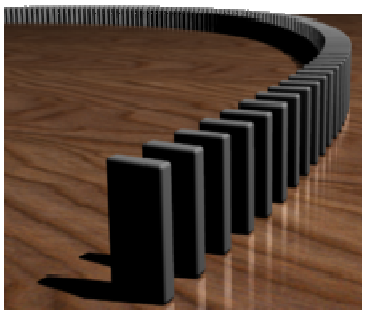


figura 1

O Princípio da Indução é um eficiente instrumento para a demonstração de fatos referentes aos números naturais. Por isso deve-se adquirir prática em sua utilização. Por outro lado, é importante também conhecer seu significado e sua posição dentro do arcabouço da Matemática. Entender o Princípio da Indução é praticamente o mesmo que entender os números naturais.

Apresentamos abaixo uma breve exposição sobre os números naturais, onde o Princípio da Indução se insere adequadamente e mostra sua força teórica antes de ser utilizado na lista de exercícios propostos ao final.

3.2 A SEQUÊNCIA DOS NÚMEROS NATURAIS

Os números naturais constituem um modelo matemático, uma escala padrão, que nos permite a operação de contagem. A sequência desses números é uma livre e antiga criação do espírito humano. Comparar conjuntos de objetos com essa escala abstrata ideais é o processo que torna mais precisa a noção de quantidade; esse processo (a contagem) pressupõe, portanto o conhecimento da sequência numérica. Sabemos que os números naturais são 1, 2, 3, 4, 5,…. A totalidade desses números constitui um conjunto, que indicaremos com o símbolo N e que chamaremos de conjunto dos naturais. Portanto N = {1, 2, 3, 4, 5,…}.

Evidentemente, o que acabamos de dizer só faz sentido quando já se sabe o que é um número natural. Façamos de conta que esse conceito nos é desconhecido e procuremos investigar o que há de essencial na sequência 1, 2, 3, 4, 5… .

Deve-se a ***Giussepe Peano*** *(1858-1932)* a constatação de que se pode elaborar a teoria dos números naturais a partir de quatro fatos básicos, conhecidos atualmente como os *axiomas de Peano*. Em outras palavras, o conjunto N dos números naturais possui quatro propriedades fundamentais, das quais resultam como consequências lógicas.

3.3 AXIOMAS DE PEANO

O conjunto dos números naturais é caracterizado pelas seguintes propriedades:

1) Todo número natural possui um único sucessor, que também é um número natural.

2) Números naturais diferentes possuem sucessores diferentes.

3) Existe um único número natural que não é sucessor de nenhum outro. Este número é chamado de número um e é representado pelo símbolo 1.

4) Se um conjunto de números naturais contém o número 1, e, além disso, contém o sucessor de cada um dos seus elementos, então esse conjunto coincide com N.

Em linguagem matemática escrevemos:

1) Existe uma função s : N $\rightarrow$ N, que associa a cada n $\in$ N um elemento s(n) $\subset$ N, chamado de sucessor de n.

2) A função s: N $\rightarrow$ N é injetiva.

3) Existe um único elemento 1 no conjunto N, tal que 1 $\neq s$(n) para todo n $\in$ N.

4) Se um subconjunto X $\subset$ N é tal que 1 $\in$ N e s(X) $\subset$ X, então X = N.

O sucessor de 1 chama-se dois (2), isto é, s(1) = 2; o sucessor de 2 chama-se três e assim sucessivamente. Indicaremos s(n) por n + 1.

O quarto axioma é chamado de axioma de indução e do ponto de vista estritamente matemático pode ser reformulado por: Um subconjunto de X de N chama-se indutivo quando s(X) $\subset$ X, isto é, quando o sucessor de qualquer elemento de X também pertence a X. Com essa definição, o axioma de indução afirma que o único subconjunto indutivo de N que contém o número 1 é o próprio N.

O axioma de indução tem um papel de fundamental não só na teoria dos números naturais como em toda matemática, pois pode ser visto como um método de demonstração, chamado de Princípio de Indução Matemática ou Princípio de Indução Finita.

A partir daí, retomamos a palavra para dizer que o sucessor de 1 chama-se "dois", o sucessor de dois chama-se "três", etc. Nossa civilização progrediu ao ponto em que temos um sistema de numeração, o qual nos permite representar, mediante o uso apropriado dos símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9, todos os números naturais. Além disso, nossa linguagem também fornece nomes para os primeiros termos da seqüência dos números naturais. (Números muito grandes não têm nomes específicos, ao contrário dos menores como "mil novecentos e noventa e oito". Quem sabe, por exemplo, o nome do número de átomos do universo?)

Voltando a usar a notação $s(n)$ para o sucessor do número natural n, teremos então 2 = s(1), 3 = s(2), 4 = s(3), 5 = s(4), etc. Assim, por exemplo, a igualdade 2 = s(1) significa apenas que estamos usando o símbolo 2 para representar o sucessor de 1. A seqüência dos números naturais pode ser indicada assim:

$$1 \xrightarrow{s} 2 \xrightarrow{s} 3 \xrightarrow{s} 4 \xrightarrow{s} 5 \xrightarrow{s} \cdots$$

As flechas ligam cada número ao seu sucessor.

Nenhuma flecha aponta para 1, pois este número não é sucessor de nenhum outro. O diagrama acima diz muito sobre a estrutura do conjunto N dos números naturais.

3.4 PRINCÍPIO DE INDUÇÃO MATEMÁTICA

Dado um subconjunto S do conjunto dos números naturais N, tal que 1 pertence a S e sempre que um número n pertence a S, o número n + 1 também pertence a S, tem-se que S = N.

Esta simples propriedade fornece uma das mais poderosas técnicas de demonstração em Matemática: a demonstração por indução.

Suponha que seja dada uma sentença matemática P(n) que dependa de uma variável natural n, a qual se torna verdadeira ou falsa quando substituímos n por um número natural dado qualquer. Tais sentenças serão ditas sentenças abertas definidas sobre o conjunto dos naturais.

A seguir damos alguns exemplos de sentenças abertas definidas sobre N:

(a) P(n) : n é par.

É claro que a afirmação P(1) é falsa, pois ela diz que 1 é par;

P(3), P(5) e P(9) são falsas, pois afirmam, respectivamente, que 3, 5 e 9 são pares.

Por outro lado, é também claro que P(2), P(4), P(8) e P(22) são verdadeiras, pois 2, 4, 8 e 22 são pares.

(b) P(n): n é múltiplo de 3.

Temos, por exemplo, que P(1), P(2), P(4) e P(5) são falsas, enquanto P(3) e P(6) são verdadeiras.

(c) P(n) : $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$.

Temos que P(1), P(2), P(3), P(4), ..., P(10) são verdadeiras.

Aqui sabemos precisamente o que significa a sentença aberta P(n), apesar dos pontinhos na sua definição. Ela significa:

"A soma dos n primeiros números ímpares é igual a n^2."

Você consegue visualizar algum número natural m tal que P(m) seja falsa? Bem, após mais algumas tentativas, você se convencerá de que esta fórmula tem grandes chances de ser verdadeira para todo número natural n; ou seja, P(n) é verdadeira para todo $n \in N$.

(d) Prove por Indução que:

$$P(n) = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... + \frac{1}{2^n} = 2 - \frac{1}{2^n}$$

Verificando a primeira propriedade, temos:

$$P(1) = 2 - \frac{1}{2^1} = 2 - \frac{1}{2} = 1, \text{ verdadeira.}$$

Suponhamos que *P(k)* seja verdadeira:

$$P(k) = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... + \frac{1}{2^k} = 2 - \frac{1}{2^k}$$

Tentaremos provar que a seqüência é verdadeira para *P(k + 1)*.

$$P(k+1) = 1 + \underbrace{\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... + \frac{1}{2^n}}_{P(k)} + \frac{1}{2^{k+1}} = 2 - \frac{1}{2^{k+1}}$$

$$\overbrace{2 - \frac{1}{2^k}}^{} + \frac{1}{2^{k+1}} = \frac{2(2^{K+1}) - 2 + 1}{2^{K+1}} \therefore$$

$$\frac{2^{K+2} - 1}{2^{K+1}} = \frac{2^{K+2}}{2^{K+1}} - \frac{1}{2^{K+1}} = 2 - \frac{1}{2^{k+1}}$$

P(k+1) é verdadeira, logo *P(n)* é verdadeira $\forall n \in N$.

(e) Prove por Indução que:

$$S(n) = 2 + 2^2 + 2^3 + 2^4 + ... + 2^n = 2^{n+1} - 2$$

Verificando a primeira propriedade, temos:

$$S(1) = 2 = 2^{1+1} - 2 = 2^2 - 2 = 4 - 2 = 2, \text{ verdadeira.}$$

Suponhamos que *S(k)* seja verdadeira:

$$S(k) = 2 + 2^2 + 2^3 + 2^4 + ... + 2^k = 2^{k+1} - 2$$

Tentaremos provar que a seqüência é verdadeira para *S(k + 1)*.

$$S(k+1) = \underbrace{2+2^2+2^3+2^4+...+2^k}_{S(k)} + 2^{k+1} = 2^{(k+1)+1} - 2$$

$$S(k+1) = 2^{k+1} - 2 + 2^{k+1} = 2.2^{k+1} - 2 = 2^{(k+1)+1} - 2$$

S(k+1) é verdadeira, logo *S(n)* é verdadeira $\forall n \in N$.

(f) Prove que $10^n - 1$ é divisível por 9.

De fato para n = 1 temos:

$10^1 - 1 = 10 - 1 = 9$, verdadeiro.

Supondo como verdadeiro que $9 \mid 10^k - 1$

Verificaremos que $10^{k+1} - 1 = 9.a$

Como estamos supondo $10^k - 1 = 9a$ x (10) $\Rightarrow 10.\ 10^k - 10 = 90.a$

$\Rightarrow 10^{k+1} - 1 - 9 = 90.a \Rightarrow 10^{k+1} - 1 = 90.a + 9 \Rightarrow 10^{k+1} - 1 = 9.(10.a + 1)$.

Como $9 \mid 10^{k+1} - 1$ temos que $9 \mid 10^n - 1$ é verdadeira $\forall n \in N$.

3.5 APLICAÇÕES

Dentro dos muitos problemas que podem ser aplicado o método da indução podemos relacionar os três mais importantes:

- demonstração de identidades;
- demonstração de problemas de divisibilidade;
- demonstração de desigualdades.

Os dois primeiros já exemplificados acima, vamos ver agora um exemplo de desigualdades.

(g) prove que $3^{n-1} < 2^{n^2}$ para todo $n \in N$.

Verificamos para n = 1.

$3^{1-1} < 2^{1^2} \Rightarrow 3^0 < 2^1 \Rightarrow 1 < 2$ (verdade)

Supondo verdadeiro $3^{k-1} < 2^{k^2}$

Vamos verificar se $3^{(k+1)-1} < 2^{(k+1)^2}$

$3^{(k+1)-1} < 2^{(k+1)^2} \Rightarrow 3^{k-1} . 3 < 2^{k^2+2k+1} = 2^{k^2}.2^{2k+1}$ também é verdadeiro uma vez que $3 < 2^{2k+1} \ \forall k \in N$.

3.6 INDUÇÃO NA GEOMETRIA

Prove que um polígono convexo de *n* lados possui $D = \frac{n.(n-3)}{2}$ diagonais.

$$\frac{n.(n-3)}{2}$$

Demonstração

i) Se *n* = 3, o polígono é um triângulo e possui $\frac{3.(3-3)}{2} = 0$ diagonais, ou seja, não possui diagonais;

ii) Suponhamos que, para algum *n*, seja verdade que o número de diagonais de um polígono convexo de lados seja $D = \frac{n.(n-3)}{2}$;

iii) Considere um polígono de $n + 1$ lados, com vértices V_1, V_2 , V_3 , ...,V_n , V_{n+1}. Se unirmos V_1 a V_n teremos um polígono de *n* lados que, por hipótese, possui $\frac{n.(n-3)}{2}$ diagonais.

Vejamos a figura abaixo.

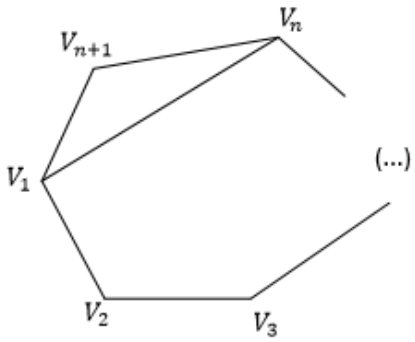


Figura 2

Temos que o número de diagonais de $n + 1$ lados será:

• Número de diagonais do polígono de *n* lados (hipótese de indução): $\frac{n.(n-3)}{2}$

• O lado V_1V_n do polígono de n lados passa a ser uma diagonal para o polígono de $n + 1$ lados: soma 1

• o número de diagonais saindo de V_{n+1} será: (n + 1) – 3

$$D = \frac{n.(n-3)}{2} + 1 + (n+1) - 3 = \frac{n^2 - 3n + 2 + 2(n+1) - 6}{2} \Rightarrow$$

$$\Rightarrow D = \frac{n^2 - n - 2}{2} = \frac{(n+1)(n-2)}{2} = \frac{(n+1)[(n+1)-3]}{2}$$

O que prova, via indução, a proposição.

3.7 PRINCÍPIO DA INDUÇÃO GENERALIZADO

Seja P uma propriedade referente a números naturais, cumprindo as seguintes condições:

1) O número natural *k* goza da propriedade P;

2) Se um número natural $n \geq k$ goza da propriedade P então seu sucessor $n + 1$ também goza de P.

Então todos os números naturais maiores do que ou iguais a *k* gozam da propriedade P.

3.8 EXERCÍCIOS RESOLVIDOS

3.8.1 Prove que a soma dos n primeiros números inteiros e positivos é igual a

$$S(n) = \frac{n.(n+1)}{2}$$

Solução: $1 + 2 + 3 + 4 + . \cdots + n = \frac{n.(n+1)}{2}$

(1) Para $n = 1$ temos: $1 = \frac{1.(1+1)}{2} = \frac{1.2}{2} = 1$

(2) Hipótese: $1 + 2 + 3 + 4 + . \cdots + n = \frac{n.(n+1)}{2}$

(3) Tese: $1 + 2 + 3 + 4 + . \cdots + n + (n+1) = \frac{(n+1).[(n+1)+1]}{2} = \frac{(n+1).(n+2)}{2}$

Somando aos dois membros da hipótese o número $n + 1$, obtemos:

$$1+2+3+4+.\cdots+n+(n+1)=\frac{n.(n+1)}{2}+(n+1)$$

$$1+2+3+4+.\cdots+n+(n+1)=\frac{n.(n+1)+2(n+1)}{2}=\frac{(n+1).(n+2)}{2}$$

3.8.2 Prove que a soma dos n primeiros números impares positivos é igual n^2 como citado na letra (c) dos exemplos de **3.4**.

Solução: $1+2+3+4+.\cdots+(2n-1)=n^2$

(1) Para $n = 1$ temos: $1=1^2=1$

(2) Hipótese: $1+2+3+4+.\cdots+(2n-1)=n^2$

Tese: $1+2+3+4+.\cdots+(2n-1)+[2(n+1)-1]=(n+1)^2$

Somando aos dois membros da hipótese o número $[2(n + 1) – 1]$, obtemos:

$$1+2+3+4+.\cdots+(2n-1)+[2(n+1)-1]=n^2+[2(n+1)-1]$$

$$1+2+3+4+.\cdots+(2n-1)+[2(n+1)-1]=n^2+2n+2-1$$

$$1+2+3+4+.\cdots+(2n-1)+[2(n+1)-1]=n^2+2n+1$$

$$1+2+3+4+.\cdots+(2n-1)+[2(n+1)-1]=(n+1)^2$$

3.8.3 Demonstre que $\forall n\in$ N, o número $3^{2n+1}+2^{n+2}$ é divisível por 7.

Solução: $3^{2n+1}+2^{n+2}=7.k$

(1) Para $n = 1$ temos: $3^{2.1+1}+2^{1+2}=3^3+2^3=27+8=35=7.5$

(2) Hipótese: $3^{2n+1}+2^{n+2}=7.q$ Tese: $3^{2n+3}+2^{n+3}=7.k$

Temos: $3^{2n+3}+2^{n+3}=3^{2(n+1)+1}+2^{(n+2)+1}=3^{2n+1}.3^2+2^{n+2}.2=3^{2n+1}.9+2^{n+2}.2$

Como 9 = 7 + 2, segue-se:

$$3^{2n+1}.(7+2)+2^{n+2}.2=3^{2n+1}.7+3^{2n+1}.2+2^{n+2}.2=3^{2n+1}.7+\underbrace{(3^{2n+1}+2^{n+2}).2}_{\text{divisível por 7 por hipótese.}}$$

Como as duas parcelas são divisíveis por 7, logo a proposição é válida $\forall n\in$ N.

3.8.4 Verifique se $\forall n \in$ N, a validade da desigualdade:

$$2n+1<2^n$$

Solução: $2n+1<2^n$

Examinando temos: $n=1 \Rightarrow 2.1+1<2^1$, $3<2$ (falso)

$n=2 \Rightarrow 2.2+1<2^2$, $5<4$ (falso)

$n=3 \Rightarrow 2.3+1<2^3$, $7<8$ (verdade)

$n=4 \Rightarrow 2.4+1<2^4$, $9<16$ (verdade)

Há um forte indicio de que a desigualdade é válida para $n \geq 3$. Vamos verificar.

(1) Para $n = 3$, já verificado.

(2) Hipótese: Considerando $2n+1<2^n$ válido vejamos:

Tese: $2(n+1)+1<2^{n+1}$ ou $2n+3<2^{n+1}$

Multiplicando por 2 a sentença $2n+1<2^n$, teremos:

$$(2n+1).2<2^n.2 \Rightarrow 4n+2<2^{n+1} \Rightarrow 2n+2n+3-1<2^{n+1} \Rightarrow (2n+3)+(2n-1)<2^{n+1}$$

Como $0 < 2n - 1$ implica que $2n+3<4n+2<2^{n+1}$, portanto.

$$2n+3<2^{n+1}$$

3.9 EXERCÍCIOS PROPOSTOS

Demonstre nos exercícios de **3.9.1** a **3.9.10**, por "indução matemática", que as proposições abaixo são validas $\forall n \in$ N:

3.9.1 $1^2+2^2+3^2+4^2+.\cdots+n^2=\dfrac{n.(n+1).(2n+1)}{6}$

3.9.2 $2+4+6+.\cdots+2n=n.(n+1)$

3.9.3 $\dfrac{1}{1.2}+\dfrac{1}{2.3}+\dfrac{1}{3.4}+\cdots+\dfrac{1}{n.(n+1)}=\dfrac{n}{n+1}$

3.9.4 $\dfrac{1}{2}+\dfrac{2}{2^2}+\dfrac{3}{2^3}+\cdots+\dfrac{n}{2^n}=2-\dfrac{n+2}{2^n}$

3.9.5 $1^3 + 2^3 + 3^3 + 4^3 + .\cdots + n^3 = \frac{n^2.(n+1)^2}{4}$

3.9.6 Demonstre que $\forall n \in$ N, o número $n^3 + 5n$ é divisível por 6.

3.9.7 Mostre que $5^n - 1$ é múltiplo de 24 para todo número natural n par.

3.9.8 Demonstre que $\forall n \in$ N, o número $5^n + 2.11^n$ é divisível por 3.

3.9.9 Prove por indução matemática que $n^2 < 2^n$, para todos inteiros n $\geq$ 5.

3.9.10 Prove a seguinte frase usando indução matemática:
- *Qualquer número inteiro positivo n≥8 pode ser escrito como a soma de 3's e 5's.*

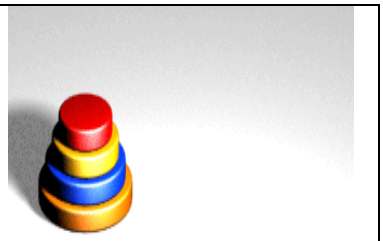
3.10 APLICAÇÕES INTERESSANTES DA INDUÇÃO MATEMÁTICA

3.10.1 TORRE DE HANÓI

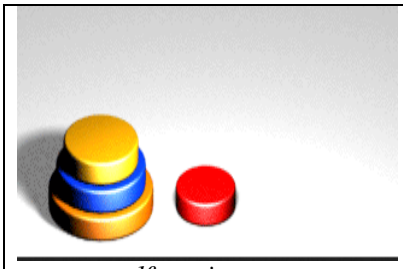
Torre de Hanói é um "quebra-cabeça" que consiste em uma base contendo três pinos, em um dos quais são dispostos alguns discos uns sobre os outros, em ordem crescente de diâmetro, de cima para baixo. O problema consiste em passar todos os discos de um pino para outro qualquer, usando um dos pinos como auxiliar, de maneira que um disco maior nunca fique em cima de outro menor em nenhuma situação. O número de discos pode variar sendo que o mais simples contém apenas três.

A Torre de Hanói tem sido tradicionalmente considerada como um procedimento para avaliação da capacidade de memória de trabalho, e principalmente de planejamento e solução de problemas.

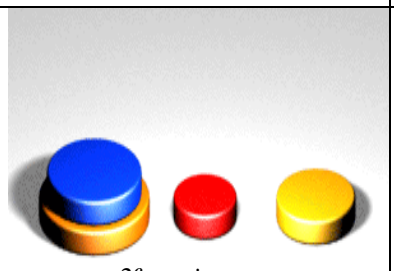
Vejamos os movimentos para uma Torre de Hanói com quatro discos.



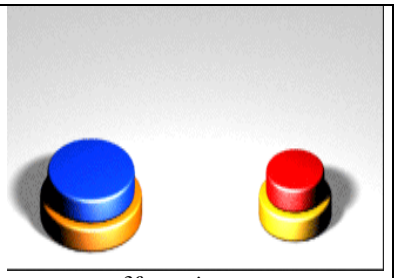
Inicio



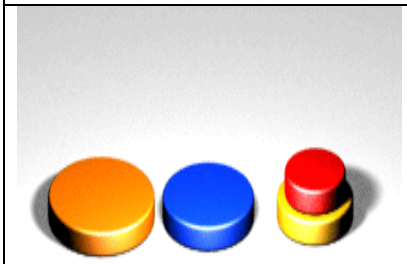
1º movimento



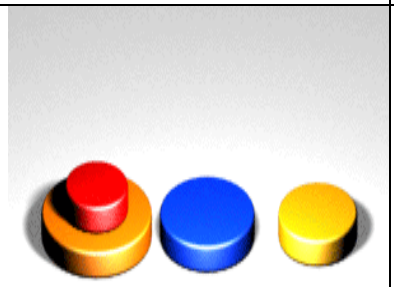
2º movimento



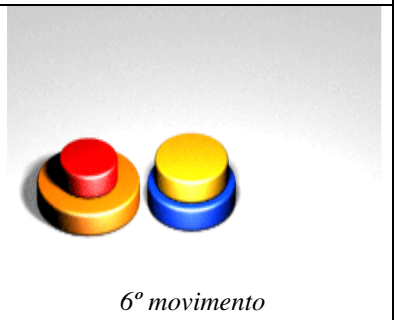
3º movimento



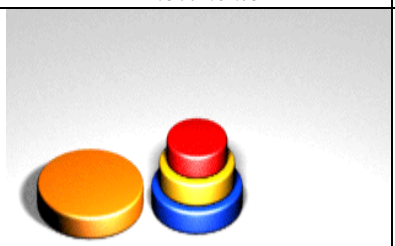
4º movimento



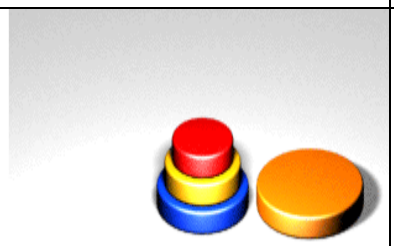
5º movimento



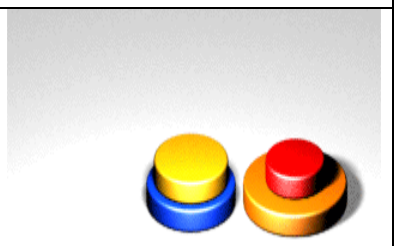
6º movimento



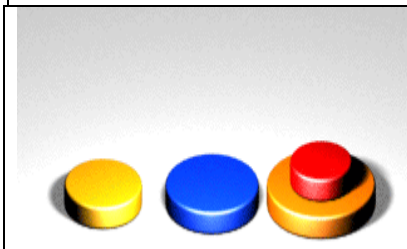
7º movimento



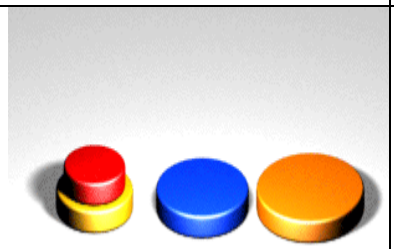
8º movimento



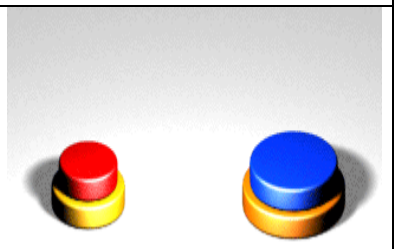
9º movimento



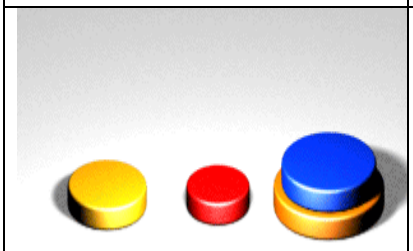
10º movimento



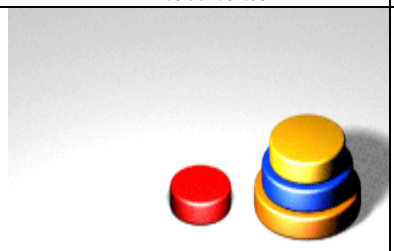
11º movimento



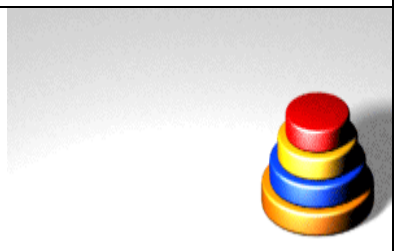
12º movimento



13º movimento



14º movimento



15º movimento

As perguntas naturais que surgem são as seguintes:

1. O jogo tem solução para cada $n \in N$?

2. Em caso afirmativo, qual é o número mínimo de j_n de movimentos para resolver o problema com n discos?

Usando Indução Matemática, vamos ver que a resposta à primeira pergunta é afirmativa, qualquer que seja o valor de n. Em seguida, deduziremos uma fórmula que nos fornecerá o número j_n. Considere a sentença aberta

P(n): O jogo com n discos tem solução.

Obviamente, P(1) é verdade. Suponha que P(n) seja verdadeiro, para algum n; ou seja, que o jogo com n discos tem solução. Vamos provar que o jogo com $n + 1$ discos tem solução. Para ver isso, resolva inicialmente o problema para os n discos superiores da pilha, transferindo-os para uma das hastes livre (isso é possível, pois estamos admitindo que o problema com n discos possua solução):

Em seguida, transfira o disco que restou na pilha original (o maior dos discos) para a haste vazia:

Feito isto, resolva novamente o problema para os n discos que estão juntos, transferindo-os para a haste que contém o maior dos discos:

Isso mostra que o problema com n + 1 discos também possui solução, e, portanto, por Indução Matemática, que P(n) é verdadeira para todo $n \in N$. Para determinar uma fórmula para jn, veja que, para resolver o problema para $n + 1$ discos com o menor número de passos, temos, necessariamente, que passar duas vezes pela solução mínima do problema com n discos. Temos, então, que

$$j_{n+1} = 2j_n + 1.$$

Obtemos, assim, uma sequência (j_n) definida recorrentemente. Pode-se mostrar, sem dificuldade, por indução, que seu termo geral é dado por $j_n = 2^n - 1$.

Esse jogo foi idealizado e publicado pelo matemático francês Edouard Lucas, em 1882, que, para dar mais sabor à sua criação, inventou a seguinte "lenda":

Na origem do tempo, num templo oriental, Deus colocou 64 discos perfurados de ouro puro ao redor de uma de três colunas de diamante e ordenou a um grupo de sacerdotes que movessem os discos de uma coluna para outra, respeitando as regras acima explicadas. Quando todos os 64 discos fossem transferidos para outra coluna, o mundo acabaria. Você não deve se preocupar com a iminência do fim do mundo, pois, se, a cada

segundo, um sacerdote movesse um disco, o tempo mínimo para que ocorresse a fatalidade seria de $2^{64} - 1$ segundos e isto daria, aproximadamente, um bilhão de séculos!

3.10.2 DESCOBRINDO A MOEDA FALSA

Têm-se 2^n moedas de ouro, sendo uma delas falsa, com peso menor do que as demais. Dispõe-se de uma balança de dois pratos, sem nenhum peso. Vamos mostrar, por indução sobre n, que é possível achar a moeda falsa com n pesagens.

Para n = 1, isso é fácil de ver, pois, dadas as duas moedas, basta pôr uma moeda em cada prato da balança e descobre-se imediata- mente qual é a moeda falsa.

Suponha, agora, que o resultado seja válido para algum valor de *n* e que se tenha que achar a moeda falsa dentre 2^{n+1} moedas dadas. Separemos as 2^{n+1} moedas em 2 grupos de 2^n moedas cada. Coloca-se um grupo de 2^n moedas em cada prato da balança. Assim, poderemos descobrir em que grupo de 2^n moedas encontra-se a moeda falsa. Agora, pela hipótese de indução, descobre-se a moeda falsa com n pesagens, que, junto com a pesagem já efetuada, perfazem o total de n + 1 pesagens.

3.10.3 A PIZZA DE STEINER

O grande geômetra alemão Jacob Steiner (1796-1863) propôs e resolveu, em 1826, o seguinte problema:

Qual é o maior número de partes em que se pode dividir o plano com n cortes retos?

Pensando o plano como se fosse uma grande pizza, temos uma explicação para o nome do problema.

Denotando o número máximo de pedaços com n cortes por pn, vamos provar por indução a fórmula:

$$s_n = \frac{n.(n+1)}{2} + 1$$

Para n = 1, ou seja, com apenas um corte, é claro que só podemos obter dois pedaços. Portanto, a fórmula está correta, pois

$$s_n = \frac{1.(1+1)}{2} + 1 = \frac{1.2}{2} + 1 = 2$$

Admitamos agora que, para algum valor de n, a fórmula para s_n esteja correta. Vamos mostrar que a fórmula para s_{n+1} também está correta.

Suponhamos que, com n cortes, obtivemos o número máximo n(n + 1)/2 + 1 de pedaços e queremos fazer mais um corte, de modo a obter o maior número possível de pedaços.

Vamos conseguir isso se o (n + 1)-ésimo corte encontrar cada um dos n cortes anteriores em pontos que não são de interseção de dois cortes (faça um desenho para se convencer disso).

Por outro lado, se o (n+1)-ésimo corte encontra todos os n cortes anteriores, ele produz n + 1 novos pedaços: o corte começa em um determinado pedaço e, ao encontrar o primeiro corte, ele separa em dois o pedaço em que está, entrando em outro pedaço. Ao encontrar o segundo corte, ele separa em dois o pedaço em que está, entrando em outro pedaço, e assim sucessivamente, até encontrar o n-ésimo corte separando o último pedaço em que entrar em dois. Assim, são obtidos n + 1 pedaços a mais dos que já existiam; logo,

$$s_{n+1} = s_n + n + 1 = \frac{n.(n+1)}{2} + 1 + n + 1 = \frac{n^2 + n + 2 + 2n}{2} + 1 = \frac{n^2 + 3n + 2}{2} + 1$$
$$= \frac{(n+1).(n+2)}{2} + 1 = \frac{(n+1).[(n+1)+1]}{2} + 1$$

mostrando que a fórmula está correta para n + 1 cortes. O resultado segue então o Principio da Indução Infinita.

4. TEOREMA FUNDAMENTAL DA ARITIMÉTICA

4.1 NÚMEROS PRIMOS

Iniciaremos este capitulo com o estudo dos números primos, um dos conceitos mais importantes de toda a Matemática. Esses números desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos. A descoberta dos números primos é imprescindível na Matemática, pois eles intitulam o princípio central na teoria dos números, consistindo no **Teorema Fundamental da Aritmética**. Esse Teorema satisfaz uma condição interessante no conjunto dos números naturais, ele afirma que todo número inteiro natural, sendo maior que 1, pode ser escrito como um produto de números primos, enfatizando que o número 1 não pode ser considerado primo, pois ele tem apenas um divisor e não pode ser escrito na forma de produto de números primos.

Números primos e sua importância para a Matemática
(Figura 3)

4.1.1 Definição: *Um número natural* ***maior*** *ou* ***igual*** *do que 2 que só possui como divisores positivos 1 e ele próprio é chamado de* ***número primo***.

De outra forma podemos dizer que um número natural n é primo se, sempre que escrevemos $n = a.b$, com $a, b \in$ N, temos necessariamente $a = 1$ e $b = n$ ou $a = n$ *e* $b = 1$. Consequentemente, um número natural n é composto, se existem $a, b \in$ N, com $1 < a < n$ e $1 < b < n$, tais que $n = a.b$. Observe que o número 1 não é primo.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:
I) Se $p \mid q$, então $p = q$.
De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

II) Se $p \nmid a$, então mdc $(p; a) = 1$.

De fato, se mdc $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$.

Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será chamado composto.

Portanto, se um número inteiro $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq n$. Portanto, existirá um número natural n_2 tal que $n = n_1.n_2$; com $1 < n_1 < n$ e; $1 < n_2 < n$

Números primos são como "tijolos" com os quais você pode construir todos os números naturais. Como isso pode ser feito? Considere o número 420. Ele é composto, pois pode ser representado como 420 = 42.10. Mas o número 42 e 10 também são compostos. De fato 42 = 6.7 e 10 = 2. 5. Como 6 = 2.3, temos 420 = 42.10 = 6.7.2.5 = 2.3.7.2.5 = 2.2.3.5.7 = 2^2.3.5.7 que é a sua representação como produto de números primos (figura).

Figura 4 – construção do número 420.

Os exemplos, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 10, 15, 35 e 348 são compostos.

Uma pergunta que surge espontaneamente é a seguinte: Quantos são os números primos? Euclides de Alexandria, em 300 a.C., ou seja, há mais de 2 300 anos, mostrou que existem infinitos números primos. Veremos esta afirmação mais adiante.

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, logo todos os números inteiros, conforme veremos mais adiante no ***Teorema Fundamental da Aritmética***.

A seguir, estabelecemos um resultado fundamental de Euclides (*Os Elementos, Proposição 30, Livro VII*).

Proposição 4.1.2 Sejam $a; b; p \in \mathbb{N}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração:

Basta provar que, se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que mdc $(p,a) = 1$, e o resultado segue-se do Teorema 5.2.2 da referência [2].

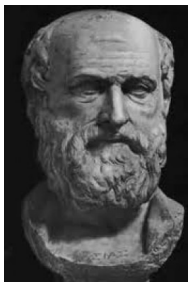
Corolário 4.1.3 Sejam $p, p_1, p_2, \ldots, p_n$ números primos. Se $p|p_1.p_2. \ldots .p_n$, então $p = p_i$ para algum $i = 1, 2, \ldots, n$.

Demonstração:

Demonstra-se o resultado por indução sobre n. Se $n = 2$, o resultado vale pela Proposição 4.1.2. Como hipótese de indução suponha que o resultado vale para $n - 1$. Agora se, $p|p_1.p_2....p_n$ tem-se que $p|p_1.p_2....p_{n-1}$ ou $p|p_n$. Se $p|p_n$ o resultado segue. Se $p \nmid p_n$ então $p|p_1.p_2....p_{n-1}$ e, pela hipótese de indução p = pi para algum $i = 1, 2, \ldots, n - 1$.

4.2 O CRIVO DE ERATÓSTENES

Um método muito antigo para se obter de modo sistemático números primos é o chamado ***Crivo de Eratóstenes***, devido ao matemático grego Eratóstenes.



ERATÓSTENES

Eratóstenes de Cirene foi um importante geográfo, matemático, astrônomo e filósofo pré-socrático. Nasceu na cidade de Cirene, antiga colônia grega na atual Líbia, em 276 a.C. e morreu aos 82 anos na cidade de Alexandria (Egito) em 194 a.C. Entre muitos dos seus feitos foi o criador do Crivo de Eratóstenes, método (algoritmo) prático para encontrar números primos dentre os naturais.

A eficiência do método é baseada na observação bem simples a seguir.

Para se obter os números primos até uma certa ordem n, escreva os números de 2 até n em uma tabela.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
...	...	...	...	...	...	...	...	...	n

Dicionário

A palavra crivo significa peneira.
O método consiste em peneirar os números naturais em um intervalo [2; n], jogando fora os números que não são primos.

• Observamos que o primeiro primo que aparece na tabela acima é 2 e imediatamente apagamos da lista todos os múltiplos de 2 maiores que ele, por serem compostos; resta assim a seguinte lista.

2, 3, 5, 7, 9, 11, 13, 15, 17 . . .

• O primeiro número não apagado que aparece na lista restante é 3, que também é primo. Imediatamente apagamos da lista todos os múltiplos de 3 maiores que ele, por serem compostos; resta agora a lista

2, 3, 5, 7, 11, 13, 17, . . .

• O primeiro número não apagado que aparece na lista que restou do passo anterior é 5, que também é primo. Imediatamente apagamos da lista todos os múltiplos de 5 maiores que ele, por serem compostos. Se repetirmos este processo até o maior número menor que $\sqrt{n}$, os números que sobram são exatamente os números primos.

Exemplo: Fazendo $n = 80$, temos que $\sqrt{80} = 8{,}94442719...$. Então, aplicando o método:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

Etapa 1: Ordenamos os números

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	

Etapa 2: Tiramos os múltiplos de 2

	2	**3**		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	

Etapa 3: Tiramos os múltiplos de 3

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	

Etapa 4: Tiramos os múltiplos de 5

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	

Etapa 5: Tiramos os múltiplos de 7

Deveríamos seguir mais uma etapa, pois $11^2 > 80$, no entanto todos os múltiplos de 11 menores que 80 já foram eliminados, temos então listados todos os primos de 2 até 79.

4.3 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Apresentaremos um dos principais teoremas da aritmética que diz que todo número inteiro maior ou igual a 2 pode ser escrito como produto de números primos. Por exemplo, 2100 é escrito de maneira única, a menos pela ordem dos fatores, como $2^2 \times 3^1 \times 5^2 \times 7^1$.

A ordem dos fatores, pela propriedade comutativa da multiplicação, é irrelevante. O que torna tal teorema interessante é a garantia de obtenção de uma representação única para todo e qualquer número natural. Isso abre diversas possibilidades de aplicação, como em criptografia, onde um texto pode ser codificado como uma sequência de números primos.

4.3.1 Teorema (Teorema Fundamental da Aritmética).

Todo número natural $n \geq 2$ ou é primo ou pode ser escrito como um produto de números primos. Essa decomposição é única, a menos da ordem dos fatores.

Demonstração do Teorema.

(i) Sendo n primo, mais nada a mostrar.

(ii) Supondo n composto um inteiro maior que 1. Seja $p_1 > 1$ o menor dos divisores primos positivos de n tem-se:

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

Se $n_1 = 1$, então $n = p_1$ obtemos a composição em fatores.

Caso contrário, temos $n_1 = p_2.n_2.$, $p_2 > 1$ o menor dos divisores primos positivos de n_1 tem-se:

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

Se $n_2 = 1$, então $n = p_1.p_2$ obtemos do mesmo modo a composição em fatores.

Caso contrário $n_2 = p_3.n_3.$ então teríamos

$$n = p_1.p_2.\ p_3.n_3, \quad 1 \leq n_3 < n_2 < n_1$$

Fazendo esse processo sucessivamente temos uma sequência estritamente decrescente

$$1 \leq \ ..< n_{k+1} < n_k < ... < n_3 < n_2 < n_1 < n$$

Como todos são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, ..., p_k$ não são necessariamente distintos, n terá, em geral, a forma:

$$n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}.p_4^{a_4}....p_k^{a_k}$$

onde $k \geq 1$ é um número natural, $a_i \in \mathrm{N}$ e p_i é primo para todo $1 \leq i \leq k.$ Além disso, a fatoração é única se exigirmos $p_1 < p_2 < ... < p_k.$

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1.p_2.....p_k = q_1.q_2...q_s$$

com $p_1 \leq p_2 \leq ... \leq p_k$, $q_1 \leq q_2 \leq ... \leq q_s$ e que n é mínimo com tal propriedade. Como p_1 divide $q_1 . q_2. ... . q_s$ temos pelo Corolário 4.1.3, que, para algum i, $p_1 = q_i$, e logo $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n / p_1 = p_2.p_3.....p_k = q_2.q_3...q_s$$

admite uma única fatoração, pela minimalidade de n, donde $k = s$ e $p_i = q_i$ para todo $_i$, o que contradiz o fato de n ter duas fatorações.

Outra forma de escrever a fatoração acima

$$n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}.p_4^{a_4}....p_k^{a_k}$$

com $p_1 < \cdots < p_k$ e $a_i > 0$. Ainda outra formulação é escrever

$$n = 2^{a_1}.3^{a_2}.5^{a_3}.7^{a_4}....p^{a_i}$$

4.3.2 TEOREMA (Teorema de Euclides). A quantidade de números primos é infinita.

Demonstração:

Faremos a prova por redução ao absurdo. Suponha que existe uma quantidade finita de números primos e denotemos estes por

$$p_1, p_2, p_3, p_4, p_5, p_6, ..., p_r.$$

Consideremos o número

$$n = p_1. p_2. p_3. p_4. p_5. p_6. .... p_k. \text{ , sendo } n > 1$$

temos que esse número tem um sucessor que chamamos de $n + 1$ que podemos afirmar que não é primo, pois senão ele estaria entre os p_k do número n *e* $n + 1$ é um número composto, então podemos escreve-lo como:

$$n + 1 = k.p_j \quad \text{(i)}$$

$$n = k'.p_j \quad \text{(ii)}$$

logo substituindo (ii) em (i) ficaremos com: $k'.p_j + 1 = k.p_j \rightarrow k.p_j - k'.p_j = 1 \rightarrow p_j.(k - k') = 1$ que teríamos o 1 como um número composto que é um ***Absurdo***.

Concluímos a afirmação de Euclides que a quantidade de números primos é infinita.

Uma das aplicações do Teorema Fundamental da Aritmética é encontrar o número de divisores de um número n e quem são estes divisores. Faremos isto através de exemplos.

Exemplo: Quantos são os divisores de 24.

Decompondo o 24 em fatores primos teremos:

$24 = 4 \times 6 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$ então os divisores de 24 podem ser todos números da forma 2×3 . Onde os valores dos expoente do 2 vão variar de 0 a 3 e os do número 3 serão 0 e 1.

Vejamos: $2^0 \times 3^0 = 1$ $2^1 \times 3^1 = 6$

$2^1 \times 3^0 = 2$ $2^3 \times 3^0 = 8$

$2^0 \times 3^1 = 3$ $2^2 \times 3^1 = 12$

$2^2 \times 3^0 = 4$ $2^3 \times 3^1 = 24$

Então teremos 8 divisores que pode ser facilmente verificado com a contagem dos expoentes. D(24) = 4.2 = 8, onde 4 é o número de expoentes do 2 (0, 1, 2, 3) e 2 são os expoentes do 3 (0 e 1).

Generalizando dizemos que o número de divisores de um número N será dado por:

$$D(N) = (a_1 + 1).(a_2 + 1). \ldots . (a_i + 1),$$

onde $a_i > 0$ são os expoentes dos primos decompostos.

4.4 EXERCÍCIOS PROPOSTOS

4.4.1 Diga quais dos seguintes números são primos e quais são compostos:

9; 12; 16; 17; 21; 23; 47; 49.

4.4.2 O número $n = 2^{20} - 25^4$ é composto?

Solução: Sendo $n = 2^{20} - 25^4$, temos:

$$n = (2^{10})^2 - (25^2)^2 =$$
$$= 1024^2 - 625^2 =$$
$$= (1024 - 625).(102^2 + 625) =$$
$$= 399. 1649 = 3.133.1649$$

Portanto $n = 2^{20} - 25^4$ é composto.

4.4.3 Determinar todos os inteiros positivos n tais que n, n+2 e n+4 são todos primos.

4.4.4 (OBM – 2004) Dizemos que um número natural é composto quando pode ser escrito como produto de dois números naturais maiores que 1. Assim, por exemplo, 91 é composto porque podemos escrever $91 = 7 \times 13$.

Mostre que o número $2^{\left(2^{2004}+2\right)}+1$

é composto.

4.4.5 Determine todos os números primos *p* que são iguais a um quadrado perfeito menos 1.

Solução: Sendo $p = n^2 - 1$, temos que $p = (n + 1).(n - 1)$. Pela definição de numero primo só existem duas possibilidades:

$n + 1 = 1$ e $n - 1 = p$ onde teremos $n = 0$ e $p = -1$, pois $p \in \mathbb{N}$, logo não convém,

ou

$n + 1 = p$ e $n - 1 = 1$ onde teremos $n = 2$ e $p = 3$, então $p = 3$.

4.4.6 Determine $m \in \mathbb{N}$ de modo que o número 20.21^m tenha exatamente 96 divisores positivos.

4.4.7 Seja $N = 12^{2012} + 2012^{12}$. O maior valor de n tal que 2^n é divisor de N é:

(A) 10 (B) 12 (C) 16 (D) 24 (E) 36

4.4.8 As casas do quadrado da figura foram preenchidas com nove números inteiros positivos, de modo a fazer com que os produtos dos números de cada linha, de cada coluna e de cada diagonal fossem todos iguais.

	6	9
		12

Em seguida, seis números inteiros foram apagados, restando os números 6, 9 e 12, nas posições mostradas. Se x era o número escrito na casa que está na primeira linha e na primeira coluna, e y era o número escrito na casa que está na primeira linha e na terceira coluna, então a soma x + y é igual a

(A) 5 (B) 9 (C) 18 (D) 20 (E) 36

4.4.9 Ache os possíveis valores de n, $m \in \mathbb{N} \cup \{0\}$ de modo que o número $9^m.10^n$ tenha:

a) 27 divisores positivos b) 243 divisores positivos

5. CONGRUÊNCIAS

5.1 INTRODUÇÃO

SEXTA-FEIRA 13...

Mês ruim para quem tem paraskevidekatriaphobia. Surpreso com a estranha palavra? Segundo o dicionário inglês Macmillan, "paraskevidekatriaphobia" significa fobia por sexta-feira 13, verbete criado a partir das palavras gregas "paraskevi" (sexta-feira) e "dekatria" (treze), com sufixo referente à fobia. Se você tem fobia por sexta-feira 13, é bom se preparar porque teremos três dias assim no ano de 2015.

A má notícia para os fóbicos é que em 2015, além de fevereiro e março, também teremos uma sexta-feira 13 no mês de novembro, e a boa é que em 2016 teremos apenas uma sexta-feira treze, que, aliás, é o menor número de sextas-feiras 13 que podemos ter em um ano. Provaremos mais a frente que em um ano qualquer, seja ele bissexto ou não, sempre temos o mínimo de uma e o máximo de três sextas-feiras 13.

Para esse e outros tipos de problemas utilizaremos de uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Uma congruência é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Por exemplo, o número 9 é congruente ao número 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2$, mod. 7. Foi o brilhante Gauss que observou que usávamos com muita frequência frases do tipo "***a*** dá o mesmo resto que ***b*** quando divididos por ***n***" e que essa relação tinha um comportamento semelhante à igualdade. Foi Gauss então que introduziu uma notação específica para este fato e que denominou de "congruência".

(Adaptado do Painel I, do Prof. José Luiz Pastore Mello pág. 18, da Revista do Professor de Matemática nº 82)

DESCOBRINDO O DIA DA SEMANA QUE UMA PESSOA NASCEU.

Existe uma brincadeira bem interessante de fazer com alunos que é como descobrir o dia da semana que uma pessoa nasceu.

A regra para determinarmos o dia da semana de qualquer data entre 01 de Janeiro de 1900 até 2399 será dada fazendo os seguintes passos:

Passo 1: Calcule quantos anos se passaram desde 1900 até o ano em que você nasceu. Chamaremos esse valor de **A**.

Passo 2: Calcule quantos 29 de Fevereiro existiram depois de 1900. Para isso, basta dividir por 4 o valor de A, ficando somente com a parte inteira, desconsiderando o resto da divisão. Chamaremos esse valor de **B**. Caso seja ano bissexto e a data for anterior ou igual a 29 de Fevereiro, considere então **B-1**.

Passo 3: Considerando o mês do nascimento, obtenha o número associado a ele (que chamaremos de **C**), que está presente na seguinte tabela:

Janeiro	0	**Julho**	6
Fevereiro	3	**Agosto**	2
Março	3	**Setembro**	5
Abril	6	**Outubro**	0
Maio	1	**Novembro**	3
Junho	4	**Dezembro**	5

Passo 4: Considere o dia do nascimento **x**. Calcule **x – 1**, divida por 7 e encontre o resto (congruência mod 7) chamaremos essa quantidade de **D**.

Passo 5: Some os quatro valores anotados **A, B (ou B – 1), C** e **D** então divida o resultado por 7 e tome o resto dessa divisão, após isso confira o dia da semana associado à esse resto:

2ª feira	**3ª feira**	**4ª feira**	**5ª feira**	**6ª feira**	**Sábado**	**Domingo**
0	1	2	3	4	5	6

Vejamos a data de nascimento de um famoso matemático brasileiro – 8 de fevereiro de 1973 temos:

A = 1973 – 1900 = 73

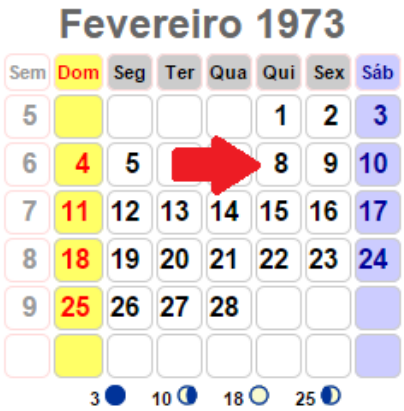
B = 73 : 4 = 18 (parte inteira)

C = 3

D = 8 – 1 = 7 que dividido por 7 deixa resto 0

Somando tudo teremos:

A + B + C + D = 73 + 18 + 3 + 0 = 94 que quando dividido por 7 deixa resto 3 (congruência módulo 7), logo pela tabela ele nasceu na 5ª feira!!! Vamos conferir:



Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O que não é muito comum é o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, NUP, criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos em nosso estudo.

5.2 DEFINIÇÃO

Seja n um número inteiro diferente de zero. Diremos que dois números inteiros a e b são **congruentes** módulo n se os restos de sua divisão euclidiana por n são iguais. Quando os inteiros a e b são congruente módulo n, escreve-se:

$$a \equiv b \bmod n$$

Exemplo 1: $37 \equiv 25 \bmod 3$, *pois* $37 = 3.12 + 1$ *e* $25 = 3.8 + 1$, *ambos têm resto* 1 *na divisão por* 3.

Do mesmo modo $-43 \equiv -88 \bmod 5$, pois $-43 = 5.(-9) + 2$ e $-88 = 5.(-18) + 2$, ambos têm resto 2 na divisão por 5.

Observação: Desta mesma forma, pode-se definir números incôngruos módulo n (com notação $\not\equiv$), quando dois números a e b não têm os mesmos restos na divisão por n.

Exemplo 2: $13 \not\equiv 16 \bmod 7$, *pois* $13 = 1.7 + 6$ *e* $16 = 2.7+ 2$, ambos restos diferentes na divisão por 7.

Repare que no exemplo 1 acima que $73 - 52 = 3.24 + 1 - 3.17 - 1 = 21$ e $3 \mid 21$, esta relação não é coincidência. Veja a proposição seguinte:

Proposição 5.1.1 *Dados* $a,b \in \mathbb{Z}$ *tem-se* $a \equiv b \bmod n$ *se, e somente se,* $n \mid b - a$.

Demonstração:

Se $a \equiv b \bmod n$ significa dizer que n divide $a - b$, logo pelo algoritmo da divisão, existem q_1, q_2, r_1 *e* r_2 inteiros tais que, $a = q_1.n + r_1$ *e* $b = q_2.n + r_2$ de forma que:

$b - a = q_2.n + r_2 - (q_1.n + r_1) = (q_2 - q_1).n + (r_2 - r_1)$, *como pela definição* $r_2 = r_1$ *temos que* $b - a = (q_2 - q_1).n \rightarrow n \mid b - a$.

Se $n \mid b - a$ significa que a divisão de $b - a$ por n deixa resto igual a zero logo como $b=q_2.n+ r_2$ e $a=q_1.n+r_1$ temos que $b - a = q_2.n + r_2 - (q_1.n + r_1) = (q_2 - q_1).n + (r_2 - r_1)$ como $r_2 - r_1 = 0$ temos que $r_2 = r_1 \rightarrow a \equiv b \bmod n$

Exemplo 3: $7 \equiv 2 \bmod 5$, *pois* $5 \mid 7 - 2$ *e* $6 \equiv 2 \bmod 4$, *porque* $4 \mid 6 - 2$.

Proposição 5.1.2 Dados $a,b,c \in \mathbb{Z}$ e $n \in \mathbb{N}$, tem-se:

i) $a \equiv a \bmod n$,

ii) se $a \equiv b \bmod n$, então $b \equiv a \bmod n$,

iii) se $a \equiv b \bmod n$ *e* $b \equiv c \bmod n$ *então* $a \equiv c \bmod n$.

Teorema. Se $a \equiv b \pmod n$ e $c \equiv d \pmod n$, então:

i) $\boldsymbol{a + c \equiv b + d \pmod n}$

Demonstração:

Como $a \equiv b \pmod n$ e $c \equiv d \pmod n$ temos que $n \mid b - a$ e $n \mid d - c$ *e* também $n \mid (b - a) + (d - c) = (b+d) - (a + c)$ logo $a + c \equiv b + d \pmod n$.

ii) $\boldsymbol{a - c \equiv b - d \pmod n}$

Demonstração:

Como $a \equiv b \pmod n$ e $c \equiv d \pmod n$ temos que $n \mid b - a$ e $n \mid d - c$ *e* também

$n \mid (b - a) - (d - c) = (b - d) - (a - c)$ logo $a - c \equiv b - d \pmod{n}$.

iii) $ka \equiv kb \pmod{n}$ $\forall k \in \mathbf{Z}$

Demonstração:

Como $a \equiv b \pmod{n}$ temos que $n \mid b - a$ e também $n \mid k(b - a) = k.b - k.a$,

logo $k.a \equiv k.b \pmod{n}$.

iv) $a.c \equiv b.d \pmod{n}$

Demonstração:

Como $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ temos que $n \mid b - a$ e $n \mid d - c$

$n \mid b - a \rightarrow n \mid (b - a).d = b.d - a.d$ e $n \mid d - c \rightarrow n \mid (d - c).a = a.d - c.a$

$n \mid (b.d - a.d) + (a.d - c.a) = b.d - a.d + a.d - c.a = b.d - c.a \Rightarrow b.d \equiv c.a$

v) $a^k \equiv b^k \pmod{n}$ $\forall k \in \mathbf{N}$

Demonstração: por indução:

Fazendo c = a e d = b e aplicando o item anterior teremos:

(i) $a.a \equiv b.b \pmod{n}$, logo $a^2 \equiv b^2 \pmod{n}$,

dessa forma teremos que $a^2.a \equiv b^2.b \pmod{n}$ que é igual a $a^3 \equiv b^3 \pmod{n}$.

(ii) Hipótese: $a^k \equiv b^k \pmod{m}$ $\forall k \in N$

(iii) Tese: $a^{k+1} \equiv b^{k+1} \pmod{m}$ $\forall k \in N$

Como $a^k \equiv b^k \pmod{m}$ e fazendo c = a e d = b e aplicando o item iv) $a^k.a \equiv b^k.b \pmod{n} = a^{k+1} \equiv b^{k+1} \pmod{m}$ $\forall k \in N$.

vi) Se mdc(k,n) = d, então ka ≡ kb (mod n) ⇔ a ≡ b (mod n/d)

($\Rightarrow$) $ka \equiv kb \pmod{n} \rightarrow n \mid kb - ka = k(b - a)$ e como mdc(k,n) = d podemos dizer que k = k'.d e n = n'.d sendo mdc(k', n') = 1. Agora temos n'.d| k'.d(b – a) → n'| b – a , pois k' e n' são primos entre si. n' = n/d → n/d| b – a logo $a \equiv b \pmod{n/d}$.

($\Leftarrow$) dizendo que k = k'.d e n = n'.d sendo mdc(k', n') = 1 e $a \equiv b \pmod{n/d} \rightarrow$ n' = n/d → n'| b – a → n'.d| k'.d(b – a) → n | k (b – a) = kb – ka → $ka \equiv kb \pmod{n}$.

Em termos práticos, podemos realizar quase todas as operações elementares envolvendo igualdade de inteiros. Uma das diferenças cruciais é a operação de divisão como mostra o último item do teorema anterior.

Exemplo 4: Calcule o resto da divisão 12^{12} por 5.

Como $12^2 = 144 \equiv 4 \pmod 5$, temos que $12^4 = (12^2)^2 \equiv 4^2 = 16 \equiv 1 \pmod 5$ logo

$12^{12} = (12^4)^3 \equiv 1^3 = 1 \pmod 5$.

Exemplo 5: Calcule o resto da divisão da expressão 78549238 + 31484569 – 62474806 por 5.

Veja: $78549238 \equiv 3 \pmod 5$

$31484569 \equiv 4 \pmod 5$

$62474806 \equiv 1 \pmod 5$

Aplicando o item i) e ii) do teorema teremos que:

$78549238 + 31484569 - 62474806 \equiv 3 + 4 - 1 = 6 \equiv 1 \pmod 5$ então o resto é 1.

5.3 EXERCÍCIOS PROPOSTOS

5.3.1 Ache o resto da divisão de 5^{60} por 26.

$5^2 = 25 \equiv -1 \pmod{26}$ então temos que $5^{60} = (5^2)^{30} \equiv (-1)^{30} = 1 \pmod{26}$

5.3.2 Determine o resto da divisão de $2^9.3^8.5^{13}$ por 7

$2^3 = 8 \equiv 1 \pmod 7 \rightarrow (2^3)^3 \equiv 1^3 = 1 \pmod 7$.

$3^3 = 27 \equiv -1 \pmod 7 \rightarrow (3^3)^2 = 3^6 \equiv (-1)^2 = 1 \pmod 7 \rightarrow 3^8 = 3^6.3^2 \equiv 1.2 = 2 \pmod 7$.

$5^3 = 125 \equiv -1 \pmod 7 \rightarrow (5^3)^4 = 5^{12} \equiv (-1)^4 = 1 \pmod 7 \rightarrow 5^{13} = 5^{12}.5 \equiv 1.5 = 5 \pmod 7$.

$2^9.3^8.5^{13} \equiv 1.2.5 = 10 \equiv 3 \pmod 7$

Portanto, o resto da divisão de $2^9.3^8.5^{13}$ por 7 é 3.

5.3.3 Determine o resto de $2^{20} - 1$ na divisão por 41.

$2^5 = 32 \equiv -9 \pmod{41} \rightarrow (2^5)^2 = 2^{10} \equiv (-9)^2 = 81 \equiv -1 \pmod{41}$ então teremos:

$2^{20} = (2^{10})^2 \equiv (-1)^2 = 1 \pmod{41} \rightarrow 2^{20} \equiv 1 \pmod{41} \rightarrow 2^{20} - 1 \equiv 0 \pmod{41}$.

Portanto, o resto da divisão de $2^{20} - 1$ por 41 é 0.

5.3.4 Ache o resto da divisão de $2^{50} + 41^{65}$ por 7

5.3.5 Demostre $31 | 20^{15} - 1$.

5.3.6 Se $a = (72)^6 + (72)^5 + 2$, mostre que $7 | a$.

5.3.7 Demonstre que $\forall n \in$ N, o número $n^3 + 5n$ é divisível por 6, utilizando congruência.

5.3.8 Mostre que o número $43^{101} + 23^{101}$ é divisível por 66.

5.3.9 (CMRJ) Considere três números naturais representados por m, n e p. Se os restos das divisões de m, n e p por 11 são, respectivamente, 3, 4 e 5, então, o resto da divisão de (m + n + p) por 11 é: a) 5 b) 4 c) 3 d) 1

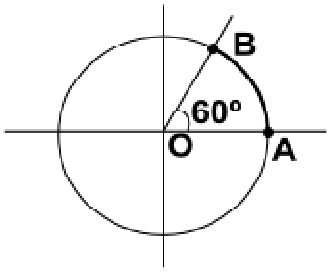
5.4 APLICAÇÕES INTERESSANTES DE CONGRUÊNCIAS

5.4.1 CONGRUÊNCIAS NA TRIGONOMETRIA (ARCOS CONGRUÔS)

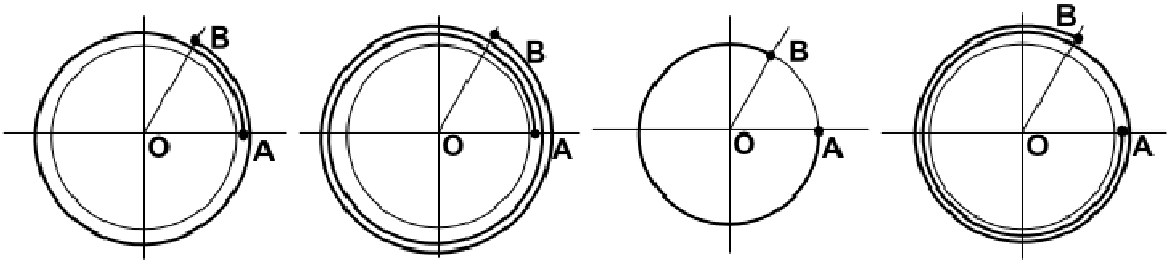
CONGRUÊNCIA

Dois arcos são ***côngruos*** *(ou* ***congruentes****) quando têm a mesma extremidade e se diferem apenas pelo número de voltas inteiras.*
Assim, se um arco mede α rad, a expressão geral dos arcos côngruos a ele é dada por $\alpha + 2k\pi$ *em que* $k \in Z$. *Na figura abaixo exibimos vários arcos côngruos ao arco de 60º ou de π/3 rad.*

Um arco de 60º (ou π/3 rad)...



...e seus arcos côngruos



http://rived.mec.gov.br/atividades/matematica/mundo_trigonometria/teoria/circulo.html

Exercício 5.4.1.1 Obtenha as menores determinações não negativas dos arcos.
a) 1300º

Solução: Temos que
360º ≡ 0 (mod 360º)
720º = 360º + 360º ≡ 0 (mod 360º)

1080º = 720º + 360º ≡ 0 (mod 360º)

1300º = 1080º + 220º ≡ 220º (mod 360º) logo 1300º é côngruo com 220º

b) –1200º

Resolução: Temos que
–1200º = –1080º - 120º ≡ –120º (mod 360º)

–1200º ≡ –120º (mod 360º)

–1200º = –1080º - 120º ≡ –120º (mod 360º)

–1200º + 360º ≡ –120º + 360º = 240º (mod 360º)

Exercício 5.4.1.2 Numa competição escolar, um aluno tinha que percorrer 2925º de uma pista circular. Se ele tivesse que percorrer o arco côngruo a este arco quantos graus ele correria?

Solução: 2925º = 1080º + 1080º + 720º + 45º ≡ 45º (mod 360º)

5.4.2 CONGRUÊNCIAS EM COMPLEXOS (POTÊNCIAS DE i)

Exemplo 5.4.2.1 Efetue as operações indicadas:

$i^0, i^1, i^2, i^3, i^4, i^5, i^6, i^7, i^8$

Solução: Resolvendo diretamente, sem muitos detalhes:

$i^0 = 1$

$i^1 = i$

$i^2 = -1$

$i^3 = i^2.i = (-1).i = -i$

$i^4 = (i^2)^2 = (-1)^2 = 1$

$i^5 = i^4.i = (1).i = i$

$i^6 = i^4.i^2 = (1).(-1) = -1$

$i^7 = i^4.i^3 = (1).(-i) = -i.i^8 = i^4.i^4 = (1).(1) = 1.$

Continuando as potências de i, percebemos que trata-se de um problema cíclico, onde as potencias se repetem a cada ciclo de 4, conforme quadro:

$i^{4n} = (i^4)^n = (1)^n = 1$

$i^{4n+1} = (i^4)^n.i = (1)^n.i = i$

$i^{4n+2} = (i^4)^n.(i^2) = (1)^n.(-1) = -1$

$i^{4n+3} = (i^4)^n.(i^3) = (1)^n.(-i) = -i.$

Desse modo pode-se usar as seguintes congruências sobre o expoente das potências de i e então determinar quais valores do conjunto $\{1, i, -1, -i\}$ vale a potência, assim:

expoente de i ≡ 0 mod 4 ⟹ potência de i = 1,

expoente de i ≡ 1 mod 4 ⟹ potência de i = i,

expoente de i ≡ 2 mod 4 ⟹ potência de i = −1,

expoente de i ≡ 3 mod 4 ⟹ potência de i = −1.

Exemplo 5.4.2.2 Calcule o valor de: a) i^{56} b) i^{2015} c) $4i^{70} - i^{15}$

Solução:

(a) Como 56 ≡ 0 mod 4 , então $i^{56} = i^0 = 1$.

(b) Da mesma forma 2015 ≡ 3 mod 4 e então $i^{2015} = i^3 = -i$.

(c) De um lado 70 ≡ 2 mod 4 e 15 ≡ 3 mod 4 , por outro lado $4i^{70} - i^{15}$ é o mesmo que $4i^2 - i^3$ que por sua vez vale $4(-1)-(-i) = -4+i$.

5.4.3 APLICAÇÃO DE CONGRUÊNCIAS A POLINÔMIOS

Assim como a idéia de se associar a divisão euclidiana à notação em módulo é real e útil com números inteiros, podemos também utilizá-la para polinômios, veja alguns exemplos:

Exemplos:

5.4.3.1 $P(x) = x^4 - 1 \equiv 0(\text{mod}.x^3 + x^2 + x + 1)$,

Fatorando x^4-1, tem-se que $x^4-1=(x-1).(x^3+x^2+x+1)$, ou seja, x^4-1 deixa resto zero na divisão por x^3+x^2+x+1.

5.4.3.2 $P(x)=x^4+x-1\equiv x(\text{mod}.x^2-1)$

Dividindo x^4+x-1, por x^2-1 tem-se resto *x*.

5.4.3.3 Calcular o resto da divisão de $P(x)=x^5+x+1$ por $.x^3-1$.

Solução:

Temos que $.x^3-1\equiv 0(\text{mod}\,x^3-1)$, logo somando 1 em ambos os lados da congruência chega-se que $.x^3\equiv 1(\text{mod}\,x^3-1)$. $P(x)=x^5+x+1\equiv x^2(\overset{\equiv 1}{x^3})+x+1\equiv x^2+x+1$.

Logo o resto da divisão de $.P(x)$ por $.x^3-1$ é x^2+x+1.

6. RESOLUÇÃO DOS PROBLEMAS PROPOSTOS

6.1 - Capitulo 3

3.9.1 $1^2+2^2+3^2+4^2+.\cdots+n^2=\dfrac{n.(n+1).(2n+1)}{6}$

(i) Para *n = 1* temos

$$1^2=\frac{1.(1+1).(2.1+1)}{6}=\frac{1.2.3}{6}=1$$

(ii) Hipótese:

$$1^2+2^2+3^2+4^2+.\cdots+n^2=\frac{n.(n+1).(2n+1)}{6}$$

Verdadeiro para $\forall n\in \mathrm{N}$

Tese: $1^2+2^2+3^2+4^2+.\cdots+n^2+(n+1)^2=\dfrac{(n+1).[(n+1)+1].[2(n+1)+1]}{6}$

Somando $(n+1)^2$ em ambos os lados da hipótese temos:

$$1^2+2^2+3^2+4^2+.\cdots+n^2+(n+1)^2=\frac{n.(n+1).(2n+1)}{6}+(n+1)^2=$$
$$=\frac{n.(n+1).(2n+1)+6(n+1)^2}{6}=\frac{(n+1).[n.(2n+1)+6(n+1)]}{6}=$$
$$=\frac{(n+1).(2n^2+n+6n+6)}{6}=\frac{(n+1).(2n^2+7n+6)}{6}=\frac{(n+1).(2n^2+3n+4n+6)}{6}=$$
$$=\frac{(n+1).[n.(2n+3)+2.(2n+3)]}{6}=\frac{(n+1).[(n+2).(2n+3)]}{6}=\frac{(n+1).[(n+1)+1].[2(n+1)+1]}{6}$$

3.9.2 $2+4+6+.\cdots+2n=n.(n+1)$

(i) Para $k = 1$ temos

$$2=1.(1+1)=1.2=2$$

(ii) Hipótese:

$$2+4+6+.\cdots+2n=n.(n+1)$$

Tese:

$$2+4+6+.\cdots+2n+2(n+1)=(n+1).[(n+1)+1]$$

Somando $2(n + 1)$ de cada lado da Hipótese temos

$$2+4+6+.\cdots+2n+2(n+1)=n.(n+1)+2(n+1)=$$
$$=(n+1).(n+2)=(n+1).[(n+1)+1]$$

3.9.3 $\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\cdots+\frac{1}{n.(n+1)}=\frac{n}{n+1}$

(i) Para $k = 1$ temos

$$\frac{1}{1.2}=\frac{1}{1+1}=\frac{1}{2}$$

(ii) Hipótese: para $n = k$

$$\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\cdots+\frac{1}{n.(n+1)}=\frac{n}{n+1}$$

Tese:

$$\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\cdots+\frac{1}{n.(n+1)}+\frac{1}{(n+1).[(n+1)+1]}=\frac{n+1}{(n+1)+1}$$

Somando $\frac{1}{(n+1).[(n+1)+1]}=\frac{1}{(n+1).(n+2)}$ em ambos os lados da hipótese temos:

$$\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\cdots+\frac{1}{n.(n+1)}+\frac{1}{(n+1).(n+2)}=\frac{n}{n+1}+\frac{1}{(n+1).(n+2)}=$$
$$=\frac{n.(n+2)+1}{(n+1).(n+2)}=\frac{n^2+2n+1}{(n+1).(n+2)}=\frac{(n+1)^2}{(n+1).(n+2)}=\frac{(n+1)}{(n+2)}=\frac{(n+1)}{(n+1)+1}$$

3.9.4 $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}=2-\frac{n+2}{2^n}$

(i) Para $k = 1$ temos

$$\frac{1}{2}=2-\frac{1+2}{2^1}=2-\frac{3}{2}=\frac{4-3}{2}=\frac{1}{2}$$

(ii) Hipótese: para $n = k$

$$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n}=2-\frac{n+2}{2^n}$$

Tese:

$$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n+1}{2^{n+1}}=2-\frac{(n+1)+2}{2^{n+1}}$$

Somando $\frac{n+1}{2^{n+1}}$ de cada lado da Hipótese temos

$$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots++\frac{n}{2^n}+\frac{n+1}{2^{n+1}}=2-\frac{n+2}{2^n}+\frac{n+1}{2^{n+1}}=$$
$$=\frac{2.2^{n+1}-2(n+2)+n+1}{2^{n+1}}=\frac{2^{n+2}-2n-4+n+1}{2^{n+1}}=$$
$$=\frac{2^{n+2}}{2^{n+1}}-\frac{n+3}{2^{n+1}}=2-\frac{(n+1)+2}{2^{n+1}}$$

3.9.5 $1^3+2^3+3^3+4^3+.\cdots+n^3=\frac{n^2.(n+1)^2}{4}$

(i) Para $k = 1$ temos

$$1^3 = \frac{1^2.(1+1)^2}{4} = \frac{1^2.2^2}{4} = 1$$

(ii) Hipótese:

$$1^3 + 2^3 + 3^3 + 4^3 + .\cdots + n^3 = \frac{n^2.(n+1)^2}{4}$$

Tese:

$$1^3 + 2^3 + 3^3 + 4^3 + .\cdots + n^3 + (n+1)^3 = \frac{(n+1)^2.[(n+1)+1]^2}{4}$$

Somando $(n + 1)^3$ de cada lado da Hipótese temos

$$1^3 + 2^3 + 3^3 + 4^3 + .\cdots + n^3 + (n+1)^3 = \frac{n^2.(n+1)^2}{4} + (n+1)^3 =$$

$$= \frac{n^2.(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2.[n^2 + 4(n+1)]}{4} = \frac{(n+1)^2.(n^2 + 4n + 4)}{4} =$$

$$= \frac{(n+1)^2.(n+2)^2}{4} = \frac{(n+1)^2.[(n+1)+1]^2}{4}$$

3.9.6 Demonstre que $\forall n \in$ N, o número $n^3 + 5n$ é divisível por 6.

(i) Para $k = 1$, a desigualdade $1^3 + 5.1 = 6$ é verdadeira.

(ii) Hipótese: consideremos que $k^3+5k = 6.q$ é verdadeiro para $n = k$.

Tese: $(k+1)^3+5(k+1) = 6.q'$

$(k+1)^3+5(k+1) = k^3 +3k^2 + 3k + 1 + 5k +5 = k^3 + 5k + 3k^2 + 3k + 6 =$

$= \underbrace{(k^3 + 5k)}_{\text{Hipótese}} + 3(\underbrace{k^2 + k + 2}_{\text{paridade sempre teremos 3.2.k}}) = 6.q'$ *logo* $n^3 + 5n$ *é sempre divisível por 6.*

3.9.7 Mostre que $5^n - 1$ é múltiplo de 24 para todo número natural n par.

(i) Para $k = 2$, a desigualdade $5^2 - 1 = 25 - 1 = 24$ é verdadeira.

(ii) Hipótese: consideremos que $5^{2k} - 1 = 24.q$ é verdadeiro para $n = 2k$.

Tese: $5^{2(k+1)} - 1 = 24.q'$

$5^{2k} - 1 = 24.q \; x \; (25) \Rightarrow 5^{2k}.25 - 25 = 5^{2k}.5^2 - 24 - 1 = 5^{2k+2} - 1 - 24 =$

$= 5^{2(k+1)} - 1 - 24 = 24.q \; x \; (25) \Rightarrow 5^{2(k+1)} - 1 = 24.q \; x \; (25) + 24 =$

$24(25q + 1) = 24q' \Rightarrow 5^{2(k+1)} - 1 = 24.q'$

3.9.8 Demonstre que $\forall n \in$ N, o número $5^n + 2.11^n$ é divisível por 3.

(i) Para $k = 1$, a desigualdade $5^1 + 2.11^2 = 5 + 2.11 = 27$ é verdadeira.

(ii) Hipótese: consideremos que $5^k + 2.11^k = 3.q$ é verdadeiro para $n = k$.

Tese: $5^{k+1} + 2.11^{k+1} = 3.q'$

$5^{k+1} + 2.11^{k+1} = 3.q' \Rightarrow 5^k.5 + 2.11^k.11 = 5^k.(3+2) + 2.11^k.(9+2) =$

$= 5^k.3 + 5^k.2 + 2.11^k.9 + 2.11^k.2 = 2.(5^k + 2.11^k) + 3.5^k + 2.9.11^k =$

$= \underbrace{2.(5^k + 2.11^k)}_{\text{hipótese}} + \underbrace{3.(5^k + 2.3.11^k)}_{\text{múltiplo de 3}}$, logo $5^{k+1} + 2.11^{k+1} = 3.q'$

3.9.9 Prove por indução matemática que $n^2 < 2^n$, para todos inteiros $n \geq 5$.

(i) Para $k = 5$, a desigualdade $5^2 < 2^5$ é verdadeira.

(ii) Hipótese: $k^2 < 2^k$ para $k \geq 5$.

Tese: $(k+1)^2 < 2^{(k+1)}$

$(k+1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1$ temos que $2k + 1 < 2^k$ para $k \geq 3$

Então $(k+1)^2 < 2^k + 2k + 1 < 2^k + 2^k = 2.2^k = 2^{k+1}$.

3.9.10 Prove a seguinte frase usando indução matemática:

- *Qualquer número inteiro positivo $n \geq 8$ pode ser escrito como a soma de 3's e 5's.*

(i) Para n = 8 $\Rightarrow$ 3 + 5 = 8 é verdadeiro.

(ii) Hipótese: considere verdadeira para $n = k = 3.a + 5.b$

Tese: $k + 1 = 3.a + 5.b$

Dois casos a considerar para k + 1:
(1) b≠ 0: É possível substituir um 5 por dois 3's quando é feita a soma de:
k + 1 = 3a + 5b + 1 = 3a + 5(b – 1) + 5 + 1 = 3a + 2.3 + 5(b – 1) = 3a' + 5b'
(2) b = 0: Neste caso, deve haver pelo menos três 3's para termos valores de n ≥ 9. Assim, temos: k + 1 = 3a + 1 = 3(a – 3) + 3.3 + 1 = 3a' + 2.5 = 3a' + 5b'.

6.2 - Capitulo 4

4.4.3 n não pode ser par pois n = 2k, teríamos n + 2 = 2k + 2 = 2(k + 1) é par, portanto, não primo. Assim, n, n + 2 e n + 4 são três ímpares consecutivos. Para n = 3, n + 2 = 5 e n + 4 = 7. 3, 5 e 7 são três primos consecutivos.

4.4.4 O número $2^{(2^{2004}+2)}+1$ é equivalente a $4^{(2^{2003}+1)}+1$.

Como toda potência de 2 é par então $2^{2003}+1$ será ímpar.

Como 4 elevado a um número ímpar dá um número cujo último algarismo é 4, então $4^{(2^{2003}+1)}+1$ terá 5 como último algarismo.

Como todo número que termina com 5 é múltiplo de 5 então o número $2^{(2^{2004}+2)}+1$ será múltiplo de 5 e poderá ser escrito como $5x$, com x maior do que 1, o que prova que $2^{(2^{2004}+2)}+1$ é composto.

4.4.6 Decompondo $20.21^m = 2^2.5.(3.7)^m = 2^2.3^m.5.7^m$, o número de divisores é dado por:

$D(N) = (2+1).(m+1).(1+1).(m+1) = 96 \rightarrow 3.(m+1).2.(m+1) = 6.(m+1)^2 = 96 \rightarrow (m+1)^2 = 16$

$m+1 = \pm 4 \rightarrow m = 4 - 1 = 3$ ou $m = -4 - 1 = -5$, mas como $m \in N$ a resposta será m = 3.

4.4.7 $N = 12^{2012} + 2012^{12} = (3.4)^{2012} + (4.503)^{12} = 3^{2012}.4^{2012} + 4^{12}.503^{12} =$

$= 4^{12}[(3^{2012}.4^{2000}) + 503^{12}] = 2^{24}[(3^{2012}.4^{2000}) + 503^{12}]$. Logo $2^n = 2^{24}$ temos n = 24.

Letra (D).

4.4.8 Temos x.6.12 = y.9.12, ou seja, $x.2.3.3.4 = y.3.3.3.4 \Rightarrow 2^3.3^2.x = 2^2.3^3.y$. Observe o que falta em cada lado para igualdade um x = 3 e um y = 2, logo x + y = 5.

4.4.9 Ache os possíveis valores de n, $m \in N \cup \{0\}$ de modo que o número $9^m.10^n$ tenha:

a) 27 divisores positivos

$9^m.10^n = (3^2)^m.(2.5)^n = 2^n.3^{2n}.5^n \Rightarrow D = (n+1).(2m+1).(n+1) = (n+1)^2.(2m+1) = 27$

1ª possibilidade: $(n+1)^2 = 9$ e $2m+1=3$ teremos n = 2 e m = 1

2ª possibilidade: $(n+1)^2 = 1$ e $2m+1=27$ teremos n = 0 e m = 13

b) 243 divisores positivos

$9^m.10^n = (3^2)^m.(2.5)^n = 2^n.3^{2n}.5^n \Rightarrow D = (n+1).(2m+1).(n+1) = (n+1)^2.(2m+1) = 243$

1ª possibilidade: $(n+1)^2 = 81$ e $2m+1=3$ teremos n = 8 e m = 1

2ª possibilidade: $(n+1)^2 = 9$ e $2m+1=27$ teremos $n = 2$ e $m = 13$

3ª possibilidade: $(n+1)^2 = 1$ e $2m+1=243$ teremos $n = 0$ e $m = 121$

6.3 - Capitulo 5

5.3.5 Demostre $31|20^{15} - 1$.

$$20 \equiv -11(\mathrm{mod}\,31) \rightarrow 20^2 \equiv 121(\mathrm{mod}\,31) \rightarrow 20^2 \equiv -3(\mathrm{mod}\,31)$$

$$20.20^2 = 20^3 \equiv (-11).(-3) = 33 \equiv 2(\mathrm{mod}\,31)$$

$$20^{15} = (20^3)^5 \equiv 2^5(\mathrm{mod}\,31) \rightarrow 2^{15} \equiv 1(\mathrm{mod}\,31)$$

$$2^{15} - 1 \equiv 0(\mathrm{mod}\,31)$$

5.3.6 Se $a = (72)^6 + (72)^5 + 2$, mostre que $7|a$.

$72 \equiv 2(\mathrm{mod}\,7) \rightarrow 72^2 \equiv 4(\mathrm{mod}\,7) \rightarrow 72^3 \equiv 1(\mathrm{mod}\,7) \rightarrow 72^3.72^3 = 72^6 \equiv 1(\mathrm{mod}\,7)$

$72^3.72^2 = 72^5 \equiv 4(\mathrm{mod}\,7)$

$a = 72^6 + 72^5 + 2 \equiv 1 + 4 + 2 = 7 \equiv 0(\mathrm{mod}\,7)$

Logo 7|a.

5.3.7 Demonstre que $\forall n \in$ N, o número $n^3 + 5n$ é divisível por 6, utilizando congruência.

Temos:

$n \equiv 0(\mathrm{mod}\,6) \rightarrow n^2 \equiv 0(\mathrm{mod}\,6) \rightarrow n^3 \equiv 0(\mathrm{mod}\,6) \rightarrow 5n \equiv 0(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 0(\mathrm{mod}\,6)$

$n \equiv 1(\mathrm{mod}\,6) \rightarrow n^2 \equiv 1(\mathrm{mod}\,6) \rightarrow n^3 \equiv 1(\mathrm{mod}\,6) \rightarrow 5n \equiv 5(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 1 + 5 = 6 \equiv 0(\mathrm{mod}\,6)$

$n \equiv 2(\mathrm{mod}\,6) \rightarrow n^2 \equiv 4(\mathrm{mod}\,6) \rightarrow n^3 \equiv 2(\mathrm{mod}\,6) \rightarrow 5n \equiv 4(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 2 + 4 = 6 \equiv 0(\mathrm{mod}\,6)$

$n \equiv 3(\mathrm{mod}\,6) \rightarrow n^2 \equiv 3(\mathrm{mod}\,6) \rightarrow n^3 \equiv 3(\mathrm{mod}\,6) \rightarrow 5n \equiv 3(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 3 + 3 = 6 \equiv 0(\mathrm{mod}\,6)$

$n \equiv 4(\mathrm{mod}\,6) \rightarrow n^2 \equiv 4(\mathrm{mod}\,6) \rightarrow n^3 \equiv 4(\mathrm{mod}\,6) \rightarrow 5n \equiv 2(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 4 + 2 = 6 \equiv 0(\mathrm{mod}\,6)$

$n \equiv 5(\mathrm{mod}\,6) \rightarrow n^2 \equiv 1(\mathrm{mod}\,6) \rightarrow n^3 \equiv 5(\mathrm{mod}\,6) \rightarrow 5n \equiv 1(\mathrm{mod}\,6) \rightarrow n^3 + 5n \equiv 5 + 1 = 6 \equiv 0(\mathrm{mod}\,6)$

Logo $n^3 + 5n$ é divisível por 6

5.3.8 Mostre que o número $43^{101} + 23^{101}$ é divisível por 66.

Como 66 = 6x11 verifiquemos

$43 \equiv 1(\mathrm{mod}\,6) \rightarrow 23 \equiv -1(\mathrm{mod}\,6) \rightarrow 43^{101} \equiv 1^{101} = 1(\mathrm{mod}\,6) \rightarrow 23^{101} \equiv (-1)^{101} = -1(\mathrm{mod}\,6) \rightarrow$

$43^{101} + 23^{101} \equiv 1 + (-1) = 0(\mathrm{mod}\,6)$

O que mostra que $43^{101} + 23^{101}$ é divisível por 6. Faremos o mesmo com 11.

$43 \equiv -1(\mathrm{mod}\,11) \rightarrow 23 \equiv 1(\mathrm{mod}\,11) \rightarrow 43^{101} \equiv (-1)^{101} = -1(\mathrm{mod}\,11) \rightarrow 23^{101} \equiv 1^{101} = 1(\mathrm{mod}\,11) \rightarrow$

$43^{101} + 23^{101} \equiv -1 + 1 = 0(\mathrm{mod}\,11)$

O que mostra que $43^{101} + 23^{101}$ é divisível por 11. Logo é divisível por 66.

5.3.9 Temos $m \equiv 3\ (\mathrm{mod}11)$, $n \equiv 4\ (\mathrm{mod}11)$ e $p \equiv 5\ (\mathrm{mod}11)$, o resto da divisão de

$m + n + p \equiv 3+4+5=12 \equiv 1\ (\mathrm{mod}11)$. Letra d) 1

7. CONSIDERAÇÕES FINAIS

Avaliando as pesquisas com os professores tanto no Rio de Janiro como no Pará, verificamos que a totalidade dos docentes apontam que os alunos do ensino médio têm dificuldade em assuntos de aritmética, fato que também verificado por mim e pelo professor Silvio. A falta de compreensão dos alunos em situações de ensino aprendizagem em aritmética faz com que muitos deles acreditem que a matemática é difícil e em grande parte inútil. É nesse contexto que estamos trazendo essa proposta de inclusão dos assuntos citados, afim reforçar o conhecimento numa área básica para compreensão de toda a matemática que é a Teoria dos Números.

Outro fato observado durante a montagem deste trabalho é que conversando com alguns professores de matemática muitos, onde me incluo, não tiveram a matéria de aritmética durante a formação que acho de suma importância, o que reforça a proposta deste, pois com a inclusão do conteúdo no ensino médio fará que as faculdades reformulem suas grades incluindo também a aritmética.

Este trabalho aponta ainda para a possibilidade de inserir os conceitos congruência Ensino Básico, pois além de aprofundar o significado do resto e manipulá-lo, os alunos ganham uma ferramenta importante em aplicações de outros assuntos; por exemplo, no ensino médio, no momento em que se estuda arcos côngruos, nas potências naturais do número complexo i e em divisão de polinômios promovendo assim uma conexão entre temas matemáticos.

Os resultados deste estudo assinalam que, mediante a escolha adequada dos conteúdos e da metodologia de ensino, o estudo de assuntos inerentes à teoria dos números, neste caso indução matemática, teorema fundamental da aritmética e congruências pode contribuir para a promoção do pensamento aritmético e algébrico à medida que favorece o desenvolvimento de competências e habilidades, como formular e validar conjecturas, representar e analisar situações matemáticas e estruturas usando símbolos algébricos; produzir modelos para representar e expressar uma situação-problema; desenvolver algum tipo de generalização; realizar demonstração de regularidades ou invariâncias e desenvolver e elaborar uma linguagem mais concisa e precisa ao expressar-se matematicamente.

Finalmente, baseado em nossa pesquisa, que apontou que o melhor momento para serem inseridos, como apontou quase 60% docentes do Rio de Janeiro e

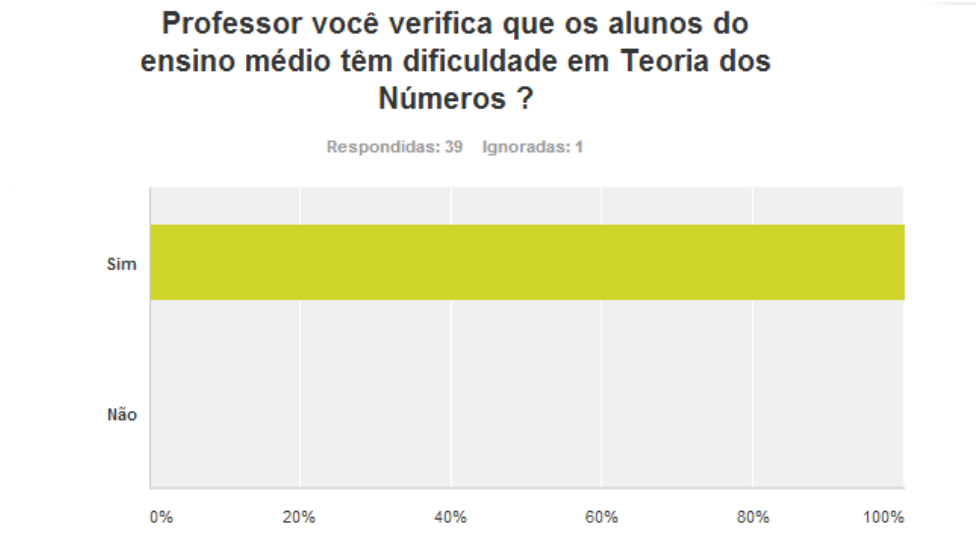
aproximadamente 67% no Pará, será na 1ª série do Ensino Médio, momento em que trabalhamos os conjuntos numéricos e dentro desse contexto cabe reforçarmos a Teoria dos Números, dando uma base para os demais assuntos. Esperamos que os trabalhos apresentados por mim e pelo Prof Silvio Freitas juntamente com nossas referências sirvam de base para uma mudança no currículo do Ensino Médio e para contribuir a melhora do conhecimento matemático e do raciocínio lógico dedutivo de nossos alunos, preparando-os para os cursos de graduação e para vida.

ANEXO A

Pesquisa sobre o ensino da aritmética no ensino médio – Rio de Janeiro - RJ.

1 – Professor você verifica que os alunos do ensino médio tem dificuldade em assuntos de aritmética?

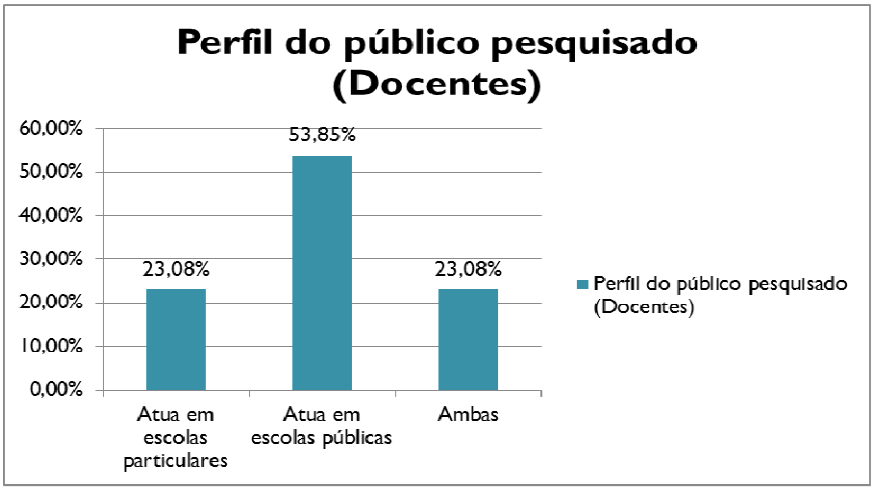
( ) Sim ( ) Não



Opções de resposta	Respostas	
Sim	100%	39
Não	0%	0
Total		39

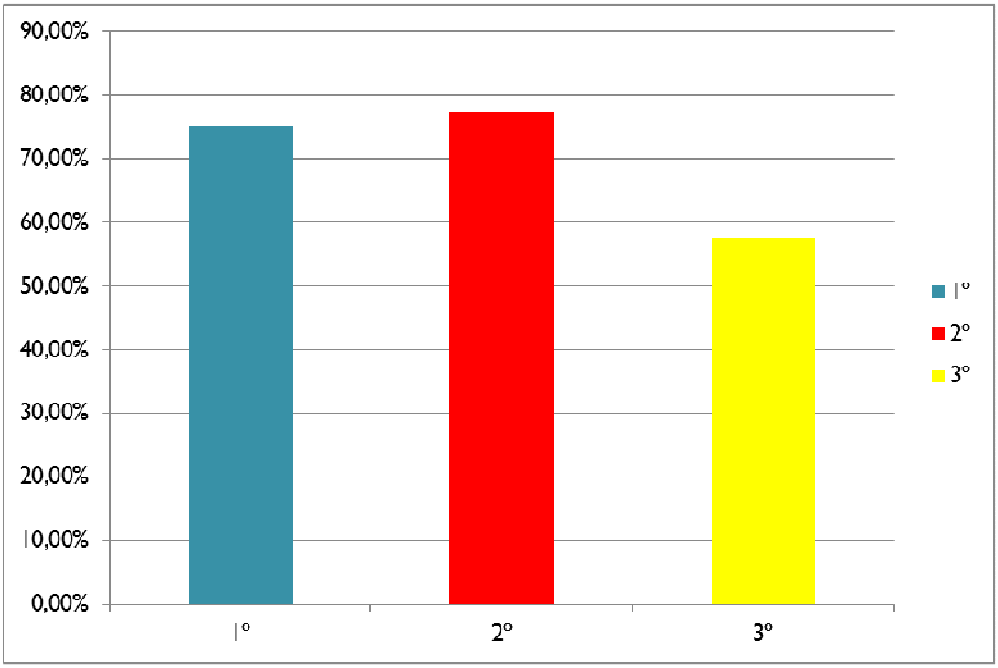
2 – Você trabalha com turmas do ensino médio da rede pública, escola particular ou ambas?

( ) Rede Pública ( ) Escola Particular ( ) Ambas

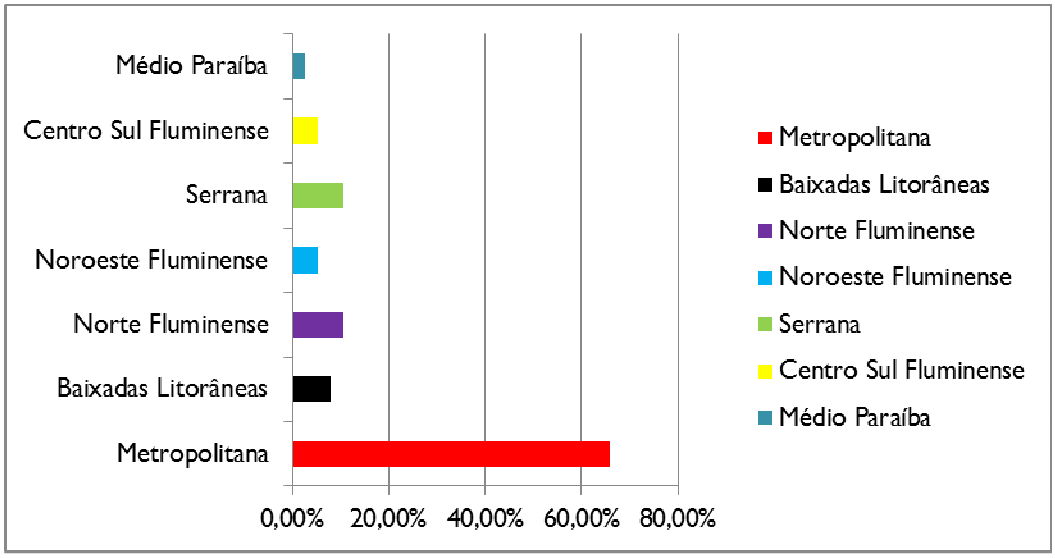


3 – Quais as séries que trabalha?

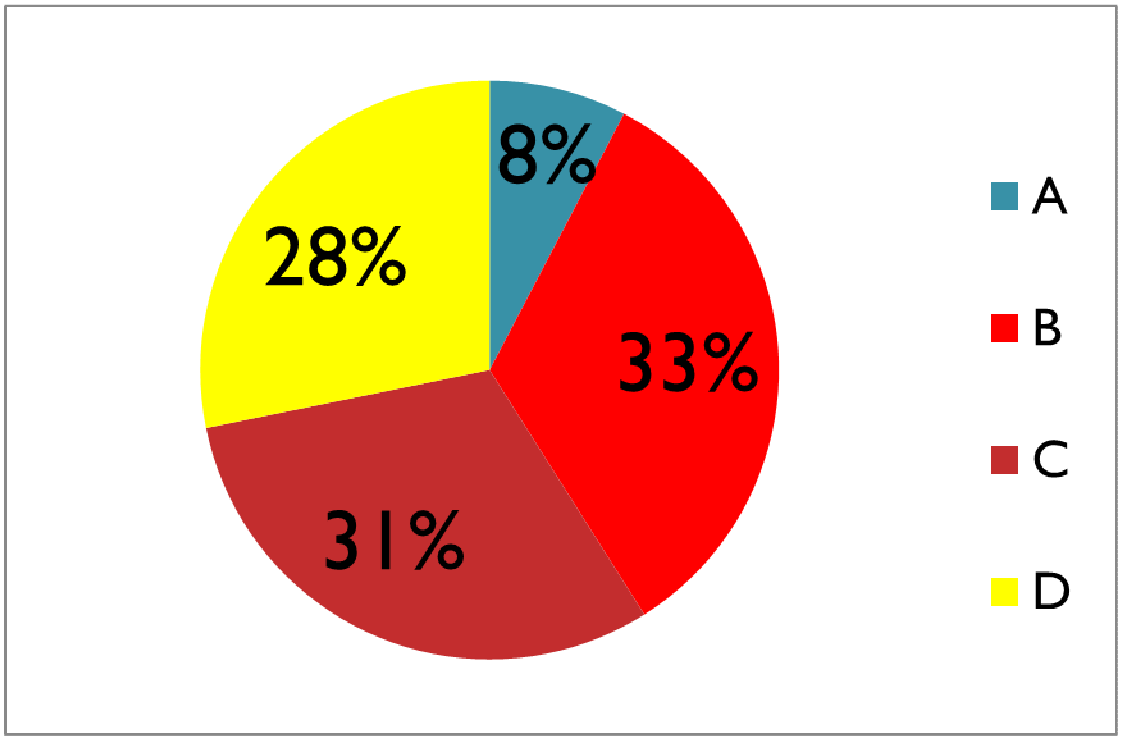
( ) 1º Ano EM ( ) 2º Ano EM ( ) 3º Ano EM ( ) Outros (Especifique)



4 – A escola que trabalha fica localizada.....(Explicitar local e tipo de público, exemplo periferia, região metropolitana)



5 – Qual a classe social dos discentes?



6 – Você aceitaria aplicar um teste experimental sobre aritmética em suas turmas.

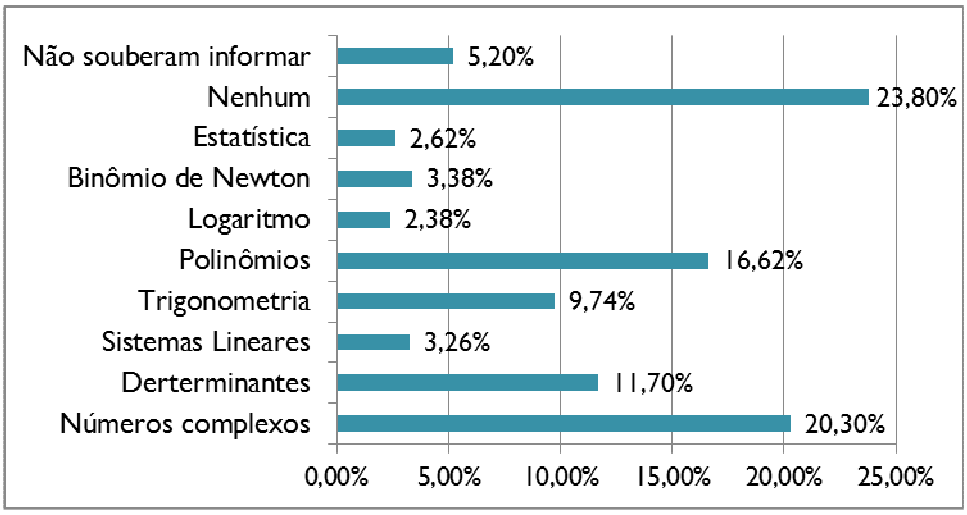
( ) Sim ( ) Não

Perguntados sobre: Aplicaria uma avaliação experimental sobre aritmética?	
Sim	95%
Não	5%

7. Em que série(s)?

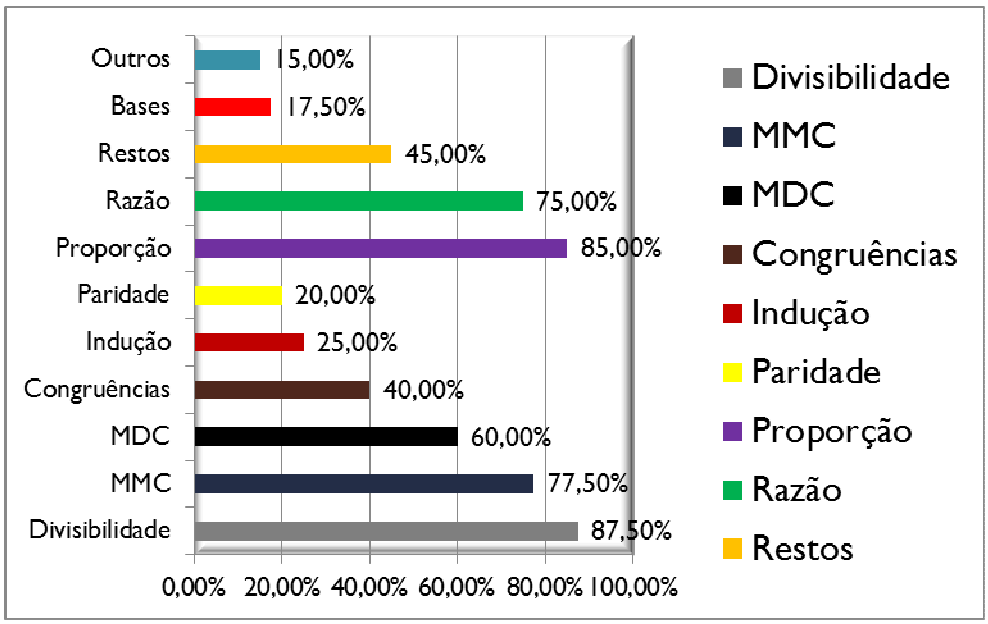
Se fosse acrescentar algum tópico mencionado anteriormente, em qual das séries incluiria o assunto?	
1ª	59,46%
2ª	27,03%
3ª	35,14%

8. Qual (ou quais) assunto(s) pode(riam) dar lugar aos conteúdos de aritmética a serem inseridos no ensino médio?



9. Entre os assuntos abaixo marque qual (ou quais) é (ou são) o(s) mais importante(s) que os alunos deve(m) ter domínio na aritmética?

( ) divisibilidade ( ) MMC e MDC ( ) congruências ( ) indução ( ) paridade
( ) proporção ( ) Razão ( ) Restos ( ) Bases ( ) Outros



ANEXO B

Pesquisa sobre o ensino da aritmética no ensino médio – Belém - PA.

1 – Professor você verifica que os alunos do ensino médio tem dificuldade em assuntos de aritmética?

( ) Sim ( ) Não

Os discentes apresentam alguma dificuldade em assuntos relacionados a aritmética?	
Sim	100%
Não	0%

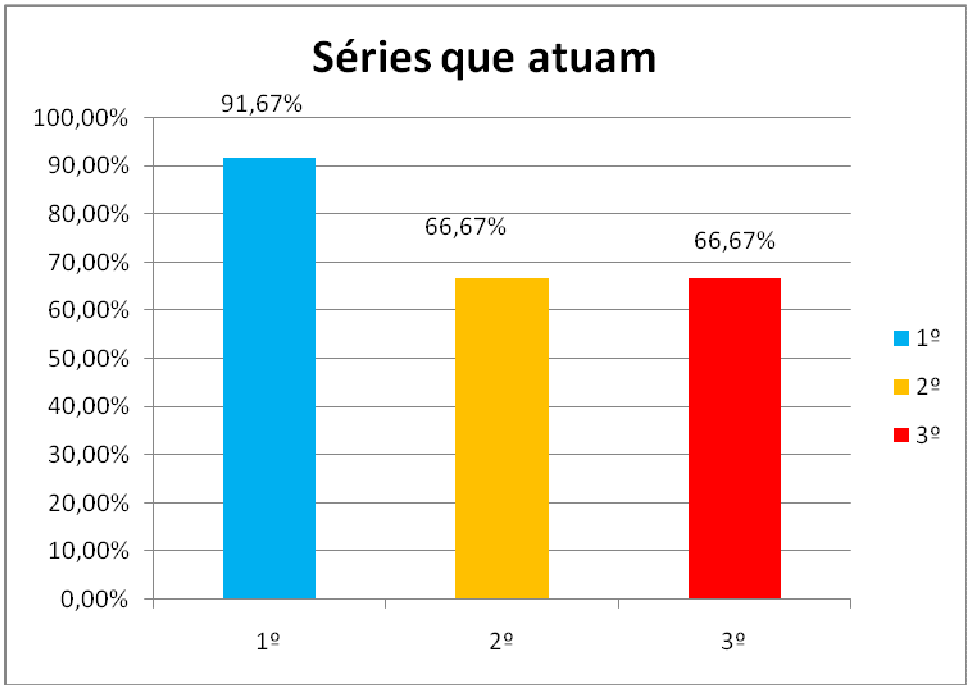
2 – Você trabalha com turmas do ensino médio da rede pública, escola particular ou ambas?

( ) Rede Pública ( ) Escola Particular ( ) Ambas

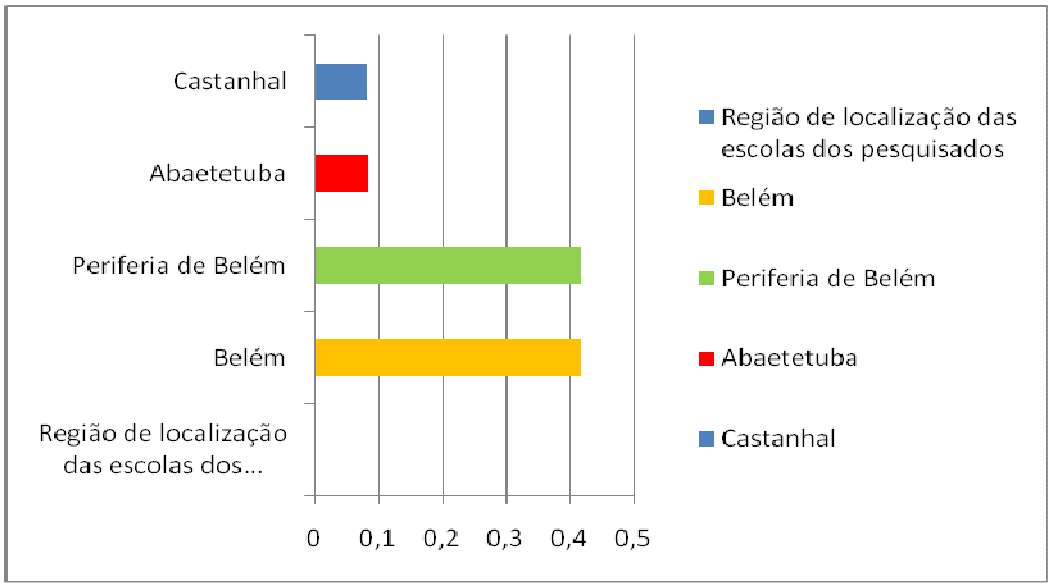
Perfil do público pesquisado (Docentes)	
Atua em escolas particulares	16,67%
Atua em escolas públicas	58,33%
Ambas	25,00%

3 – Quais as séries que trabalha?

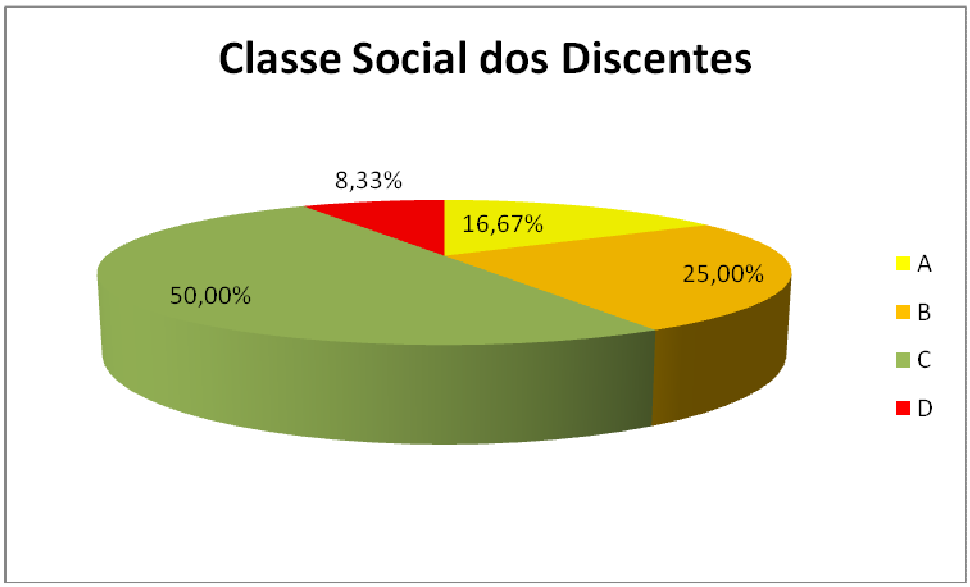
( ) 1º Ano EM ( ) 2º Ano EM ( ) 3º Ano EM ( ) Outros (Especifique)



4 – A escola que trabalha fica localizada.....(Explicitar local e tipo de público, exemplo periferia, região metropolitana)



5 – Qual a classe social dos discentes?



6 – Você aceitaria aplicar um teste experimental sobre aritmética em suas turmas.

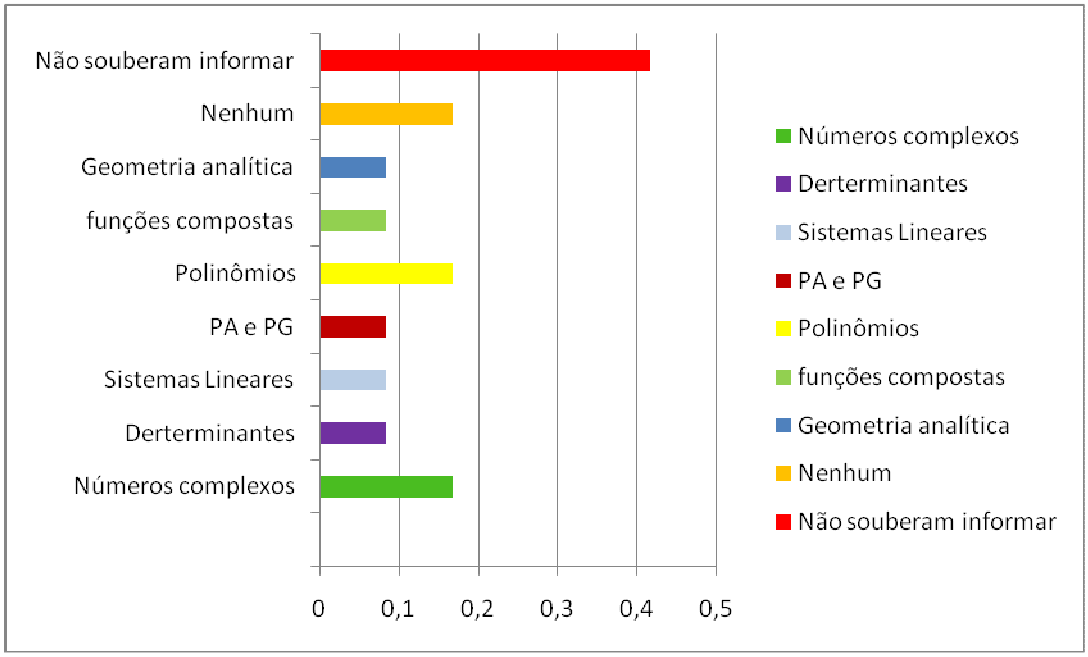
( ) Sim ( ) Não

Perguntados sobre: Aplicaria uma avaliação experimental sobre aritmética?	
Sim	75,00%
Não	25,00%

7. Em que série(s)?

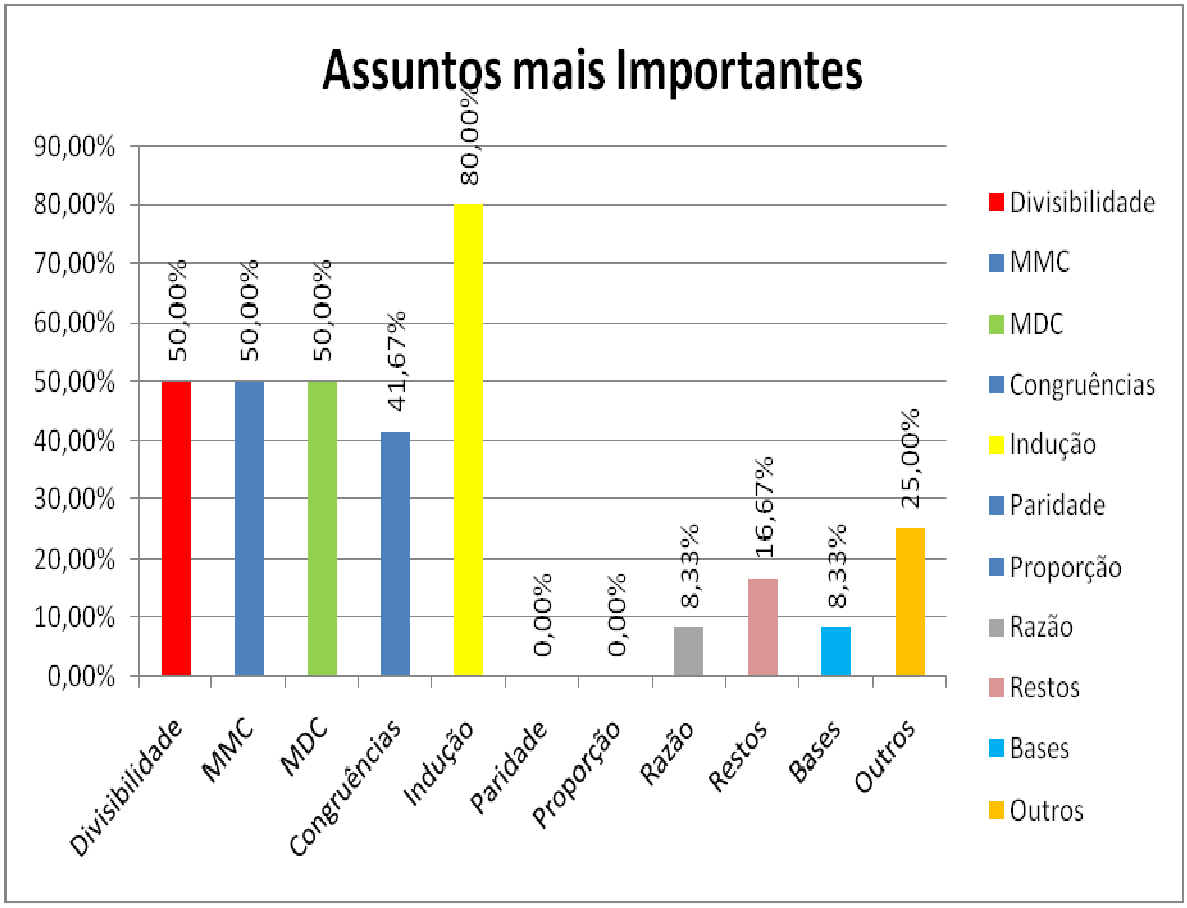
Se fosse acrescentar algum tópico mencionado anteriormente, em qual das séries incluiria o assunto?	
1ª	66,67%
2ª	16,67%
3ª	0,00%

8. Qual (ou quais) assunto(s) pode(riam) dar lugar aos conteúdos de aritmética a serem inseridos no ensino médio?



9. Entre os assuntos abaixo marque qual (ou quais) é (ou são) o(s) mais importante(s) que os alunos deve(m) ter domínio na aritmética?

( ) divisibilidade ( ) MMC e MDC ( ) congruências ( ) indução ( ) paridade
( ) proporção ( ) Razão ( ) Restos ( ) Bases ( ) Outros


Assuntos mais Importantes
90,00%
80,00%
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
50,00%
50,00%
50,00%
41,67%
80,00%
0,00%
0,00%
8,33%
16,67%
8,33%
25,00%
Divisibilidade
MMC
MDC
Congruências
Indução
Paridade
Proporção
Razão
Restos
Bases
Outros

BIBLIOGRAFIA

[1] FREITAS, Ricardo Luiz Queiroz, Tópicos de Álgebra, 1ª edição, FTC – EAD - SOMESB

[2] HEFEZ, A. – Elementos de Aritmética; SBM, 2011.

[3] HEFEZ, Abramo. Introdução a Aritmética, PIC, 2011.

[4] LIMA, E. L. - Artigo: O PRINCÍPIO DA INDUÇÃO – Revista Eureka. (www.obm.org.br/export/sites/default/revista_eureka/.../inducao.doc) Acesso em 06 jan 14.

[5] LIMA, e. L.; CARVALHO, P. C.P.; WAGNER, E. E MORGADO, A. C.. A Matemática no Ensino Médio, 6ª edição, 2004 – SBM.

[6] LINS, Romulo Campos e GIMENEZ, Joaquim, Perspectivas em Aritmética e Álgebra para o Século XXI – 7ª edição (1997) – SBEM – Papirus.

[7] MOREIRA, C. G. de Araújo, Teoria dos números um passeio com primos e outros números familiares pelo mundo inteiro. 15-26 2° Ed. (2013) –Projeto Euclides.

[8] MOREIRA, C. G., Curso de Teoria dos Números - Polos Olímpicos de Treinamento.

[9] NETO, Aref Antar [et al]. Progressões e Logaritmos - Noções de Matemática vol 2. Editora Moderna

[10] OLIVEIRA, Krerley Irraciel Martins Oliveira e FERNÁNDEZ, Adán José Corcho. Iniciação à Matemática: um curso com problemas e soluções, 2ª edição, SBM, SBM

[11] RPM nº 82 e OBMEP Edição Especial.

[12] SANTOS, Graça Luzia Dominguez - Aspectos da Indução, nas Ciências e na Matemática - Departamento de Matemática - Universidade Federal da Bahia;

[13] http://pt.wikipedia.org/wiki/Indu%C3%A7%C3%A3o_matem%C3%A1tica.

[14] http://www.brasilescola.com/matematica/numeros-primos.htm.

[15] http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf .