Matemática

Introdução à Teoria dos Números

Francisco César Aires

2ª Edição

Fortaleza
2019

Geografia

História

Educação Física

Química

Ciências Biológicas

Artes Plásticas

Computação

Física

Matemática

Pedagogia

Editora Filiada à

ASSOCIAÇÃO BRASILEIRA DAS EDITORAS UNIVERSITÁRIAS

Dados Internacionais de Catalogação na Publicação
Sistema de Bibliotecas
Biblioteca Central Prof. Antônio Martins Filho
Thelma Marylanda Silva de Melo – CRB-3 / 623
Bibliotecária

A98i Aires, Francisco César.
Introdução à teoria dos números / Francisco César Aires.
2. ed. Fortaleza : EdUECE, 2015.
70 p. ; il. (Matemática)

ISBN: 978-85-7826-397-3

1. Teoria dos números. I. Título.

CDD: 52.7

Editora da Universidade Estadual do Ceará – EdUECE
Av. Dr. Silas Munguba, 1700 – Campus do Itaperi – Reitoria – Fortaleza – Ceará
CEP: 60714-903 – Fone: (85) 3101-9893
Internet: www.uece.br – E-mail: eduece@uece.br

Secretaria de Apoio às Tecnologias Educacionais
Fone: (85) 3101-9962

Sumário

Apresentação

Os números fascinam e estão presentes na vida do homem a vários séculos, sendo talvez uma das ideias mais marcantes da humanidade, pois estavam presentes no florear de todas as civilizações. "O conceito de número inteiro é o mais antigo na matemática e sua origem não se pode precisar na história da Matemática.

Mas afinal o que é um número ? Número é uma ideia abstrata de quantidade. Exemplifico: Existem mais cabelos na cabeça de uma pessoa do que os dedos de suas mãos. Sem contarmos a quantidade de cabelos, afirmamos que esta é maior que o número de dedos, isto é, as quantidades de cabelos e de dedos são exemplos de números.

O homem para chegar ao número criou inicialmente a contagem, que auxilia na percepção das quantidades. Portanto, contagem é uma sequencia que associa cada elemento de uma coleção a um único elemento de outra. A oito mil anos a.C ocorreu a história do pastor e suas ovelhas: pela manhã, ao saírem as ovelhas do cercado, o pastor colocava uma pedra de lado para cada animal que passava na porteira, formando um monte de pedras. No fim do dia, o pastor retirava do monte uma pedra para cada ovelha que retornava para o cercado. Se faltassem pedras, o pastor sabia que o número de ovelhas havia aumentado e se sobrassem, o pastor sabia que algumas ovelhas haviam ficado para trás e sairia para procurá-las.

No leste europeu foi achado um osso de lobo com profundas incisões em número de cinquenta e cinco. Estavam dispostos em duas séries, com vinte e cinco numa e trinta na outra, com riscos em cada série dispostos em grupos de cinco. Note que o homem primitivo criou agrupamentos dentro do próprio processo de contagem, isto é, formou grupos menores e passou a contar os grupos. Nasce a base de contagem. Foram encontradas nas civilizações antigas as seguintes bases:

- Grupo de 2 (base binária)
- Grupo de 3 (base ternária)
- Grupo de 5 (base quinária)
- Grupo de 10 (base decimal)
- Grupo de 20 (base vigesimal)
- Grupo de 60 (base sexagesimal)

Mais adiante o homem civilizado criou os símbolos para representar os números e assim aperfeiçoou cada vez mais a forma de contagem. Modernamente chamamos de algarismos os símbolos que combinamos para a formação dos números. Exemplifico: 344 é o número trezentos e quarenta e quatro e possui três algarismos. A forma de se escrever por extenso os números nasceu no século III com os astrônomos e matemáticos indianos. Hoje, a palavra dígito, originária do latim e que significa dedo, é usada para indicar qualquer dos algarismos de 0 a 9.

A Índia é um país que ocupa uma extensa região da Ásia, entre o oceano Índico e a cordilheira do Himalaia, banhada pelos rios Indo e Ganges. Essa civilização indiana criou o nosso sistema de numeração, que é sem dúvida, uma das criações mais importantes no desenvolvimento das ciências.

Os matemáticos indianos sabiam que 3 dezenas e 1 unidade é diferente de 3 centenas e 1 unidade. Mas como registrar esses símbolos? Foi quando um desconhecido hindu, no século V, teve a ideia de criar um símbolo para representar o NADA. Esse símbolo era o ponto e a palavra era sunya (vazio). Então aqueles dois números anteriores eram representados assim:

1 3	1.3
(10+3)	(100 + 3)

pois os hindus escreviam os números começando pela esquerda. Estava criado o zero, significando ausência da unidade, ou dezena, etc, isto é, o zero tornou-se um algarismo, instrumento de grande importância como base da contagem.

O Autor.

Capítulo 1

História dos Números

Objetivos

- Conhecer um pouco da História dos números.
- Apresentar os números na Grécia Antiga.

Introdução

Apesar de termos falado na apresentação deste livro sobre a história dos números, dedicamos este primeiro capítulo ao conhecimento de mais um pouco dessa história, visto que os números são o objetivo maior desse texto. As grandes civilizações que povoaram a história da humanidade tiveram seus pensadores ou filósofos que nos deixaram alguma contribuição no que diz respeito aos números.

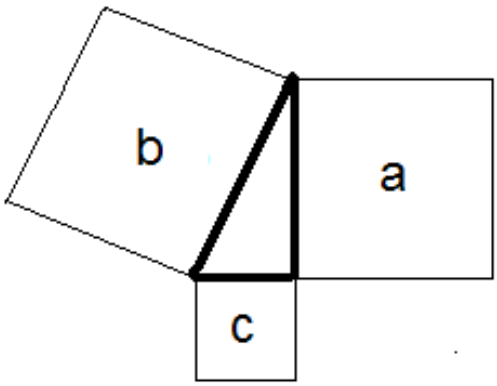
1. Surgimento e evolução da Teoria dos Números

No quarto milênio a.C existiram duas civilizações brilhantes. A Mesopotâmia (Território pertencente hoje ao Irã) banhada pelos rios Tigre e Eufrates foi sempre uma região muito conturbada por guerras entre seus habitantes. Os Sumérios, que inventaram a escrita por volta de 3.500 a. C, construíram casas decoradas com cerâmicas e mosaicos com desenhos geométricos. Acredita-se que depois da invenção da escrita, foram criadas as primeiras escolas, para treinar escribas para trabalhos comerciais e governamentais. O sistema de numeração dos Sumérios usava como base o número 60, que originou a convenção até hoje de dividir o círculo em 360°, a hora em 60 minutos e o minuto em 60 segundos.

Os Sumérios foram conquistados pelos Acádios, que se estabeleceram na cidade de Ur, que poucos séculos depois foram conquistados pelos Elamitas que destruíram Ur e a Suméria. Por volta de 1.800 a.C, os Elamitas foram conquistados pelos Amoritas, que fizeram da Babilônia sua capital. O rei Hamurabi (1.700 a. C?) cria o primeiro código de leis (Dente por dente, olho por olho) e eleva a Babilônia a uma posição importante na região.

A Mesopotâmia, que desenvolveu um sistema de escrita na forma de cunha feita com estilete em placas de argila, cosidas em fornos ou sol (cuneiformes), também nos deixou muitas informações sobre a matemática daquele período. Em 1870 descobriu-se a pedra behistein que trazia uma narração trilingue (Persa, Elamítico, Babilônica) que continha entre outras informações:

- a noção do zero como vazio
- um valor aproximado de raiz quadrada de dois, $\sqrt{2} = 1{,}414222$
- a área do quadrado,
- o volume do tronco de cone
- formas de fatoração e a figura



Do Egito, país que fica na África banhado pelo rio Nilo, sede de uma das civilizações mais antigas, herdamos a divisão do dia em 24 horas. Em 1799 uma expedição de Napoleão descobriu a pedra de rosetta com narração trilingue (Grego, Demótica, Hieroglífica) que continha

- numeração de base 10
- cálculo preciso das pirâmides
- astronomia relacionada com as enchentes do rio Nilo
- calendário
- área do triângulo isósceles e do círculo.

Outras importantes descobertas na antiguidade foram o papiro de Moscou (1.850 a. C) que continha 25 problemas resolvidos de aritmética e geometria e o papiro Ahmes (1.600 a. C) , descoberto no século XX pelo escocês Henry Rhind que contém 85 problemas de aritmética e geometria.

Os Babilônios e Egípcios construíram, ao longo de suas histórias um acúmulo matemático significativo, mas totalmente desprovido de conceitos teóricos, deduções lógicas e muito menos de abstração

1.2 O Milagre Grego

A partir do século VI a. C. s civilizações Mesopotâmica e Egípcia começaram a entrar em dclínio, e foi quando os gregos chamados helenos (antigos antepassados) começaram a dominar a região mediterrânea. A Grécia está situada entre os mares Egeu e Jônio e muitos viajantes de origem Mesopotâmica e Egípcia chegaram às colônias gregas devido às atividades comerciais, como também os gregos viajaram bastante para a Mesopotâmia e o Egito. Nesse período os gregos usando a razão, mas sem desprezar a experimentação e a observação, tiveram uma atitude ousada, desenvolvendo a abstração e o raciocínio lógico.

Na cidade de Mileto (Território pertencente a atual Turquia) viveu um homem admirável chamado Tales de Mileto (624 a. C – 548 a. C ?) que foi discípulo dos egípcios. É considerado o primeiro matemático e o primeiro filósofo da humanidade. Para Tales "A água era o princípio fundamental de todas as coisas" e a frase "Conhece a ti mesmo" é também de Tales. Em 585 a. C. Tales assombrou seus contemporâneos ao predizer um eclipse.

Pouco se sabe sobre a vida e a obra de Tales. Sua atividade rotineira era o comércio. O filósofo grego Aristóteles (384 a. C – 322 a. C) relata a fortuna de Tales no monopólio de prensas de azeite e mercado de sal. Por ser discípulo dos egípcios, fez varias viagens para aquele país visitando as pirâmides. Medindo a sombra da pirâmide de Quéops e de um bastão que plantara verticalmente na areia, calculou a altura da pirâmide, com o uso de proporção.

Daí, seu interesse pela geometria (medida da Terra). Tales foi o primeiro individuo da história a formular algumas propriedades gerais sobre figuras geométricas. Por exemplo : "dois ângulos opostos pelo vértice são iguais". "Qualquer diâmetro divide o círculo em duas partes iguais". "Qualquer ângulo inscrito em um semi-círculo é reto". "No triângulo isósceles, os ângulos da base são iguais". Mas não foi com Tales que a matemática atingiu a abstração e as deduções lógicas.

A cerca de 50 km de Mileto, na ilha de Samos, nasceu o homem que empresta seu nome ao mais conhecido de todos os teoremas da matemática – Pitágoras (580 a. C – 500 a. C?) contemporâneo de Buda e Confúcio, fez várias viagens à Mesopotâmia, ao Egito e à Índia, É difícil separar história e lenda no que se refere ao homem, pois Pitágoras representa tantas coisas para o povo – filósofo, profeta, astrônomo, matemático, santo, abominador de feijões, místico, milagreiro, charlatão, mágico. O certo é que Pitágoras desenvolveu a ideia da lógica numérica e a abstração e foi responsável pela primeira idade de ouro da matemática.

Em 520 a. C. Pitágoras deixa sua terra por detestar o tirano Policrates que governava Samos indo para o sul da Itália e se estabelece em Crotona, onde

conheceu o patrono Milo. Milo era o homem mais rico de Crotona e um dos homens mais fortes de toda a história. Era um homem de proporções hercúleas, que fora doze vezes campeão nos jogos olímpicos. Um recorde. Em seu novo lar, funda por volta de 540 a. C, a Irmandade pitagórica, um grupo de aproximadamente seiscentos seguidores ou discípulos, capazes não apenas de entender seus ensinamentos, mas também de contribuir criando idéias novas e demostrações. Cada membro da Irmandade era forçado a jurar que nunca revelaria ao mundo exterior qualquer uma de suas descobertas matemáticas.

A estudante favorita de Pitágoras era a filha de Milo, a bela Teano, que apesar da diferença de idade, os dois se casaram. Logo depois de fundar a irmandade, Pitágoras criou a palavra Filósofo (Amante da sabedoria e da reflexão). Era norma da Irmandade atribuir todas as descobertas realizadas por seus membros ao chefe, daí não se pode discernir entre as contribuições de Pitágoras e as de seus seguidores ou discípulos.

A irmandade pitagórica tornou-se muito poderosa, mística, influente em Crotona e acabou se envolvendo na política local. Cilon, um dos rejeitados da Irmandade, surgiu como porta- voz do povo e liderou uma rebelião de sua população que temia que as terras fossem doadas para a elite pitagórica, alimentando a paranóia e a inveja na multidão contra a escola.O mesmo Cilon liderou um ataque para destruir a mais brilhante escola de matemática que o mundo já vira. Cercada, todas as portas trancadas e bloqueadas, a escola foi incendiada. Pitágoras, sua bela esposa Teano morreram como muitos dos seus discípulos. A humanidade havia perdido o pai da Matemática, mas o espírito pitagórico permaneceu. Os números e suas verdades eram imortais.

"Tudo é número" era o lema da Irmandade Pitagórica. Consideravam deus o grande geômetra do universo e que o mundo era feito de números. O símbolo da irmandade era o pentágono e também conheciam o cubo, octaedro, dodecaedro. A descoberta do dodecaedro foi revelado publicamente por um membro da Irmandade, que quebrou o juramento e foi afogado. A irmandade era realmente uma comunidade religiosa e um de seus ideais era o número. Em especial, a irmandade voltou sua atenção para os números naturais (1, 2, 3,...) e entre a infinidade dos números, buscava alguns com significado especial.

- Números ímpares (masculinos)
- Números pares (feminino)
- Número um (gera os números, número da razão)
- Números dois (primeiro número par, número da opinião)
- Número três (primeiro número impar, número da harmonia)
- Número quatro (número de justiça)

- Número cinco (número do casamento, união do primeiro par com o primeiro ímpar)
- Número seis (número da criação)
- Número dez (número sagrado, universo)
- Números excessivos (quando a soma de seus divisores é mais do que ele)
- Números fracionários (proporções entre números inteiros)
- Números perfeitos (divisores somados produzem eles mesmos, com exceção do próprio número)
- Números amigos (dois números, se cada um deles é a soma dos divisores próprios do outro)

Como vemos, os Pitagóricos tratavam os números de uma maneira filosófica e abstrata. Também as proposição seguintes eram conhecidas por eles:

- A soma de dois números pares é par.
- O produto de dois números impares é impar.
- Quando um número ímpar divide um número par, também divide sua metade.

1.3. Infinidade de Trios

Depois da morte de Pitágoras e do ataque de Cilon, a irmandade partiu para outras cidades da Magna Grécia, estabeleceram novas escolas e ensinaram aos seus alunos os métodos da provas lógica, em particular, a prova do mais conhecido de todas os teoremas da matemática o Teorema de Pitágoras:

"Em todo triângulo retângulo de lados $a > b \geq c$ vale a igualdade $a^2 = b^2 + c^2$"

É uma lei universal. Também, entre outras coisas, os pitagóricos explicaram o segredo de encontrar trios pitagóricos, ou seja, três números inteiros a, b e c que se ajustam à equação de Pitágoras $a^2 = b^2 + c^2$.

Por exemplo, são trios pitagóricos,

$a = 5,\ b = 4$ e $c = 3$

$a = 13,\ b = 12$ e $c = 5$

$a = 17,\ b = 15$ e $c = 8$

$a = 4901,\ b = 4900$ e $c = 99$.

Para descobrir tantos trios quanto possível, os pitagóricos inventaram um método de encontrá-los e provaram que existe um número infinito deles.

Ao se trocar o expoente 2 da equação de Pitágoras por qualquer número natural $n \geq 3$, a busca de trios pitagóricos deixa de ser um problema

simples e se tornar um desafio. De fato, o grande matemático Francês Pierre de Fermat (1601 – 1665) afirmou que não existem trios para esta equação. Tal afirmação ficou conhecida como o Último Teorema de Fermat e estabelece que : "não existem valores inteiros positivos para a, bec que satisfaçam a equação $a^n = b^n + c^n$ para $n \geq 3$".

O Último Teorema de Fermat tornou-se um enigma que confundiu as maiores mentes do mundo durante 358 anos. Vidas inteiras foram devotadas à busca de uma prova para um problema que é aparentemente simples. Newton (1643 – 1727), Jacques Bernoulli (1654 - 1705), (*Nenhuma família na história da matemática produziu tantos matemáticos célebres quanto a família Bernoulli, cerca de 13 membros)*, Euler (1707 - 1783), Lagrange(1736 – 1813), Gauss (1777 – 1855), que afirmou "*a Teoria dos Números é a Rainha da Matemática*", Sophie Germain (1776 – 1831), Galois (1811 - 1832), Einstein (1879 - 1956) e muitos outros.

Mas em 1995, o matemático inglês Andrew Wiles ganhou as páginas de jornais do mundo inteiro e 50 mil libras da Fundação Wolfskenl ao demonstrar o maior problema de matemática de todos os tempos: O último Teorema de Fermat.

Síntese do Capítulo

Nesse primeiro capítulo fizemos um relato sucinto da história dos números, onde mencionamos a contribuição de povos como os babilônios, sumérios e egípcios, como também nomes como Tales e Pitágoras e outros expoentes da história da matemática.

Atividades de avaliação

1. Quais são, na sua opinião, as duas mais importantes deficiências na matemática Mesopotâmia? E Egípcia?

2. Dê exemplos de números excessivos, perfeitos e amigos.

Capítulo 2

Noções de Lógica

Objetivos

- Apresentar noções de lógica proposicional.
- Conhecer a definição de proposição e os principais tipos.

Introdução

Neste capítulo estudaremos um pouco de lógica. O objetivo desse estudo de noções de lógica antes de entrarmos no estudo da teoria dos números é para se familiarizar com os conceitos de proposição, composição de proposições, e outros conceitos que nos permitam entender o que é e diferenciar um teorema de um axioma ou de um corolário, muito presentes nos capítulos subsequentes.

1. Generalidades

Em matemática o conceito de prova ou demonstração é muito mais rigoroso e poderoso do que o conceito de prova entendido pelos físicos e químicos, por exemplo. Ela é crucial para entendermos o trabalho de cada matemático, desde Pitágoras. Para Pitágoras a ideia da prova matemática era sagrada. A prova é uma verdade mais profunda do que qualquer outra, por ser resultado de uma lógica impecável, desenvolvida passo a passo. Portanto a prova ou demonstração matemática é absoluta.

Entendemos por: Raciocínio, a forma mais complexa do pensamento.

Lógica é a coerência de raciocínio ou de ideias. Modo de raciocinio peculiar a alguém ou a um grupo.

Lógico é conforme a lógica

Posto isto, podemos ainda afirmar que a lógica é a ordem no pensamento.

Exemplo:

a) Se todos os amigos de Gregório são meus amigos e se todos os meus amigos são agradáveis então todos os amigos de Gregório são agradáveis.

b) Se nenhum amigo de Gregório é meu amigo e se nenhum amigo de Gregório é agradável então nenhum de meus amigos é agradável.

Quando a conclusão (então) de um argumento segue de duas premissas (proposições que servem de base a conclusões) então dizemos que o raciocínio é válido ou logicamente válido. É o caso do argumento do exemplo (a), enquanto que no exemplo (b) a conclusão pode até ser verdadeira mas não segue de sua relação com as premissas e neste caso dizemos que o raciocínio é inválido ou logicamente inválido. O raciocínio lógico é de fundamental importância para que se identifique, dentre os argumentos que se pretende utilizar, aqueles que são válidos e os que não o são.

2. Proposições

Proposição é uma proposta, ato de propor, asserção, expressão verbal de um juízo. Uma proposição deve ser como uma oração, que tem sentido completo com sujeito e predicado. Deve ser verdadeira ou falsa. Não pode ser ao mesmo tempo verdadeira e falsa. Deve ser declarativa, afirmativa.

O valor lógico de uma proposição é verdade (V) se a proposição é verdadeira e a falsidade (F) se a proposição é falsa.

Exemplos:

a) O número $\frac{1}{2}$ é inteiro.

b) Fortaleza é a capital do estado do Ceará e fica na região nordeste.

c) 1 + 1

O valor lógico proposição (a) é a falsidade (F) e o valor lógico da proposição (b) é a verdade (V). Em (c) não temos uma proposição, pois está faltando o predicado, isto é, não tem sentido completo.

2.1. Proposição simples

Uma proposição simples é uma asserção que não contém nenhuma outra proposição como parte integrante de si mesma. Denotaremos as proposições simples pelas letras minúsculas p, q, r etc.

Exemplos:

p: Gustavo é pianista

q: Tiago é feliz

2.2. Proposição composta

As proposições compostas são asserções obtidas através de duas ou mais

proposições simples com o emprego das expressões"e", "ou", "não", "se... então", "...se e somente se...".

Denotaremos proposições compostas pelas letras maiúsculas P, Q, R, etc.

Exemplos:

P: Gustavo é pianista e Tiago é feliz.

Q: Fortaleza é a capital do estado Ceará ou $\frac{1}{2}$ é um numero inteiro

R: Não é verdade que $\pi > 5$ e $\cos(\frac{\pi}{2}) = 1$.

S Se $A e B$ são conjuntos não vazios então $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

T: O triângulo ABC é equilátero se somente se é equiângulo.

2.3. Negação de uma proposição

A negação de uma proposição "p" é denotada por "$\sim p$" e se entende como a afirmação contrária a *p*, podendo ser lida : "é falso que p" ou colocando a palavra "não" antes do verbo da proposição.

Exemplos:

$(a) p$: $2 + 5 = 2$.

$\sim p$: É falso que 2+5=2

(b) q: São Paulo é a capital do Brasil.

$\sim q$: São Paulo não é a capital do Brasil.

2.4. Proposição condicional

A condicional é uma asserção ou proposição composta obtida através de duas proposições p e q representada por "se p então q".

Denotamos por "$p \rightarrow q$" pela qual se declara: "p é suficiente para q" ou "q é necessário para p".

Observe que "$p \rightarrow q$". só é uma proposição falsa quando p é verdadeira e *q* é falsidade. Nos demais casos, "$p \rightarrow q$" é sempre verdadeira. Neste caso, dizemos que "p implica q" ou " p acarreta q ".

Exemplos: Dadas as proposições:

p: Uma função f é diferençável em x_0

q: f é continua em x_0

Traduzir para a linguagem corrente as proposições seguintes.

$(a)\ p \rightarrow q$: Se uma função f é diferenciável em x_0 então f e continua em x_0.

$(b)\ p \rightarrow \sim q$: Se uma função f é diferenciável em x_0 então f não é continua em x_0.

2.5. Proposição contrapositiva

A contrapositiva de uma proposição condicional "$p \rightarrow q$" é a proposição " $\sim q \rightarrow \sim p$".

Exemplos: A contrapositiva da proposição condicional " Se uma função f é diferenciável em x_0 então f é continua em x_0 " é "Se f não é continua em x_0 então a função f não é diferenciável em x_0".

2.6. Proposição recíproca

A recíproca de uma proposição condicional "$p \rightarrow q$" é a proposição "$q \rightarrow p$".

Exemplos: A recíproca da proposição condicional "Se uma função f é diferenciável em x_0 então f é continua em x_0 " é "Se f é continua em x_0 então a função f é diferenciável em x_0".

Observe que a recíproca de uma proposição verdadeira, em geral, não é verdadeira.

2.7. Proposição inversa

A inversa de uma proposição recíproca" $q \rightarrow p$", obtida da proposição condicional "$p \rightarrow q$", é a proposição" $\sim p \rightarrow \sim q$"

Exemplos: Pelo exemplo anterior, a inversa da proposição recíproca é " Se uma função f não é diferenciável em x_0 então f não é continua em x_0"

2.8. Proposição bicondicional

A bicondicional é uma asserção obtida através de duas proposições pe q representadas por " p se, e somente se q".

Denotamos por " $p \leftrightarrow q$" pela qual se declara: "p é condição necessária e suficiente para q" ou "q é condição necessária e suficiente para p".

Observe que " $p \leftrightarrow q$" é verdadeira quando as proposições p e q são ambas verdadeiras ou ambas falsas. Neste caso, dizemos que " p equivale a q " e denota-se por "$p \Leftrightarrow q$".

Exemplos: p: Gregório é gordo e q: Martha é magra.

Traduzir para linguagem corrente as proposições:

$(a)\ p \leftrightarrow q$: Gregório ser gordo, é necessário e suficiente para que Martha seja magra.

$(b)\ p \leftrightarrow \sim q$: Gregório ser gordo, é necessário e suficiente para que Martha não seja magra.

As relações entre proposições encontram–se resumidas no quadro abaixo

PROPOSIÇÃO	$p \Rightarrow q$	LOGICAMENTE EQUIVALENTES
CONTRAPOSITIVA	$\sim q \Rightarrow \sim p$	

RECÍPROCA	$q \Rightarrow p$	LOGICAMENTE EQUIVALENTES
INVERSA	$\sim p \Rightarrow \sim q$	

3. Proposições especiais

As proposições estudadas até agora, recebem na matemática algumas terminologias bem específicas a saber:

Axioma - é uma proposição que relaciona propriedades de evidência imediata, proveniente da experiência e da observação.

Exemplo: Por um ponto passam infinitas retas.

Teorema - é uma proposição que exige prova para assegurar a veracidade de seu enunciado. Compõem-se de três partes.

1ª parte: **Sujeito** que é a figura estudada.

2ª parte: **Hipótese** conjunto de condições atribuídas ao sujeito consideradas verdadeiras.

3ª parte: **Tese** conclusão da hipótese.

Corolário - é uma proposição que é consequência imediata de outra ou de um Teorema já demonstrado.

Lema - é uma proposição que será utilizada na prova de uma outra ou de um teorema.

Sabe-se que em matemática 98% das proposições (Teoremas) estão na forma se "p então q"(Proposição condicional) e neste contexto a proposição "p" é a hipótese e a proposição "q" a tese. E como provar ou demonstrar ? Como "p" é a hipótese, p é verdadeira logo "$p \Rightarrow q$" é verdadeiro se e somente

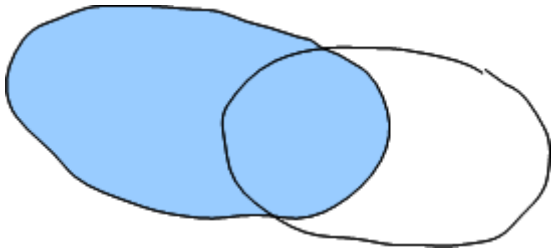
se "q" o é. Portanto provar "$p \Rightarrow q$" é supor p verdadeiro e concluir daí que "q" também o é. Este tipo de prova ou demonstração é chamada **prova direta** (Utiliza a hipótese para em seguida concluir a tese). Veja como se prova o teorema seguinte:

Teorema: Se A, B são conjuntos não vazios então $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

Hipótese: A e B conjuntos não vazios.

Tese: $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

Prova: (Prova Direta)



Ora, observa-se na figura que $A \cup B = (A - B)U(B - A)U(A \cap B)$ onde esta união é disjunta, isto é, $(A - B) \cap (B - A) = \varphi$, $(A - B) \cap (A \cap B) = \varphi$ e $(B - A) \cap (A \cap B) = \varphi$

Então $n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B)$.

Mas $n(A - B) = n(A) - n(A \cap B)$ e $n(B - A) = n(B) - n(A \cap B)$, e consequentemente $n(A \cup B) = [n(A) - n(A \cap B)] + [n(B) - n(A \cap B)] + n(A \cap B) = n(A) + n(B) - n(A \cap B)$

Lema:

Se A, B são conjuntos não vazios e disjuntos então $n(A \cup B) = n(A) + n(B)$

Hipótese: A, B conjuntos não vazios e $A \cap B = \varphi$ (disjuntos)

Tese: $n(A \cup B) = n(A) + n(B)$.

Prova:

Pelo Teorema anterior, $n(A \cup B) = n(A) + n(B) - n(A \cap B)$ e como por hipótese $A \cap B = \varphi$, segue- se que $n(A \cap B) = 0$ e consequentemente $n(A \cup B) = n(A) + n(B)$.

O matemático grego Euclides de Alexandria (Século III a.C) dedicou boa parte de sua vida ao trabalho de escrever os elementos, o livro texto mais bem sucedido de toda a história. Até este século tratava-se do segundo maior best-seler mundial depois da bíblia. Subdivididos em 13 livros, sendo que o 7^0, 8^0 e 9^0 livros são dedicados ao estudo da Teoria dos Números, ao exame dos números primos, máximo divisor comum e a fatoração.

Euclides também explorou uma arma lógica conhecida como "redução ao absurdo" ou "prova por absurdo" (Por contradição) que chamamos de prova indireta. Sua abordagem envolve a ideia inversa de negar a tese a admitir a hipótese. Portanto o teorema fica provado se isto acarretar um absurdo (contradição), pois a matemática abomina o absurdo, e assim a negação da tese é falsidade logo a tese é verdadeira. Euclides, no seu 10^0 livro dos elementos utiliza redução ao absurdo de modo a provar que $\sqrt{2}$ não pode ser escrito como uma fração. Veja a prova do teorema seguinte:

Teorema: Se X é um conjunto qualquer e φ é o conjunto vazio então $\varphi \subset X$.

Hipótese: φ e X conjuntos

Tese: $\varphi \subset X$

Prova (Prova Indireta): Vamos negar a tese, ou seja, suponha que $\varphi \not\subset X$ logo existe pelo menos um elemento $x \in \varphi$ tal que $x \notin X$. Mas o conjunto vazio não possui elemento algum, portanto $x \in \varphi$ é um absurdo, logo, a negação da tese é falsidade e consequentemente a tese é verdadeira, isto é, $\varphi \subset X$.

4. Quantificadores

Uma sentença aberta com uma variável x em um conjunto $X \neq \varphi$ é toda afirmação $p(x)$ aplicável aos elementos $x \in X$.

Exemplo:

X é uma bela mulher. O conjunto X, que contem x, está implícito.

Quando todos os elementos de X satisfazerem $p(x)$ escrevemos

(i) Para todo $x \in X, p(x)$

(ii) Qualquer que seja $x \in X, p(x)$

(iii) Para cada $x \in X, p(x)$

No simbolismo da lógica matemática escrevemos (i), (ii), (iii), abreviadamente como segue: "$\forall\, x \in X, p(x)$" O símbolo $\forall$ é chamado quantificador universal.

Por outro lado, quando pelo menos um elemento $x \in X$ satisfaz $p(x)$ escrevemos:

(i) Existe um $x \in X$ tal que $p(x)$

(ii) Existe pelo menos um $x \in X$ tal que $p(x)$

(iii) Pra algum $x \in X$ tal que $p(x)$

Escrevemos $(i),(ii),(iii)$, abreviadamente como segue: "$\exists x \in X$; $p(x)$". O símbolo $\exists$ é chamado quantificador existencial.

A negação da proposição "$\forall x \in X, p(x)$" é "$\exists x \in X; \sim p(x)$" e a negação da proposição "$\exists x \in X; p(x)$" é "$\forall x \in X, \sim p(x)$".

Exemplo: A negação de "Toda mulher é bela " é: "Existe pelo menos uma mulher que não é bela"

5. Contra-exemplo

Para se provar que uma proposição é falsa, é suficiente que se apresente uma situação particular em que essa afirmação não é verdadeira. Isso é o que chamamos de contra-exemplo.

Suponhamos que queremos provar que a proposição "$\forall x \in X, p(x)$" é falsidade. Então basta provar que a negação "$\exists x \in X; \sim p(x)$" é verdadeira, isto é, existe algum $x_0 \in X$ tal que $p(x_0)$ é falsidade. O elemento $x_0 \in X$ é chamado contra-exemplo.

Exemplo: A proposição "$\forall x \in \mathbb{R}, x^2 > x$" é falsidade, sendo por exemplo $x_0 = \frac{1}{2}$um contra - exemplo, visto que $\frac{1^2}{2} < \frac{1}{2}$.

Definições na matemática

A palavra **pato**, sabemos que possui mais de um significado na língua portuguesa. Vejamos o que diz o dicionário novo Aurélio século XXI.

> *PATO[1] . S.m. 1. Zool. Ave anseriforme. 2. Iguaria feitacom pato 3. Bras. Mau jogador.*
>
> *PATO[2] . Paga o pato. Fam. 1 sofrer as consequências de alguém. 2. Pagar as despesas*
>
> *PATO[3] .1. Etnôn.* Individuo dos patos, povo indígena caiapó que habitava as margens da lagoa dos Patos.2. Pertencente ou relativo a esse povo.

Esses diferentes significados para uma mesma palavras causam confusão, e o seu significado depende do contesto onde ela é inserida. No caso da matemática, as definições têm um papel de extrema importância, pois quando definimos uma palavra na matemática, a palavra e sua definição têm o mesmo significado.

Se definimos a palavra pato como "Uma ave aquática que possui bico plano e pés achatados" podemos também dizer que "Se um animal é um pato então é um ave aquática que possui bico plano e pés achatados" ou ainda "Se uma ave é aquática e possui bico plano e pés achatados, então esse animal é um pato".

Fazendo p: "Um animal é um pato" e q: "É uma ave aquática que possui bico plano e pés achatados", a proposição" se q então p " é a recíproca da proposição condicional "se p então q". Já estudamos que, em geral, a recíproca de uma proposição condicional verdadeira não é necessariamente verdadeira. No caso das definições na matemática tanto é verdade a proposição condicional quanto sua recíproca, isto é, o nome a ser definido "p" e sua definição "q" têm o mesmo significado, logo "$p \Leftrightarrow q$".

Posto isto, a definição de pato é assim escrita: "Um animal é um pato se somente se é uma ave aquática que possui bico plano e pés achatados".

Síntese do Capítulo

Neste segundo capítulo estudamos noções de lógica, onde apresentamos alguns conceitos de grande importância no desenvolvimento e organização do raciocínio.

Inicialmente definimos a proposição simples e através da composição de proposições chegamos a definir um teorema, um corolário ou um axioma. Com esses conceitos, aprendemos a diferenciar uma prova de uma demonstração, e estudamos também quantificadores e definição.

Atividades de avaliação

1. Determine o valor lógico de cada uma das seguintes proposições:

a) Não é verdade que 12 é um numero impar.

b) É falso que $2+3=5$ e $1+1=3$.

c) É falso que $3+3=6$ ou $\sqrt{(-1)}=0$.

d) $\sim(1+1=5 \Leftrightarrow 3+3=1)$

e) $\sim(2+2 \neq 4 e 3+5=8)$.

2. Sejam as proposições p: Está frio e q: Está chovendo. Traduzir para a linguagem corrente as seguintes proposições:

a) $\sim p$

b) $q \Leftrightarrow p$

c) $p \rightarrow \sim q$

d) $q \rightarrow p$

e) $\sim p \rightarrow q$

f) (p)

3. Os exercícios seguintes se referem a estas proporções: "Se você mora em Fortaleza então você mora no Ceará. "

a) Qual é hipótese deste proposição ?

b) Qual é a sua conclusão ?

c) Reescreva essa proposição na forma"$bsea$"

4. Reescreva cada uma das orações seguintes na forma "$se...então$."

a) Nenhum fantasma tem sombra.

b) Todos os anos bissextos têm 366 dias.

c) Quando o gato está na gaiola não é para cantar.

d) Use a escada em vez do elevador em caso de incêndio.

e) Nenhum numero de telefone genuíno começa com 555.

5. Como é formada cada uma das proposições seguintes ?

a) A recíproca de uma proposição condicional.

b) A inversa de uma proposição condicional.

c) A contrapositiva de uma proposição condicional.

6. Considere a proposição " Se sua temperatura é maior que 38^0 então você tem febre."

a) Esta proposição é verdadeira.

b) Se a proposição for representada pelo símbolo "$p \rightarrow q$", que palavras representam as proposições "p" e "q"?

c) Escreva com palavras a proposição que é representada por "$\sim p \rightarrow \sim q$

d) Esta proposição é verdadeira ?

e) Como é chamada essa proposição com relação a proposição original ?

f) Esta proposição tem o mesmo significado da proposição original ?

g) Escreva com palavras a proposição que é representada por "$q \rightarrow p$"

h) Esta proposição é verdadeira ?:

i) Como é chamada esta proposição com relação a proposição original ?

j) Esta proposição possui o mesmo significado da proposição original ?

7. Cada uma das proposições escritas abaixo e seguida de alguns outras proposições. Identifique a relação de cada uma delas com a proposição inicial. Escreva recíproca, inversa contra-positiva ou proposição original como apropriado

Proposição Inicial: " Se você mora no Rio então você precisa de um equipamento de mergulho."

a) Se você não mora no Rio então você não precisa de um equipamento de mergulho.

b) Se você não precisa de um equipamento de mergulho então você não mora no Rio.

c) Você precisa de um equipamento de mergulho se você mora no Rio.

8. Sendo X = {3, 5, 7, 9} dar um conta-exemplo para cada uma das seguintes proposições:

a) $(\forall x \in X)(x + 3 \geq 7)$

b) $(\forall x \in X)(x \acute{e} primo)$

c) $(\forall x \in X)(|\ x\ | = x)$

9. Sendo X = {1, 2, 3, 4} ache o valor lógico de cada uma das seguintes proposições:

a) $(\forall x \in X)(x + 3 < 6)$

b) $(\forall x \in X)(x^2 - 10 \leq 8)$

c) $(\exists x \in X)(x + 3 < 6)$

d) $(\exists x \in X)(x^2 + x = 15)$

10. Dar a negação das proposições do exercício 9.

11. Decida quais os das orações são boas definições, determinado quando sua recíprocas são verdadeiras e quando não o são.

a) Se é dia de ano então é 1^0 de Janeiro.

b) Se é dia de ano então é feriado.

c) Uma câmera é um equipamento para tirar retrato.

d) Um gambá é um animal que tem couro preto e branco.

e) Gelo seco é dióxido de carbono congelado.

12. A seguinte afirmação "Uma criatura extraterrestre é um ser de outro lugar que não a terra" é uma definição de criatura extraterrestre. Quais das seguintes proposições são verdadeira ?

a) Se uma criatura é extraterrestre então ela é de outro lugar que não a Terra.

b) Se uma criatura é um ser de outro lugar que não a Terra então ela e extraterrestre.

c) Se uma criatura não é extraterrestre então ela não é um ser de outro lugar que não a Terra.

d) Se uma criatura não é ser de outro lugar que não a Terra então ela não é extraterrestre.

Capítulo 3

Números naturais e Números inteiros

Objetivos

- Conhecer o conjunto dos números naturais e dos inteiros.
- Estudar indução nos naturais, divisores, divisibilidade e m.d.c., múltiplos e m.m.c.
- Conhecer números primos e compostos.

Introdução

Neste terceiro capítulo iremos conhecer e estudar o conjunto dos números naturais e dos números inteiros relativos. No conjunto dos naturais estudaremos métodos de indução, divisibilidade, onde teremos os conceitos de divisor, múltiplo, m.d.c. e m.m.c. Como também conheceremos números primos e compostos.

1. Generalidades

Faremos inicialmente um estudo do conjunto N = {0, 1, 2, 3, ...} ou N = {0, 1, 2, 3, ...} dos números naturais. Colocar ou não o algarismo zero no conjunto $\mathbb{N}$ é uma mera questão de conveniência. Não iremos fazer uma construção lógica impecável do conjunto $\mathbb{N}$, mas apresentar alguns princípios básicos de extrema importância. Essa construção lógica a qual me refiro, teve sua primeira tentativa no século XI com Campano, quando este enunciou a existência de um elemento mínimo em um sub-conjunto $A \neq \Phi$ de $\mathbb{N}$. Posteriormente, Leibiniz (1646 – 1716) assinala que as propriedades das operações adição e multiplicação deveriam ser provadas.

Em 1862, Grassmann (1809 – 1877) define adição e multiplicação e prova as propriedades dessas operações e utiliza o princípio de indução. Em 1891 Giuseppe Peano (1858 – 1932) utiliza conceitos primitivos (Termos sem uma explicação formal) e alguns axiomas para explicar a existência de $\mathbb{N}$. Mas foi Richard Dedekind (1883 – 1916) o primeiro a formular, através de axiomas, a existência de $\mathbb{N}$.

Outra propriedade fundamental em $\mathbb{N}$ é a relação de ordem $\leq$ (menor ou igual): Dados $a, b \in \mathbb{N}$, diz-se que a $\leq$ b (a menor ou igual a b) se existe $d \in \mathbb{N}$

tal que $b = a + d$. O número "d" é chamado diferença entre a e b e indica-se por $d = b - a$. De maneira análoga define-se a ≥ b (a menor ou igual a b), a < b (a menor que b) e a > b (a maior que b).

Os números negativos foram introduzidos na matemática pelos indianos. O primeiro a utilizar os números negativos foi o matemático indiano Brahmagupta *(Século VI)* quando afirmou que todo número positivo tem duas raízes quadráticas, uma positiva e outra negativa.

Da relação de ordem $a > b$ a diferença $d = a - b$ é sempre positiva enquanto b – a é sempre negativa. Manipulando valores convenientes para a e b encontramos uma infinidade de números negativos a saber: $-1, -2, -3, \ldots = -\mathbb{N}$ e assim N ∪ (–N) = {..., –3, –2, –1, 0, 1, 2, 3, ...} = Z chamado conjunto dos números inteiros.

2. Indução Matemática em □

2.1. Elemento mínimo

Seja $A \neq \varphi$ sub-conjunto de $\mathbb{N}$. Chama-se elemento mínimo de A um elemento $a \in A$ tal que $a \leq x$ para todo $x \in A$. Denota-se $a = min(A) \Leftrightarrow (\forall x \in A, a \leq x)$.

Teorema: Se $a = min(A)$ então a e único.

Hipótese: $a = min(A)$

Tese: a é único

Prova: Suponhamos que exista um outro $a' \in A$ tal que $a' = min(A)$ para provemos que $a = a'$.

Por hipótese, $a = min(A) \Leftrightarrow (\forall a' \in A, a \leq a')$ e como $a' = min(A) \Leftrightarrow (\forall a \in A, a' \leq a)$.

Das relações de ordem $a \leq a'$ e $a' \leq a$ conclui-se que $a = a'$.

Se o elemento mínimo de A existe, ele é chamado também de menor número natural de A.

Exemplo: O conjunto $\mathbb{N}$ possui elemento mínimo $1 = min(\mathbb{N})$, pois $1 \in \mathbb{N}$ e para todo $x \in \mathbb{N}, 1 \leq x$.

Exemplo: O subconjunto $A = \{x \in \mathbb{N}; 7 < x \leq 15\}$ possui elemento mínimo $8 = min(A)$, pois $8 \in A$ e para cada $x \in A$, $8 \leq x$.

Exemplo: O conjunto $A = \{-1, -2, -3, \ldots\}$ de $\mathbb{Z}$ não tem elemento mínimo, pois não existe $a \in A$ tal que $a \leq x$ para todo $x \in A$.

2.2. Princípio da boa ordenação

Axioma: "Todo subconjunto $A \neq \varphi$ de $\mathbb{N}$ possui elemento mínimo".

$$\forall \varphi \neq A \subset \mathbb{N} \Rightarrow \exists min(A).$$

2.3. Princípio de indução

Teorema: Seja $A \subset \mathbb{N}$ tal que $1 \in A$ e para todo $k \in \mathbb{N}$, se $k \in A$ então $k+1 \in A$. Sob estas condições $A = \mathbb{N}$.

Hipótese: $A \subset \mathbb{N}$; $1 \in A$ e para todo $k \in \mathbb{N}$, se $k \in A$ então $k+1 \in A$

Tese: $A = \mathbb{N}$.

Prova: (Prova Indireta). Vamos negar a tese, isto é, suponhamos que $A \neq \mathbb{N}$ e seja $\varphi \neq X = \mathbb{N} - A = \{x; x \in \mathbb{N} e x \notin A\}$, Como $\varphi \neq X \subset \mathbb{N}$ pelo Princípio da Boa Ordenação existe $x_o = min(X)$. Por hipótese, $1 \in A$ logo $x_o > 1$, $(x_o - 1) \notin X$ e assim $(x_o - 1) \in A$. Pela hipótese temos que $(x_o - 1) + 1 = x_o \in A$, que é um absurdo, pois $x_o \in X$. Portanto $X = \varphi$ e consequentemente $A = \mathbb{N}$.

Corolário (Indução Matemática)

Seja $p(n)$ uma proposição associada a cada $n \in \mathbb{N}$ e que satisfaça as propriedades:

$P.1$ $p(1)$ é verdadeiro

$P.2$ Para todo $k \in \mathbb{N}$, se $p(k)$ é verdadeiro então $p(k+1)$ também é verdadeiro.

Nestas condições $p(n)$ é verdadeira para todo n.

Hipótese: $p(n)$ é uma proposição e as propriedades $P.1$ e $P.2$.

Tese: $p(n)$ é verdadeira para todo n.

Prova: Seja $A = \{n \in \mathbb{N}; p(n) é verdadeira\}$. Pela hipótese $P.1$, $p(1)$ é verdadeiro logo $1 \in A$. Pela hipótese $P.2$, para todo $k \in \mathbb{N}$, se $k \in A$ então $(k+1) \in A$. Pelo Teorema anterior $A = \mathbb{N}$, isto é, $p(n)$ é verdadeiro para todo n.

A prova por indução matemática consiste em verificar a propriedade $P.1$ em seguida a propriedade $P.2$ que tem como hipótese: $p(k)$ é verdadeira e tese: $p(k+1)$ é também verdadeira.

Exemplo: Prove por indução matemática as seguintes proposições :

1. $p(n): 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo n

Prova: Se $n = 1$ então $\frac{1(1+1)(2+1)}{6} = 1 = 1^2$, isto é, $p(1)$ é verdadeira .

Vamos admitir, por hipótese de indução, que para $n = k$, ou seja, $p(k): 1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$ seja verdadeira para provar que para $n = k+1$, isto é, $p(k+1)$ também o é.

Mas $1^2 + 2^2 + \ldots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$\frac{k(k+1)(2k+1)+6(k+1)^2}{6} = \frac{(k+1)[k(2k+1)+6(k+1)]}{6} = \frac{(k+1)[(k+2)(2k+3)]}{6}$, provando que $p(k+1)$é verdadeiro.

2. $p(n): 1+\frac{1}{2^2}+\ldots+\frac{1}{n^2} \leq 2-\frac{1}{n}$ para todo n

Prova: Se $n=1$ então $1 \leq 1$, ou seja, $p(1)$ é verdadeira.

Supor por hipótese de indução que para $n=k$, ou seja,

$p(k): 1+\frac{1}{2^2}+\ldots+\frac{1}{k^2} \leq 2-\frac{1}{k}$ seja verdadeira e vamos provar que para $n=k+1$, isto é, $p(k+1)$ também o é. Mas

$$1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}+\frac{1}{(k+1)^2} \leq 2-\frac{1}{k}+\frac{1}{(k+1)^2} = 2-\frac{k^2+k+1}{k(k+1)^2} < 2-\frac{k^2+k}{k(k+1)^2} = 2-\frac{1}{k+1}$$

provando que $p(k)$ é verdadeira.

3. $p(n): n! > n^2$, para todo $n \geq 4$

Prova: Se $n=4$ então $4! = 4.3.2 = 24 = 4^2$, ou seja , $p(4)$ é verdadeira.

A hipótese de indução $p(k): k! > k^2$ é verdadeira logo $(k+1)k! > (k+1)k^2 = k^3+k^2$, ou ainda, $(k+1)! > k^3+k^2$. Para $k \geq 4, k^3 > 2k+1$ e assim $(k+1)! > (2k+1)+k^2 = (k+1)^2$.provando que $p(k+1): (k+1)! > (k+1)^2$.é verdadeiro.

4. $p(n): 2^n > 2n+1$ para todo $n \geq 5$

Prova: Para $n=5, 2^5 = 32 > 11 = 2.5+1$ logo $p(5)$ é verdadeira.

Admitimos que a hipótese de indução $p(k): 2^k > 2k+1$ é verdadeira, vamos provar que para $n=k+1$, ou seja , $p(k+1)$ é verdadeira também. Mas para $k \geq 5, 2^k > 2$ e somando a $2^k > 2k+1$ encontramos $2^k+2^k > 2k+1+2$, ou ainda, $2^{k+1} > 2(k+1)+1$ o que prova que $p(k+1)$é verdadeira.

5. $p(n): 2^n > n^2$ para todo $n \geq 5$.

Prova: Se $n=5$ então $2^5 = 32 > 25 = 5^2$, isto é, $p(5)$, é verdadeira.

A hipótese indutiva $p(k): 2^k > k^2$é verdadeira. Somando a $2^k > 2k+1$(Exercícios anterior) obtemos $2^k+2^k > k^2+2k+1$, isto é, $2^{k+1} > (k+1)^2$provando que $p(k+1)$ é verdadeira.

Para refletir

1. Prove por indução matemática as proposições seguintes:

a) $1+3+5+\ldots+(2n-1) = n^2$, para todo n.

b) $\frac{1}{1.2}+\frac{1}{2.3}+\ldots+\frac{1}{n(n+1)} = \frac{n}{n+1}$ para todo n.

c) $1^3+2^3+\ldots+n^3 = (1+2+\ldots+n)^2 = \frac{n^2(n+1)^2}{4}$, para todo n.

d) $a+aq+\ldots+aq^n = \frac{a(q^{n+1}-1)}{q-1}, q \neq 1$ para todo *n*

e) Se $a \geq 2$ então $2a^n \leq a^{n+1}$, para todo *n*.

f) Se $a \geq 2$ então $1+a+\ldots+a^n < a^{n+1}$, para todo *n*.

g) $n^3 < n!$, para todo $n \geq 6$.

h) $a \geq 2$ para todo $n \geq 10$.

2. Ache $n \in \mathbb{N}$ tal que $3^{n+2}.2^{n+3} = 2592$.

3. Verificar se o quadrado de um número natural pode terminar em 2,3,7,ou 8.

4. Prove que o produto de quatro números naturais, acrescido de 1, é um quadrado perfeito.

5. Seja $a \in \mathbb{Z}$ e suponha que para cada para todo $n \geq a$ esteja associado a proposição $p(n)$ que satisfaz as propriedades:
$P.1\ p(a)$. é verdadeira.
$P.2$ Para todo $r \geq a$, se $p(r)$ é verdadeira então $p(r+1)$ também é verdadeira. Nestas condições $p(n)$ é verdadeira para todo $n \geq a$. Prove.
Sugestão:

6. Tome $A = \{x \in \mathbb{N}; x \geq aep(x)éfalsa\}$ e prove que $A = \varphi$ (Prova Indireta)

7. Prove que $2^{n+1} \geq n+2$ qualquer $n \geq -1$.

3. Divisibilidade

O número natural "$a \neq 0$ divide o número natural b" se, e somente se, existe pelo menos um número natural q tal que $b = a.q$.Neste caso diz-se ainda que "a é divisor de b", "b é múltiplo de a" e que "b é divisível por a".

Denota-se $a/b \Leftrightarrow (\exists q \in \mathbb{N}; b = a.q)$.

O elemento $q \in \mathbb{N}$ tal que $b = a.q$ é chamado de quociente de b por α. Quando "a não divide b", escreve-se $a \nmid b \Leftrightarrow (\forall q \in \mathbb{N}, b \neq a.q)$

Exemplo: Em $\mathbb{Z}$, se a/b então existe $q \in \mathbb{Z}$ tal que $b = a.q \Rightarrow b = (-a).(-q)$, ou seja, $-a/b$

É verdadeira a relação zero divide zero, pois $0 = 0.q$, para todo $q \in \mathbb{N}$, enquanto que $\frac{0}{0}$ é uma indeterminação.

Para a relação a/b são válidas as propriedades seguintes:

$P.1\ a/0, 1/a$ e a/a

$P.2$ Se $a \in \mathbb{Z}$ e $a/1$ então $a = \pm 1$

$P.3$ Se $a, b \in \mathbb{Z}$ e se a/b e b/a então $a = \pm b$

$P.4$ Se a/b e b/c então a/c

$P.5$ Se a/b e a/c então $a/(xb \pm yc)$, quaisquer $x, y \in \mathbb{N}$.

Deixamos como exercícios as demostrações das propriedades $P.1$ a $P.4$ e provaremos a proposição $P.5$.

Hipótese: a/b e a/c

Tese: $a/(xb \pm yc), \forall x, y \in \mathbb{N}$

Prova: Por Hipótese $a/b \Leftrightarrow (\exists q_1 \in \mathbb{N}; b = aq_1 \Rightarrow xb = a(xq_1), \forall x \in \mathbb{N})$

$a/c \Leftrightarrow (\exists q_2 \in \mathbb{N}; c = aq_2 \Rightarrow yc = a(yq_2), \forall y \in \mathbb{N})$

logo $xb \pm yc = a(xq_1 \pm yq_2) \Rightarrow a/(xb \pm yc)$.

Indicaremos por $D(a) = \{x \in \mathbb{N}; x/a\}$, o conjunto dos divisores de "a".

É imediato que se $0 \neq a \in \mathbb{Z}$ então $a/a, -a/a, 1/a$ e $-1/a$ logo $\pm 1 \pm a$ são chamados divisores triviais de "a", e mais, se x/a e $a > 0$ então $-a \leq x \leq a$ ou seja $D(a) \subset [-a, a]$.

Divisor comum de $a, b \in \mathbb{N}$ é todo natural d tal que d/a e d/b. Indica-se por $D(a,b) = \{d \in \mathbb{N}; d/aed/b\} = \{d \in \mathbb{N}; d \in D(a)ed \in D(b)\}$ $= \{d \in \mathbb{N}; d \in D(a) \cap D(b)\}$, portanto, podemos afirmar que D(a, b) = $D(a) \cap D(b)$.

Exemplo: Em $\mathbb{Z}$, temos $D(3) = \{\pm 1, \pm 3\}$,
$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ logo $D(3) \cap D(12) = \{\pm 1, \pm 3\}$.

Indicaremos por $M(a) = \{x \in \mathbb{N}; a/x\} = \{x \in \mathbb{N}; x = a.q\} = \{a, 2a, 3a, \dots\}$ conjunto dos múltiplos de "a" . Se em particular $a = 1$ então $M(1) = \mathbb{N}$ e se $a = 2$ então $M(2) = \{2,4,6, \dots\}$ conjunto dos números pares, e mais $\mathbb{N} - M(2) = \{1,3,5, \dots\}$ conjunto dos números ímpares.

Exemplo: Em $\mathbb{Z}$, temos:

$$(a) M(1) = M(-1) = \mathbb{Z}$$

$$(b) M(3) = \{3q, q \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

Múltiplo comum de $a, b \in \mathbb{Z}$ com $a \neq 0$ e $b \neq 0$ é todo inteiro $x \in \mathbb{Z}$ tal que a/x e b/x.

Indica-se por

$M(a,b) = \{x \in \mathbb{Z}; a/xeb/x\} = \{x \in \mathbb{Z}; x \in M(a)ex \in M(b)\} =$
$M(a) \cap M(b)$.

Exemplo: Sejam $a = 7$e $b = 14$ então

$M(7) = \{7q; q \in \mathbb{Z}\} = \{0, \pm 7, \pm 14, \dots\}$
$M(14) = \{14q'; q' \in \mathbb{Z}\} = \{0, \pm 14, \pm 28, \dots\}$ logo
$M(7) \cap M(14) = \{0, \pm 14, \dots\}$.

4. Algoritmo de Euclides em □

Teorema: Se $a, b \in \mathbb{Z}$ e $b > 0$ então existem únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$ com $0 \leq r < b$

Hipótese: $a, b \in \mathbb{Z}$ e $b > 0$

Tese: Existem únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$ com $0 \leq r < b$

Prova: Seja $S = a - bx; x \in \mathbb{Z}ea - bx \geq 0$. Como $\emptyset \neq S \subset \mathbb{N}$ pelo Princípio da Boa Ordenação existe um único $r = min(S)$, isto é, $r \geq 0$ e $r = a - bq$ou $a = bq + r, q \in \mathbb{Z}$. Ademais $0 \leq r < b$, pois se fosse $r \geq b$ teríamos $0 \leq r - b = (a - b.q) - b = a - b(q + 1) < r$o que é um absurdo visto que $r = min(S)$.

Para provar a unicidade de q, suponha que exista $q' \in \mathbb{Z}$ tal que $a = b.q' + r$, $0 \leq r < b$ para concluir que $q = q'$. Das identidades $a = b.q + r$ e $a = b.q' + r$encontramos $b.q = b.q'$ logo $b(q - q') = 0$ e sendo $b > 0$conclui-se que $q = q'$.

Corolário: Se $a, b \in \mathbb{Z}$ e $b \neq 0$ então existem únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$ com $0 \leq r <| b |$.

Hipótese: $a, b \in \mathbb{Z}$ e $b \neq 0$.

Tese: Existem e são únicos $q, r \in \mathbb{Z}$ tal que $a = b.q + r$ com $0 \leq r <| b |$.

Prova: Se $b > 0$ então $| b |= b > 0$ e pelo teorema anterior, existem e são únicos $q, r \in \mathbb{Z}$ tal que $a =| b | q + r = b.q + r$ com $0 \leq r < b =| b |$. Se $b < 0$ então $| b |= -b > 0$ e pelo teorema, existem e são únicos $q', r \in \mathbb{Z}$ tal que $a =| b | q' + r = b(-q') + r$ com $0 \leq r <| b |$. Portanto $q = -q'$ e assim $a = b.q + r$com $0 \leq r <| b |$.

Os inteiros a, b, qer são chamados, respectivamente, **dividendo, divisor, quociente e resto** da divisão de "a" por "b". Ademais se b/a de modo que $r = 0$, então neste caso a **divisão é exata**.

Exemplo: Na divisão de $a \in \mathbb{Z}$ por $b = 2$ o algoritmo de Euclides nos dá $a = 2.q + r$com $0 \leq r < 2$ e possíveis restos $r = 0$ou $r = 1$. Se $r = 0$ então $a = 2q$, $q \in \mathbb{Z}$ e o inteiro "$a = 2q$" é chamado **par** e o conjunto $P = \{0, \pm 2, \pm 4, \dots\}$dos múltiplos de dois é chamado de conjunto dos números pares. Se $r = 1$então $a = 2q, +1, q \in \mathbb{Z}$ e o inteiro "$a = 2q + 1$" é chamado **ímpar** e o conjunto $I = \{\pm 1, \pm 3, \dots\}$ é chamado de conjunto dos números ímpares.

Exemplo: Na divisão do quadrado a^2 de um inteiro a por 4 o resto é zero ou um.

De fato, se a é par então $a = 2q, q \in \mathbb{Z}$ logo $a^2 = 4q^2 + 0$ isto é, $r = 0$ e se a é impar então $a = 2q + 1, q \in \mathbb{Z}$ e assim $a^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$, isto é, $r = 1$.

Exemplo: O quadrado de todo inteiro ímpar é da forma $8k + 1$.

Prova: Pelo algoritmo de Euclides $a = 4.q + r$ com $0 \leq r < 4$ e os possíveis restos são $r = 0, r = 1, r = 2$ e $r = 3$. Portanto, qualquer inteiro é de uma das formas $4q, 4q + 1, 4q + 2, 4q + 3$. Mas somente os inteiros $4q + 1 e 4q + 3$ são ímpares e assim $(4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1$ e $(4q + 3)^2 = 16q^2 + 24q + q = 8(2q^2 + 3q) + 1 = 8k + 1$.

Exemplo: Se $a \in \mathbb{Z}$ então $2/a(a + 1)$.

Prova: Se $a = 2q(par), q \in \mathbb{Z}$ então

$a(a + 1) = 2q(2q + 1) = 2[q(2q + 1)] \Rightarrow 2/a(a + 1)$.

Se $a = 2q + 1(ímpar), q \in \mathbb{Z}$ então

$a(a + 1) = (2q + 1)(2q + 1 + 1) = 2[(q + 1)(2q + 1)] \Rightarrow 2/a(a + 1)$.

Portanto, em ambos os casos, $2/a(a+1)$.

Exemplo: Se $a \in \mathbb{Z}$ então um dos inteiros $a, a+2, a+4$ é divisível por 3.

Hipótese: $a \in \mathbb{Z}$

Tese: a ou $a+2$ ou $a+4$ é divisível por por 3.

Prova: Pelo algoritmo de Euclides $a = 3.\mathrm{q} + r$ com $0 \leq r < 3$ e os possíveis restos são $r = 0$, $r = 1$ e $r = 2$. Se $r = 0$ então $a = 3.\mathrm{q} \Rightarrow 3/a$.

Se $r = 1$ então

$a = 3\mathrm{q} + 1 \Rightarrow a + 2 = 3\mathrm{q} + 1 + 2 = 3(q+1) \Rightarrow 3/(a+2)$.

Por fim, se $r = 2$ então

$a = 3.\mathrm{q} + 2 \Rightarrow a + 4 = 3\mathrm{q} + 2 + 4 = 3(q+2)$logo $3/(a+4)$.

Exemplo: Determine os inteiros positivos que divididos por 17 deixam um resto igual ao quadrado do quociente.

Prova: Seja "a" o inteiro positivo. Pelo algoritmo de Euclides, $a = 17.\mathrm{q} + r = 17.\mathrm{q} + q^2$ com $0 \leq r = q^2 < 17$ e os possíveis valores para q são: $1,2,3ou4$.

Portanto $a = 18$ ou $a = 38$ ou $a = 60$ ou $a = 84$.

Exemplo: Mostre que os números inteiros "a" e "$a + 2\mathrm{b}$" têm sempre a mesma paridade

De fato, se $a = 2\mathrm{q}(par), q \in \mathbb{Z}$, então

$a + 2\mathrm{b} = 2\mathrm{q} + 2\mathrm{b} = 2(q+b) = 2\mathrm{q}'$ é par, onde $q' = q + b$.

Se $a = 2\mathrm{q} + 1(\acute{\imath}mpar), q \in \mathbb{Z}$ então

$a + 2\mathrm{b} = 2\mathrm{q} + 1 + 2\mathrm{b} = 2(q+b) + 1 = 2\mathrm{q}' + 1$

Portanto "a" e "$a + 2$" têm a mesma paridade.

Exemplo: Numa divisão de dois inteiros o quociente é 16 e o resto 167. Ache o número inteiro que se pode somar ao dividendo e ao divisor sem alterar o quociente.

Prova: Sejam a (dividendo) e b (divisor), tais que pelo algoritmo de Euclides $a = b.16 + 167$ ou $16.\mathrm{b} = a - 167$. Se x é o inteiro a ser somado ao dividendo e ao divisor e que não altera o quociente então esta divisão é exata, isto é, $a + x = (b + x).16 \Rightarrow a + x = 16\mathrm{b} + 16\mathrm{x}$.

Como $16\mathrm{b} = a - 167$ substituindo na expressão anterior encontramos $a + x = (a - 167) + 16\mathrm{x}ou15\mathrm{x} = 167$.

Portanto, valor de x inteiro é 11.

Exemplo: Ache q e r na divisão de $a = -35$ por $b = 3$.

Em valores absolutos $35 = 3.11 + 2$ logo

$-35 = 3.(-11) - 2$ e $r = -2$ não satisfaz $0 \leq r < b = 3$.

Mas $-35 = 3.(-11) - 2 = 3(-11) - 2 + (3 - 3) =$
$[3.(-11) - 3] + (-2 + 3) = 3.(-12) + 1$ onde $q = -12$ e
$0 \leq r = 1 < b = 3$.

Exemplo: Ache q e r na divisão de $a = -59$ por $b = -7$.

Em valores absolutos $59 = 7.8 + 3 \Rightarrow -59 = (-7).8 - 3$ e $r = -3$ não satisfaz $0 \leq r <| b |= 7$.

Mas $-59 = (-7).8 - 3 = (-7).8 - 3 + (7 - 7) =$
$[(-7).8 - 7] + (-3 + 7) = (-7).9 + 4$ logo $q = 9$ e
$0 \leq r = 4 <| b |= 7$.

Exemplo:

Ache q e r na divisão de $a = 59$ e $b = -14$.

Em valores absolutos $54 = 14.4 + 3 = (-14).(-4) + 3$ logo $q = -4$ e $0 \leq r = 3 <| -14 |= 14$.

Para refletir

1. Prove que:
a) Se $0 \neq a \in \mathbb{Z}$ e $b = 0$ então $b \nmid a$.
b) Se n é par então n^2 também é.
c) Se n é ímpar então n^2 também é.
d) Produto de dois inteiros par é par .
e) Produto de dois inteiros ímpares é ímpar.

2. Ache o número de múltiplos de 6, compreendidos entre 92 e 196.

3. Mostre que os inteiros "$a + b$" e "$a - b$" têm a mesma paridade.

4. Mostre que $a + b + a^2 + b^2$ é par, quaisquer $a, b \in \mathbb{N}$.

5. Se $a, b, c \in \mathbb{Z}$, mostre que:
(i) Se a/b então a/bc.
(ii) Se a/b e se a/c então a^2/bc.
(iii) a/b se somente se $ac/bc, c \neq 0$.

6. Mostre que o quadrado de um inteiro qualquer é da forma $4k$ ou $4k + 1$.

7. Se $a/(2x - 3y)$ e se a $a/(4x - 5y)$ então a/y.

8. Se a é um inteiro ímpar então $24/a(a^2 - 1)$.

9. Na divisão do inteiro $a = 427$ por um inteiro b o quociente é 12 e o resto é r. Ache o divisor b e o quociente r.

10. Na divisão do inteiro 525 por um inteiro positivo e resto é 27. Achar os inteiros que podem ser o divisor e o quociente.

11. Na divisão de dois inteiros positivos o quociente é 16 e o resto é o maior possível. Ache os dois inteiros sabendo que a soma é 341.

12. Prove por indução matemática as proposições seguintes:
a) $p(n): 7/(3^{2n+1} + 2^{n+2})$, qualquer $n \geq 0$.
b) $p(n): 9/(10^n + 3.4^{n+2} + 5)$, qualquer $n \geq 0$.
c) $p(n): 17/(3^{4n+2} + 2.4^{3n+1})$, qualquer $n \geq 0$.

5. Alguns critérios de divisibilidade

5.1. Generalidades

Seja $a_r a_{r-1} \dots a_1 a_0$, onde $a_i \in \{0,1,2,\dots,9\}$, $i = 0,1,2,\dots,r$, o número natural que representa "a". Em nosso sistema de numeração de base decimal, podemos escrevê-lo na forma $a = a_0 + a_1.10 + a_2.10^2 + \dots + a_r.10^r$, unicamente determinado.

Por exemplo, tomemos $a = 2347$, onde temos

$a_0 = 7, a_1 = 4, +a_2 = 3, a_4 = 2$

e assim

$a = a_3 a_2 a_1 a_0 = a_0 + a_1.10 + a_2.10^2 + a_3.10^3 =$

$7 + 4.10 + 3.10^2 + 2.10^3$.

5.2. Divisibilidade por 2

"Um número natural $a = a_0 + a_1.10 + \dots + a_r.10^r$ é divisível por dois se, e somente se ele é par."

A divisão de $n = 10^r (r \geq 1)$ por $b = 2$ é exata. Com efeito, se $r = 1$ então $10 = 2.q_1 + 0$, $q_1 \in \mathbb{N}$. Suponha verdadeira para $r = k$, isto é, $10^k = 2q_r + 0, q_r \in \mathbb{N} então para r = k + 1$ temos $10^{k+1} = 10^k.10 = (2q_r).10 = 2q_{r+1} + 0$, onde $q_{r+1} = 10q_r \in \mathbb{N}$, o que também é verdadeira. Portanto dado um número $a = a_0 + a_1.10 + \dots + a_r.10^r$ podemos reescrevê-lo $a = a_0 + a_1(2q_1) + \dots + a_r(2q_r) = a_0 + 2(a_1 q_1 + \dots + a_r q_r) =$ $= a_0 + 2q'_r, onde q'_r = a_1 q_1 + \dots + a_r q_r$. Como $2/2q'_r$ então $2/a \Leftrightarrow 2/a_0$.

Exemplo: O número $a = 1938$ é divisível por 2, pois $2/a_0 = 8$.

5.3. Divisibilidade por 3

"Um número natural $a = a_0 + a_1.10 + \dots + a_r.10^r$ é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3."

A divisão de $n = 10^r (r \geq 0)$ por 3 deixa resto 1. Pois bem, se $r = 0$ então $10^0 = 3.0 + 1$. Suponha verdadeiro para $n = k$, ou seja, $10^k = 3.q_r + 1, q_r \in \mathbb{N}$, então para $r = k + 1$ obtemos $10^{k+1} = 10^k.10 = (3q_r + 1).(9+1) = 3(9q_r + q_r + 3) + 1 = 3q'_r + 1, q'_r = 9q'_r + q'_r + 3$ que também é verdadeira. Portanto $a = a_0 + a_1(3q_1 + 1) + \dots + a_r(3q_r + 1) = a_0 + a_1 + \dots + a_r + 3q'_r$, onde $q'_r = a_1 q_1 + \dots + a_r q_r$,. Mas $3/3q'_r logo, 3/a \Leftrightarrow 3/(a_0 + \dots + a_r)$.

Exemplo: O número $a = 7161$ é divisível por $b = 3$, pois a soma de seus algarismos, $7 + 1 + 6 + 1 = 15$ é divisível por 3.

5.4. Divisibilidade por 4

"Um número natural $a = a_0 + a_1.10 + \ldots + a_r.10^r$ é divisível por 4 se, e somente se, o número formado pelos seus algarismos da dezena e da unidade for divisível por 4."

Considere o número "a" da forma "$100k + a_1a_0$" ou "$1000k + a_1a_0$" ou ainda "$10000k + a_1a_0$", etc, onde "a_1a_0" é o número formado pelos dois últimos algarismos (das dezenas e das unidades) de "a". Como $4/100k$ então $4/a \Leftrightarrow 4/a_1a_0 \Leftrightarrow a_1a_2$ é múltiplo de 4.

Exemplo: O número *a* = 57284 é divisível por *b* = 4, pois *a* = 57284 = 100.572 + 84 e como $4/84\ então\ 4/57284$. No entanto, *a* = 57231 não é divisível por 4, pois 31 não é múltiplo de 4.

5.5. Divisibilidade por 5

"Um número natural $a = a_0 + a_1.10 + \ldots + a_r.10^r$ é divisível por 5 se, e somente se,seu algarismo das unidades for 5 ou 0.

Se $a = a_0 + a_1.10 + \ldots + a_r.10^r$ então $a = a_0 + 10(a_1 + \ldots + a_r.10^{r-1})$ o que implica dizer que para esse número ser divisível por 5 deveremos ter $a_0 = 5$ ou $a_0 = 0$.

5.6. Divisibilidade por 7

"Um número natural $a = 10k + a_0$ é divisível por 7 se, e somente se, $k - 2a_0$ é divisível por 7."

Considere o número "a" da forma "$10k + a_0$" onde "a_0" é seu algarismo das unidades.

Posto isto, encontre o número "$k - 2a_0$" e vamos provar que "$10k + a_0$" é múltiplo de de 7 se, e somente se, "$k - 2a_0$" é múltiplo de 7.

É suficiente : Se "$10k + a_0$" é múltiplo de 7 então existe $m \in \mathbb{Z}$ tal que $10k + a_0 = 7m \Rightarrow a_0 = 7m - 10k$. Mas $k - 2a_0 = k - 2(7m - 10k) = 7m'$, $m' = 7m', m' = (3k - 2m)$ □ □, isto é ,"$k - 2a_0$" é múltiplo de 7.

É necessário: Se "$k - 2a_0$" é múltiplo de 7 então existe $n \in \mathbb{Z}$ tal que $k - 2a_0 = 7n \Rightarrow k = 7n + 2a_0$. Mas $10k - a_0 = 10(7n + 2a_0) - a_0 = 7n'$, onde $n' = (10n + 3a_0) \in \mathbb{Z}$, ou seja, "$10k + a_0$" é múltiplo de 7.

Exemplo: Seja $a = 59325 = 10.5932 + 5$, onde $k = 5932$ e $a_0 = 5$ logo $k - 2a_0 = 5932 - 2.5 = 5922$. Vamos repetir este artifício até conseguirmos um número que possamos reconhecer, se é ou não divisível por 7. Se divisível então $7/a$, caso contrário $7 \nmid a$. Continuando $592 - 2.2 = 588$, $58 - 2.8 = 42$ e como $7/42 \Leftrightarrow 7/59325$.

5.7. Divisibilidade por 9

"Um número natural $a = a_0 + a_1.10 + \ldots + a_r.10^r$ é divisível por 9 se, e somente se, a soma de seus algarismos der um número divisível por 9."

A prova desse resultado deixamos como exercício, pois o procedimento é idêntico ao procedimento usado na divisibilidade por 3.

6. Máximo Divisor Comum de dois Inteiros

Sejam $a, b \in \mathbb{Z}$ inteiros não nulos.Chama-se máximo divisor comum de aeb, o número $d \in \mathbb{N}$ que satisfaz as seguintes condições:

$(i)\ d/a$ e d/b

(ii) Se c/a e c/b então $d \geq c$. Pela condição (i), d é divisor comum de a e b, e pela condição (ii), d é o maior divisor dentre os divisores comuns de a e b. Usaremos a notação $d = mdc(a, b)$ para indicar o máximo divisor comum de a e b.

É imediato que:

a) $mdc(0,0)$ não existe

b) $mdc(a,1) = 1$

c) Se $a \neq 0$ então $mdc = (a, 0) = |\ a\ |$

d) Se a/b então $mdc = (a, b) = |\ a\ |$

e) $mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b)$.

Exemplo: Sejam $a = 12$ e $b = 18$. Então $D(12) = \{1,2,3,4,6,12\}$ e D(18) = {1, 2, 3, 6, 9, 18}, logo $D(12) \cap D(18) = \{1,2,3,6\}$ e como o maior é 6 segue que $mdc(12,18) = 6$.

Exemplo: Se $a \in \mathbb{Z}$, ache os possíveis valores do $mdc(a, a + 10)$.

Faça $d = mdc(a, a + 10)$logo $d/a \Leftrightarrow (\exists q \in \mathbb{Z}; a = d.q)$ e $d/(a + 10) \Leftrightarrow (\exists q' \in \mathbb{Z}; a + 10 = d.q')$.

Portanto

$d.q + 10 = d.q' \Rightarrow 10 = d(q' - q) \Leftrightarrow d/10 \Rightarrow d \in \{1,2,5,10\}$.

Exemplo: O $mdc(a,b)$ quando existe é único. De fato, suponha que exista um outro $d' = mdc(a,b)$ para provar que $d = d'$. Como ded' satisfazem a condição (ii) segue se que d/d' e d'/d, isto é, $d = d'$.

Teorema: Se $d = mdc(a,b)$ então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$,

Hipótese: $d = mdc(a,b)$.

Tese: Existem $x, y \in \mathbb{Z}$tais que $d = ax + by$.

Prova: Seja $A = \{az + bw; z, w \in \mathbb{Z} eaz + bw > 0\}$.

Como $\varphi \neq A \subset \mathbb{N}$ pelo Princípio da Boa Ordenação existe um único $c = min(A)$ e pela construção de Aexistem $x, y \in \mathbb{Z}$ tais que $c = ax + by$.

Se $c \nmid a$pelo algarismo de Euclides existem valores únicos de $q, r \in \mathbb{Z}$tais $a = c.q + r, 0 \leq r < c$ logo $r = a - c.q = a - (ax + by).q = a(1 - x) + b(-qy) = ax' + by'$ com $x' = 1 - x$ e $y' = -yq$, ou seja, $r \in A$ o que é um absurdo visto que $r < c = min(A)$. Portanto c/a e de modo análogo c/b, isto é, c é um outro divisor comum de a e b e como por hipótese $d = mdc(a, b)$segue-se que $d \geq c$.

Também $d/a \Leftrightarrow (\exists q_1 \in \mathbb{Z}; a = d.q_1)$ e
$d/b \Leftrightarrow (\exists q_2 \in \mathbb{Z}; b = d.q_2)$ logo
$c = x(d.q_1) + y(d.q_2) = d(x.q_1 + y.q_2) \Rightarrow d/c \Leftrightarrow d \leq c$.

Das relações de ordem $d \geq c$ e $d \leq c$ conclui-se que $d = c = ax + by$.

Exemplo: Existem $x, y \in \mathbb{Z}$ tais que $c = ax + by$ se somente se $mdc(a, b)/c$.

É suficiente: Existem $x, y \in \mathbb{Z}$ tais que $c = ax + by$. Faça $d = mdc(a, b)$
então $d/a \Leftrightarrow (\exists q \in \mathbb{Z}; a = d.q)$ e $d/b \Leftrightarrow (\exists q' \in \mathbb{Z}; b = d.q')$ e assim $c = ax + by = (d.q)x + (d.q')y = d(qx + q'y) \Rightarrow d/c$.

É necessário: Faça $d = mdc(a, b)$ e d/c. Como $d = mdc(a, b)$ existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$ e como $d/c \Rightarrow (\exists q \in \mathbb{Z}; c = d.q)$, ou seja, $c = (ax_0 + by_0)q = a(x_0q) + b(y_0q) = ax + by$, onde $x = q.x_0 \in \mathbb{Z}$ e $y = q.y_0 \in \mathbb{Z}$.

Exemplo: Ache o menor inteiro $c > 0$ da forma $c = 22x + 55y$, onde $x, y \in \mathbb{Z}$.

Ora, c deve ser múltiplo de $11 = mdc(22,55)$, e o menor inteiro positivo nesta condição é $c = 11$.

Exemplo: Ache $a, b \in \mathbb{Z}$ sabendo que $a.b = 756$ e $mdc(a, b) = 6$.

Ora, $6/a \Leftrightarrow (\exists q_1 \in \mathbb{Z}; a = 6.q_1)$ e $6/b \Leftrightarrow (\exists q_2 \in \mathbb{Z}; b = 6.q_2)$ logo $ab = (6q_1)(6q_2) = 756$ o que implica em $q_1.q_2 = 21$.

Portanto $(q_1 = 7 e q_2 = 3)$ ou $(q_1 = 3 e q_2 = 7)$ e os números procurados são 18 e 42.

6.1. Inteiros relativamente primos

Sejam $a, b \in \mathbb{Z}$ não nulos simultaneamente. Dizemos que a e $b$são relativamente primos ou primos entre si, se e somente se $mdc(a, b) = 1$. Inteiros primos entre si admitem como únicos divisores comuns ± 1.

Exemplo: São primos entre si os inteiros $2 e 3, 3 e 4, 4 e 5$,

Exemplo: Dois números consecutivos a e $a + 1$ são primos entre si.

Com efeito, é imediato $1/a$ e $1/(a + 1)$. Se c/a e $c/(a + 1)$ então $c/(a + 1) - a$, isto é, $c/1 \Leftrightarrow c = 1$.

Teorema:

Os inteiros a e b, não simultaneamente nulos, são primos entre si, se e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Hipótese: $a, b \in \mathbb{Z}(a \neq 0 ou b \neq 0)$ e $mdc(a,b) = 1$.

Tese: Existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Prova: Para essa prova usa-se o teorema em (III.6) fazendo $d = 1$.

Hipótese: $a, b \in \mathbb{Z}(a \neq 0 ou b \neq 0)$ e existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Tese: $mdc(a,b) = 1$.

Prova: Faça $d = mdc(a,b)$ para provar que $d = 1$.

Como d/a e d/b então $d/(ax + by)$ e como por hipótese existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$ segue -se que $d/1 \Leftrightarrow d = 1$.

Corolário 1

Se $mdc(a,b) = d$ então os inteiros $\frac{a}{d} e \frac{b}{d}$ são primos entre si.

Hipótese: $d = mdc(a,b)$.

Tese: $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.

Prova: Como $d = mdc(a,b)$ então existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$ ou $\frac{a}{d}x + \frac{b}{d}y = 1$ e pelo Teorema anterior $mdc\frac{a}{d}, \frac{b}{d} = 1$.

Corolário 2

Se a/b e $mdc(b,c) = 1$ então $mdc(a,c) = 1$

Hipótese: a/b e $mdc(b,c) = 1$.

Tese: $mdc(a,c) = 1$

Prova: Por hipótese $a/b \Leftrightarrow (\exists q \in \mathbb{Z}; b = aq)$ e como $mdc(b,c) = 1$ pelo Teorema anterior existem $x, y \in \mathbb{Z}$ tais que $bx + cy = 1 \Rightarrow (a.q)x + c.y = 1 \Leftrightarrow a(q.x) + c.y = 1 \Leftrightarrow mdc(a,c) = 1$.

6.2. Máximo Divisor Comum de vários Inteiros

A definição de máximo divisor comum pode ser estendida para três inteiros a, b e c, não todos nulos, e assim definimos $mdc(a,b,c) = mdc(mdc(a,b),c)$.

Exemplo: O $mdc(4,6,8) = mdc(mdc(4,6),8) = mdc(2,8) = 2$.

Teorema: Se $a = b.q + r$ então $mdc(a,b) = mdc(b,r)$.

Hipótese: $a = b.q + r$ e $d = mdc(a,b)$.

Tese: $d = mdc(b,r)$.

Prova: Como $d = mdc(a,b)$ então $(d/a e d/b)$ logo $d/(a - b.q) = r$, isto é, d/b e d/r. Por outro lado, suponha c um divisor comum qualquer de b e r de modo que $(c/b e c/r)$ o que implica que $c/(b.q + r) = a$, isto é, c/b

e $c/a(cédivisorcomumdeaeb)$ e sendo $d = mdc(a,b)$ acarreta $d \geq c$, provando que $d = mdc(b,r)$.

Admitamos agora que queremos calcular o $mdc\,(a,b)$ com $a > b > 0$ e $b \nmid a$.

Então.

$a = b.q_1 + r_1, 0 \leq r_1 < b$

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

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

. .

. .

. .

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

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

Assim, pelo teorema anterior temos que

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

Exemplo: Ache $x, y \in \mathbb{Z}$ tais que $mdc\,(a,b) = ax + by$, para $a = 306$ e $b = 657$.

Temos $657 = 306.2 + 45$, $306 = 45.6 + 36$, $45 = 36.1 + 9$, $36 = 9.4 + 0$, isto é, $9 = mdc(306,657)$.

Por outro lado $9 = 45 - 36 = 45 - (306 - 45.6)$,

$9 = 45.7 - 306 = (657 - 306.2).7 - 306$,

$9 = 567.7 + 306.(-15)$

$9 = 567.x + 306y$, onde $x = 7$ e $y = -15$.

Exemplo: Determine $x, y \in \mathbb{Z}$ tais que $78x + 32y = 2$.

Temos $78 = 32.2 + 14$, $32 = 14.2 + 2$, $14 = 4.3 + 2$, $4 = 2.2 + 0$, isto é, $mdc\,(78,32) = 2$.

Por outro lado $2 = 14 - 4.3 = 14 - (32 - 14.2).3$, $2 = 14.7 - 32.3$, $2 = (78 - 32.2).7 - 32.3$, $2 = 78.7 + 32.(-17) = 78x + 32y$, onde $x = 7$ e $y = -17$.

Para refletir

1. Calcule:
$(a) mdc(a, a+1)$, a inteiro,
$(b) mdc(a, a+2)$, a inteiro par
$(c) mdc(a, a+2)$, a inteiro ímpar,
$(d) mdc(a, a+10)$, a inteiro,
$(e) mdc(a-1, a^2+a+1)$, a inteiro.
2. Se existem $x, y \in \mathbb{Z}$ tais que $mdc(a,b) = ax + by$ então $mdc(x,y) = 1$.
3. O mdc de dois naturais é 10 e o maior deles é 120. Ache o outro.
4. Ache $a, b \in \mathbb{N}$ tais que $a + b = 63$ e $mdc(a,b) = 9$.
5. Os restos das divisões de 4933 e 4435 por $a \in \mathbb{N}$ são, respectivamente, 37 e 19. Ache a.
6. Prove que, se a/c, b/c e $mdc(a,b) = 1$ então ab/c.
7. O $mdc(a,b) = 1 = mdc(a,c)$ se somente se $mdc(a,bc) = 1$.
8. Prove o Teorema de Euclides de Alexandria: Se a/bc e $mdc(a,b) = 1$então a/c.
9. Se a/bc e $mdc(a,b) = d$ então a/cd.
10. Se $mdc(a,4) = 2 = mdc(b,4)$ então $mdc(a+b,4) = 4$.
11. Se $A = \{x \in \mathbb{Z}; mdc(x,2) = 1\}$ e $B = \{x \in \mathbb{Z}; mdc(x,3) = 1\}$, ache $A \cap B$
12. Se $a \in \mathbb{Z}$ então $mdc(a, a+2) = \begin{cases} 2, apar \\ 1, aímpar \end{cases}$,
13. Se a/c, c/b e $mdc(a,b) = 1$, então $a = \pm 1$.
14. Se a e b são primos entre si então $mdc(2a+b, a+2b) = 1 ou 3$.
15. Determinar:
$(a) mdc(-816, 7209)$
$(b) mdc(-5376, -3402)$
$(c) mdc(209, 299, 102)$
16. Ache $x, y \in \mathbb{Z}$ tais que:
$(a) mdc(56, 72) = 56x + 72y$
$(b) mdc(1769, 2378) = 1769x + 2378y$.
17. Ache $x, y \in \mathbb{Z}$ tais que
$(a) 288x + 51y = 3$
$(b) 104x + 91y = 13$

7. Mínimo Múltiplo Comum de dois números

Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Chama-se Mínimo Múltiplo Comum de $a e b$ o número natural $m \in \mathbb{N}$ que satisfaz as condições:

$(i) a/m$ e b/m.

$(ii) Se a/n$ e b/n então $m \leq n$.

Pela condição (i), m é um múltiplo comum de a e b, e pela condição (ii), m é o menor dentre todos os múltiplos comuns de a e b.

Usaremos a notação $m = mmc(a,b)$ para indicar o mínimo múltiplo comum de a e b.

É imediato que:

a) mmc (0, 0) não existe.

b) Pelo princípio da Boa Ordenação o conjunto dos múltiplos comuns de a e b possui elemento mínimo, isto é, $mmc(a,b)$ existe sempre, e é único.

c) $mmc(a,b) \leq |ab|$.

d) Se a/b então $mdc(a,b) = |b|$.

e) $mmc(a,b) = mmc(-a,b) = mmc(a,-b) = mmc(-a,-b)$.

Exemplo: Se $a = 12$ e $b = 30$ então $M(12) = \{12,24,36,\ldots\}$ e $M(30) = \{30,60,90,\ldots\}$ logo $M(12) \cap M(30) = \{60,120,180,\ldots\}$ e como o menor é 60, segue-se que $mmc(12,30) = 60$.

7.1. Mínimo Múltiplo Comum de vários inteiros

O mínimo múltiplo comum pode ser estendido para três inteiros a, b e c, não nulos, e assim definimos $mmc(a,b,c) = mmc(mmc(a,b),c)$.

Exemplo:

O $mmc(2,4,6) = mmc(mmc(2,4),6)$, logo

$mmc(2,4,6) = mmc(4,6) = 12$.

7.2. Relação entre o Máximo Divisor Comum e o Mínimo Múltiplo Comum

Teorema: Se $a, b \in \mathbb{N}$ então $mdc(a,b).mmc(a,b) = ab$.

Hipótese: $a, b \in \mathbb{N}$, $d = mdc(a,b)$ e $m = mmc(a,b)$.

Tese: $d.m = ab$.

Prova: É imediato que $a/\frac{ab}{d}$ e $b/\frac{ab}{d}$ logo $\frac{ab}{d}$ é múltiplo comum de a e b, isto é, existe $q \in \mathbb{N}$ tal que $\frac{ab}{d} = m.q$ daí $\frac{a}{d} = \frac{m}{b}q$ e $\frac{b}{d} = \frac{m}{a}q$, ou seja $q/\frac{a}{d}$ e $q/\frac{b}{d}$.

Mas $d = mdc(a,b) \Leftrightarrow 1 = mdc\frac{a}{d}, \frac{b}{d} \Leftrightarrow \frac{a}{d}$ e $\frac{b}{d}$ são primos entre si e como q divide ambos, $q = 1$. De $\frac{ab}{d} = qm \Rightarrow \frac{ab}{d} = m \Leftrightarrow d.m = ab$.

Corolário: O $mdc(a,b) = ab$ se e somente se $mdc(a,b) = 1$, com $a, b \in \mathbb{N}$.

A prova é deixada como exercício, pois decorre imediatamente do teorema anterior.

Exemplo: Ache o $mmc(306,657)$.

Sabemos que mdc $(306, 657) = 9$ logo

$9.mmc(306,657) = 201042 \Rightarrow mmc(306,657) = 22338$.

Exemplo: Se $a, b \in \mathbb{N}$ e $mdc(a,b) = mmc(a,b)$ então $a = b$.

Hipótese: $a, b \in \mathbb{N}$, $d = mdc(a,b) = mmc(a,b)$.

Tese: $a = b$.

De fato, como $d = mdc(a,b)$ então $d/a \Leftrightarrow (\exists q \in \mathbb{N}; a = d.q)$ e $d/b \Leftrightarrow (\exists q' \in \mathbb{N}; a = d.q')$.

Também $d = mmc(a,b)$ então $a/d \Leftrightarrow (\exists q_1 \in \mathbb{N}; d = aq_1)$ e $b/d \Leftrightarrow (\exists q'_1 \in \mathbb{N}; d = bq'_1)$.

Mas $a = d.q = (aq_1)q \Rightarrow 1 = q_1 q \Leftrightarrow q = q_1 = 1$. De modo análogo $q' = q'_1 = 1$ e assim de $a = d$ e $b = d$ conclui–se que $a = b$.

Para refletir

1. Calcular:
$(a) mmc(-120,68)$
$(b) mmc(-42,-54)$
$(c) mmc(-20,77,-1200)$

2. Ache $a, b \in \mathbb{N}$ sabendo:
$(a) ab = 4033 e mmc(a,b) = 336$.
$(b) mdc(a,b) = 8 e mmc(a,b) = 560$
$(c) a + b = 589 e mmc(a,b) = 84 mdc(a,b)$.

3. Encontre os valores possíveis de a tal que $mmc(a, a+15) = 180$.

4. Se $a, b \in \mathbb{N}$ então $mdc(a,b)$ divide $mmc(a,b)$.

5. Se a e b são primos entre si então $mmc(a,b) = |ab|$

8. Números Primos

8.1. Números Primos e Compostos

Um natural $p > 1$ é um número primo se, e somente se $1 e p$ são seus únicos divisores. Se $p > 1$ não é primo é chamado composto. Um inteiro $p \in \mathbb{Z}$ é primo se, e somente se $p \neq 0, p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$.

Teorema 1: Se um primo p não divide $a \in \mathbb{Z}$ então p e a são primos entre si.

Hipótese: p é primo, $p \nmid a$ e $d = mdc(p,a)$,

Tese: $d = 1$.

Prova: Como $d = mdc(p,a)$ então d/p logo $d = 1$ ou $d = p$, pois p é primo. Também d/a e se $d = p$ então p/a, absurdo visto que por hipótese $p \nmid a$.

Portanto $d = 1$.

Corolário: Se p é primo tal que p/ab então p/a ou p/b.

Hipótese: p é primo, $a, b \in \mathbb{Z}$ e p/ab.

Tese: p/a ou p/b.

Com efeito, Se p/a então com efeito. Se $p \nmid a$ então pelo Teorema $1 mdc(p,a) = 1$. Mas por hipótese p/abe como $mdc(p,a) = 1$ pelo Teorema de Euclides de Alexandria p/b.

Teorema 2: Todo inteiro composto possui um divisor primo.

Hipótese: $a > 1$ inteiro composto.

Tese: a possui divisor primo .

Prova:

Seja $A = \{x \in \mathbb{N}; x/acomx \neq 1ex \neq a\}$, conjunto de todos os divisores de a, exceto os divisores triviais 1 e a. Como $\varphi \neq A \subset \mathbb{N}$ pelo princípio da Boa Ordenação existe um único $p = min(A)$ e vamos provar que pé primo. Suponha que não, ou seja, suponha $p$composto , logo $p$admite um divisor d tal que d/p daí $d < p$. Como $p \in A$, p/a logo d/a, isto é, d é divisor de a e menor que p, absurdo visto que $p = min(A)$ e assim p é primo.

Exemplo: Se a e b são primos entre si então ab e $a + b$ também são primos entre si.

Hipótese: $mdc(a,b) = 1emdc(ab, a+b) = d$

Tese: $d = 1$.

Suponha $d > 1$ logo pelo Teorema 2, d possui um divisor primo p que também é divisor de ab e $a + b$. Se p/ab então p/a ou p/b, pois p é primo. Suponha que p/a e como $p/(a+b)$ então $p/[(a+b)-a] = b$, isto é, p/a e p/b logo $p/mdc(a,b) = 1$, o que é um absurdo. Portanto $d = 1$.

8.2. Teorema Fundamental da Aritmética

Teorema: Para todo natural $a > 1$ existem primos $p_1, p_2, \ldots, p_r (r \geq 1)$ tais que $a = p_1, p_2, \ldots, p_r$. A decomposição de a é única, a menos da ordem dos $pi's$.

Prova: Se a é primo, então nada se prova. Se a não é primo então a é composto e pelo Teorema 2 de $3.7.1a$ possui um divisor primo p_1, isto é, $a = p_1.a_1$, $1 < a_1 < a$. Se a_1 é primo então nada se prova. Se a_1 não é primo então a_1é composto e pelo Teorema 2 de $3.7.1a_1$ possui um divisor primo p_2, isto é, $a_1 = p_2.a_2$, $1 < a_2 < a_1 < a$ e assim $a = p_1.p_2.a_2$. Continuando com este processo obtemos $1 < \ldots < a_2 < a_1 < a$, ou seja, existirá um número finito de naturais entre 1 e a e consequentemente existirá um a_r que é um primo $p_r (a_r = p_r)$ de modo que $a = p_1.p_2 \ldots p_r$.

Para provar a unicidade, suponha $a = q_1.q_2 \ldots q_s (s \geq 1)$, onde os $q_i$são primos logo $p_1.p_2 \ldots p_r = q_1.q_2 \ldots q_s$. Como $p_1/q_1.q_2 \ldots q_s$então p_1 divide pelo menos um dos fatores q_j. Sem perda de tempo, suponha que p_1/q_1 e como ambos são primos entre si $p_1 = q_1$. Cancelando p_1 com q_1 na igualdade inicial obtemos $p_2.p_3 \ldots p_r = q_2.q_3 \ldots q_s$. Continuando com este processo até quando for necessário, chegamos a conclusão que $r = s$ e assim provamos a unicidade.

Exemplo: Ache as decomposições de $a = 588$ e $b = 936$. Ache ainda $mdc(a,b)$e $mmc(a,b)$.

Temos $a = 588 = 2^2.3.7^2, b = 936 = 2^2.3^2.13$ logo
$mdc(a,b) = 2^2.3 = 12$ e
$mmc(a,b) = 2^3.3^2.7^2.13 = 45864$.

8.3. Infinidade de Primos

Teorema(Euclides de Alexandria): há uma infinidade de primos.

Prova: (Prova indireta): Suponha que exista um número finito de primos. Sejam $p_1, p_2, \ldots p_n$ a enumeração de todos os números primos e considere o número $n = p_1, p_2, \ldots p_r + 1$. Como $n > 1$ pelo Teorema de 3.7.2, ou n é primo ou n possui um fator primo p, que não pertence a nossa enumeração. Portanto o número de primos não pode ser finita, isto é, há uma infinidade de primos.

8.4. Como reconhecer um Número Primo

Teorema: Se o natural $a > 1$ é composto então a possui um divisor primo $p \leq \sqrt{a}$.

Prova: Se $a > 1$ é composto então a admite um divisor d, isto é, $d/a \Leftrightarrow a = dq$, $1 < d \leq q < a$. De $d \leq q \Rightarrow d^2 \leq d.q = a \Leftrightarrow d \leq \sqrt{a}$. Como $d > 1$, o Teorema de 3.7.2 assegura que d possui pelo menos um divisor primo p, ou seja, $d/p \Leftrightarrow p \leq d \leq \sqrt{a}$. Mas p/d e como d/a segue-se que p/a e consequentemente a possui um divisor primo $p \leq \sqrt{a}$.

O Teorema anterior é logicamente equivalente ao Teorema: "Se $a > 1$ não é divisível por nenhum primo $p \leq \sqrt{a}$ então a é primo".

Exemplo: Verifique se $a = 271$ é primo ou composto.

Ora, $16 \leq \sqrt{271}$ e os primos que não superam 16 são: 2,3,5,7,11 e 13 e nenhum deles é divisor de 271 logo $a = 271$ é primo.

Exemplo: Ache todos os pares de primos a e b tais que $a - b = 3$.

Como 3 é ímpar então a e b têm paridade diferentes. Mas o único primo par é 2 e a solução é $5 - 2 = 3$, isto é, $a = 5$ e $b = 2$.

Exemplo: Mostre que todo número primo é da forma $4k + 1$ ou $4k + 3$.

De fato, dividindo $a \in \mathbb{N}$ por $b = 4$ obtemos $a = 4.k + r, 0 \leq r < 4$ com restos possíveis $r = 0,1,2,3$. Portanto o natural a é de uma das formas $a = 4k(composto)$, $a = 4.k + 1(primo), a = 4k + 2(composto)$ e $a = 4.k + 3(primo)$.

Exemplo: Ache todos os primos que são divisores de $20!$

Ora, $20! = 1.2.3\ldots18.19.20$ logo os primos divisores de $20!$ são todos menores do que 20, sendo portanto $2,3,5,7,11,13,17,19$.

Exemplo: Mostre que a soma de inteiros positivos ímpares e consecutivos é sempre um inteiro composto.

Com efeito, dois inteiros ímpares e consecutivos têm as formas $2k+1$ e $2k+3$ logo $(2k+1)+(2k+3)=4(k+1)$ é múltiplo de 4, mostrando o que queríamos.

Exemplo: Mostrar que, se a^2+2 é primo então $3/a$.

Pois bem, dividindo a por $b=3$ encontramos $a=3k+r, 0 \leq r < 3$ e os possíveis restos são $r=0,1,2$.

Se $a=3k+1$ então $a^2 + 2 = (3k + 1)^2 + 2 = 3(k^2 + 2k + 1)$ *(composto)* e múltiplo de 3 Se $a = (3k + 2)$ então $a^2 + 2 = (3k + 2)^2 + 2 = 3(k^2 + 4k + 2)$ *(composto)*, e múltiplo de 3.

Portanto a^2+2 é primo se $a=3k \Leftrightarrow 3/a$.

Síntese do Capítulo

O objetivo a ser atingido nesse terceiro capítulo era conhecer o conjunto dos números naturais, onde definimos a indução matemática, estabelecemos a propriedade de ordem desse conjunto, propriedade esta, estendida ao conjunto dos inteiros. Nos naturais definimos números divisores e múltiplos, o mínimo múltiplo comum e o máximo divisor comum, culminando com os conceitos de números primos e compostos.

Atividades de avaliação

1. Ache os cinco menores primos da forma a^2-a.

2. Mostre que todo número primo é da forma $6k+1$ ou $6k+5$.

3. Sejam $a, b \in \mathbb{N}$ e p primo. Determine o valor lógico das proposições:

a) Se $p/(a^2+b^2)$ e p/a então p/b.

b)Se p/ab então p/a e p/b.

c) Se $p/(a+b)$ então p/a e p/b.

d) Se a/p então a é primo.

e) Se a/b e p/b então p/a.

4. Se a soma de dois naturais é primo então esses números são primos entre si.

5. Todo primo da forma $3k+1$ é também da forma $6m+1$.

6. Se p é primo e p/a^2 então p^2/a^2.

7. Se $a \in \mathbb{N}$ é composto então 2^{a-1} também o é.

8. Verifique se são primos ou composto os números:

$a)169 \qquad b)239 \qquad c)197 \qquad d)473$

9. Achar o *mdc* (*a*,*b*) e o *mmc* (*a*,*b*) se $a = 2^{30}.5^{21}.19.23^{3}$ e $b = 2^{6}.3.7^{4}.11^{2}.19^{5}.23^{7}$.

Capítulo 4

Equações Diofantinas

Objetivos

- Definir as equações Diofantinas.
- Estabelecer condições de existência de soluções.

Introdução

Este quarto capítulo é totalmente dedicada a um tipo especial de equações conhecidas como equações diofantinas, nome esse que homenageia o matemático grego Diofante de Alexandria seu idealizador.

1. Generalidades

Acredita-se que Diofante viveu aproximadamente oitenta e quatro anos. A principal obra de Diofante que conhecemos é a Aritmética, tratado que era originalmente de treze livros, dos quais só os seis primeiros se preservaram. Na Grécia antiga a palavra aritmética significava teoria dos números.

Era um tratado caracterizado por um alto grau de habilidade e de engenho, um marco na História da Matemática, o que influenciou outros matemáticos da sua época e de épocas posteriores. Foi escrevendo na margem desse livro a um amigo, que Pierre de Fermat ficou conhecido mundialmente com Último Teorema de Fermat.

Nessa obra, Diafonte introduz notações algébricas e estuda equações indeterminadas, modernamente chamadas equações diofantinas em sua homenagem. Diofante teve uma influência maior sobre as teorias modernas dos números do que qualquer outro algebrista grego não geométrico.

2. Definição

Uma equação da forma $ax + by = c, a, b, c \in \mathbb{Z}$ com a e b não simultaneamente nulos e $x, y \in \mathbb{Z}$ variáveis inteiras é chamada equação diofantina. Um par $(x_0, y_0) \in \mathbb{Z}x\mathbb{Z}$ tal que $ax_0 + by_0 = c$ é verdadeira é dito uma solução de equação diofantina $ax + by = c$

Existência de Solução

Teorema: Uma equação diofantina $ax + by = c$, com $a \cdot b \neq 0$ tem solução inteira se somente se $mdc(a,b)$ divide c.

É suficiente: Suponhamos que a equação $ax + by = c$, com $ab \neq 0$ tenha solução, isto é, existe o par $(x_0, y_0) \in \mathbb{Z}x\mathbb{Z}$ tal que $ax_0 + by_0 = c$ é verdadeira e $d = mdc(a,b)$, *devemos* provar que $d \mid c$. Mas $d \mid a \Leftrightarrow (\exists q \in \mathbb{Z}; a = dq)$ e $d \mid b \Leftrightarrow (\exists q' \in \mathbb{Z}; b = dq')$ logo $ax_0 + by_0 = (dq)x_0 + (dq')y_0 = d(qx_0 + q'y_0) \Rightarrow d \mid c$.

É necessário: Suponha $d \mid c$, com $d = mdc(a,b)$ para provar que a equação $ax + by = c$, com $a.b \neq 0$ tem solução. Mas $d = mdc(a,b)$ logo existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$ e também $d/c \Leftrightarrow (\exists s \in \mathbb{Z}; c = ds)$ logo $c = ds = (ax + by)s = a(xs) + b(ys) = ax_0 + by_0$ onde o par $(x_0 = xs, y_0 = ys) \in \mathbb{Z} \times \mathbb{Z}$ é solução da equação $ax + by = c$.

O Teorema anterior é logicamente equivalente ao teorema: "O $mdc(a,b) \nmid c$ se somente se a equação $ax + by = c$, com $ab \neq 0$ e $d = mdc(a,b)$ não possui solução inteira".

3. Solução da equação ax + by = c

Teorema: Se o par $(x_0, y_0) \in \mathbb{Z}x\mathbb{Z}$ é solução particular da equação $ax + by = c, d = mdc(a,b)$ e $d \mid c$ então todas as soluções de $ax + by = c$ com $a.b \neq 0$ são dadas pelo par $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \in \mathbb{Z} \times \mathbb{Z}$, onde $t \in \mathbb{Z}$.

Hipótese: O par $(x_0, y_0) \in \mathbb{Z}x\mathbb{Z}$ é solução de $ax + by = c$, isto é, $ax_0 + by_0 = c$ é verdadeira, $d = mdc(a,b)$ e $d \mid c$.

Tese: O par $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \in \mathbb{Z} \times \mathbb{Z}$ é a solução de $ax + by = c$.

Prova: Se o par (x'_0, y'_0) é uma outra qualquer solução de $ax + by = c$ então $ax'_0 + by'_0 = c$ é verdadeira e assim

$ax'_0 + by'_0 = ax_0 + by_0 \Leftrightarrow a(x'_0 - x_0) = b(y_0 - y'_0)$.

Mas $d \mid a \Leftrightarrow (\exists q \in \mathbb{Z}; a = dq)$ e $d \mid b \Leftrightarrow (\exists q' \in \mathbb{Z}; b = dq')$ logo substituindo a e b na identidade imediatamente acima encontramos $dq(x'_0 - x_0) = dq'(y_0 - y'_0)$ ou $q(x'_0 - x_0) = q'(y_0 - y'_0)$ daí

$q \mid q'(y_0 - y'_0)$ e $q' \mid q(x'_0 - x_0)$.

Como q e q' são primos entre si pelo Teorema de Euclides de Alexandria, $q \mid (y_0 - y'_0) \Leftrightarrow (\exists t \in \mathbb{Z}; y_0 - y'_0 = tq \Leftrightarrow y'_0 = y_0 - \frac{a}{d}t)$ e $q' \mid (x'_0 - x_0) \Leftrightarrow (\exists t \in \mathbb{Z}; x'_0 - x_0 = tq' \Leftrightarrow x'_0 = x_0 + \frac{b}{d}t)$.

Portanto o par $x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t \in \mathbb{Z} \times \mathbb{Z}$

é solução de $ax + by = c$.

De fato, temos

$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c$

Exemplo: Verifique se $56x + 72y = 40$ tem solução. Em caso afirmativo ache todas as soluções, inclusive a solução particular.

Vamos calcular o mdc (56, 72)

$72 = 56.1 + 16$

$56 = 16.3 + 8$

$16 = 8.2 + 0$

logo $mdc(56,72) = 8$ e mdc (56, 72) | 40 = c segue-se que a equação $56x + 72y = 40$ tem solução.

Mas

$8 = 56 - 16.3 = 56 - (72 - 56).3$

$8 = 72.(-3) + 56.4$

$8.5 = 72.(-3.5) + 56.(4.5)$

$40 = 72(-15) + 56.20$ e a solução particular é

$(x_0 = -15, y_0 = 20) \in \mathbb{Z} \times \mathbb{Z}$ e as demais são

$(x_0 + \frac{b}{a}t = -15 + 9t, y_0 - \frac{a}{d}t = 20 - 7t) \in \mathbb{Z} \times \mathbb{Z}, t \in \mathbb{Z}$.

Exemplo: Ache todas as soluções inteiras e positivas de $5x - 11y = 29$

Em valor absoluto

$11 = 5.2 + 1$

$-11 = 5.(-2) - 1 = 5(-2) - 1 + 5 - 5$

$-11 = 5.(-3) + 4$

$5 = 4.1 + 1$, $4 = 1.4 + 0$ logo $mdc(5,-11) = 1 \mid 29$ e assim $5x - 11y = 29$ tem solução.

Mas

$1 = 5 - 4 = 5 - (-11 + 5.3)$

$1 = 5.(-2) + 11.1$

$29 = 5.(-2.29) + 11(1.29)$

$29 = 5.(-58) - 11.(-29)$ e

a solução particular é $(x_0 = -58, y_0 = -29)$ e as demais $(x_0 + \frac{b}{a}t = -58 - 11t, y_0 - \frac{a}{d}t = -29 - 5t) \in \mathbb{Z} \times \mathbb{Z}, t \in \mathbb{Z}$.

Como queremos soluções inteiras e positivas deve-se fazer $-58 - 11t > 0$ e $-29 - 5t > 0$, isto é, para $t \leq -6$ todas as soluções serão inteiras e positivas.

Exemplo: Ache o menor inteiro positivo que dividindo por 8 e por 15 deixa os restos 6 e 13, respectivamente.

Seja $a \in \mathbb{N}$ o número procurado. Pelo enunciado

$a = 8x + 6 e a = 15y + 13 com x, y \in \mathbb{Z}$ logo

$8x + 6 = 15 + 3 \Leftrightarrow 8x - 15y = 7 (Equação odiofantina)$

Vamos encontrar $mdc(-15,8)$. Em valor absoluto

$15 = 8.1 + 7$

$-15 = 8.(-1) - 7 = 8.(-1) - 7 + 8 - 8$

$-15 = 8.(-2) + 1$-

$8 = 1.8 + 0$ logo $mdc(-15,8) = 1 divide 7$ e $8x - 15y = 7$ tem solução.

Mas

$1 = -15 + 8.2$

$7 = 8.(2.7) - 15.7$

$7 = 8.(14) - 15.7$ e a solução particular é $(x_0 = 14, y_0 = 7)$

e as demais $(14 - 15t, 7 - 8t) \in \mathbb{Z} \times \mathbb{Z}, t \in \mathbb{Z}$. Como queremos soluções positivas e inteiras, $14 - 15t > 0 e 7 - 8t > 0$, ou seja, $t = 0$.

Portanto $x = 14, y = 7 e a = 8x + 6 = 8.14 + 6 = 188$ ou

$a = 15y + 13 = 15.7 + 13 = 18$.

Exemplo: Se $a, b \in \mathbb{N}$ são primos entre si então a equação diofantina $ax - by = c$ tem um numero infinito de soluções inteira e positivas.

Hipótese: $a, b \in \mathbb{N}$ e $mdc(a,b) = d = 1$

Tese: $ax - by = c$ possui infinitas solução inteiras e positivas.

Prova: Ora, a equação $ax - by = ax + (-b)y = c$ tem solução pois

$mdc(a,-b) = mdc(a,b) = 1 que divide c$ e as demais

$(x_0 - bt, y_0 - at) \in \mathbb{Z} \times \mathbb{Z}, t \in \mathbb{Z}$.

Como queremos que elas sejam positivas, fazemos $x_0 - bt > 0 \Leftrightarrow t < \frac{x_0}{b}$ e $y_0 - at > 0 \Leftrightarrow t < \frac{y_0}{a}$.

Mas *t* é menor que os dois valores, logo existem infinitos valores para *t* e consequentemente a equação $ax - by = c$ possui infinitas soluções inteiras e positivas.

Síntese do Capítulo

Neste quarto capítulo estudamos as equações diofantinas, determinamos condições de existência e critérios de solução no universo dos inteiros relativos.

Atividades de avaliação

1. Verifique se as equações diofantinas seguintes tem soluções . Em caso afirmativo, ache todas as soluções, inclusive as soluções particulares

$a) 84x - 438y = 156$ $\quad b) 44x + 66y = 11$

$c) 21x - 12y = 72$ $\quad d) 32x + 55y = 771$

2. Ache todas as soluções inteiras e positivas das seguintes equações diofantivas.

$a) 123x + 360y = 99$ $\quad b) 58x - 87y = 290$

$c) 54x - 21y = 906$ $\quad d) 30x + 17y = 300$

3. Exprimir 100 como a soma de dois naturais de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.

4. Ache as duas menores frações positivas que tenham 13 e 17 para denominadores e cuja a soma seja igual a $\frac{305}{221}$.

5. Dividir 100 em duas parcelas positivas tais que uma é múltiplo de 7 e a outra de 11.

6. Ache todos naturais com a seguinte propriedade: "Fornecem resto 6 quando divididos por 11 e o resto 3 quando divididos por 7".

7. Um parque de divisões cobra R$ 1,00 a entrada de crianças e R$ 3,00 a de adultos. Para que a arrecadação de um dia seja R$ 200,00, qual o menor numero de pessoas, entre adultos e crianças, que poderiam frequentar o parque nesse dia ? Quantas crianças ? Quantos adultos ?

8. Um fazendeiro que dispõe de R$ 1.770,00 pretende gastar esta importância na compra de cavalos e bois. Se cada cavalo custa R$ 31,00 e cada boi R$ 21,00, qual o maior numero de animais que pode adquiri? Quantos cavalos? Quantos bois?

9. Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas tinham cada monte?

Capítulo 5

Congruências

Objetivos

- Definir congruência de dois inteiros.
- Conhecer propriedades da congruências.

Introdução

Neste quinto capítulo estudaremos a congruência de dois números inteiros. O conceito de congruência se baseia nos conhecimentos adquiridos nos capítulos anteriores, principalmente nos conceitos de divisibilidade e restos de uma divisão de dois inteiros.

1. Generalidades

Genial, talentoso e virtuoso foi o matemático, astronômico e físico alemão, Carl Friendrich Gauss (1777 – 1855) ou simplesmente Gauss. Conhecido como príncipe dos matemáticos é considerado o maior gênio da Historia da Matemática. É de entendimento de todos que apenas dois outros gênios da matemática podem se igualar a Gauss.: Arquimedes de Siracusa(287 a.C - 212 a.C ?) e Isaac Newton (1643 – 1727). Ademais, Gauss foi o mais precoce dentre todos os gênios da Matemática, considerada por ele a rainha das ciências, e Teoria dos Números a rainha da Matemática.

A obra de Gauss é bastante extensa e diversa. Entre suas inúmeras publicações, aos vinte e um anos, ele escreveu Disquisitiones Arithmeticae que só foi publicado em 1801. Grande parte desse trabalho serviu de base para o crescimento da Teoria dos Números, e vários resultados que trataremos neste capitulo, também encontram-se neste trabalho, até mesmo a notação lá utilizada, é a que utilizamos ainda hoje. Gauss, sem sombra de dúvida, foi um extraordinário matemático. Sua única ambição era o progresso matemático, pelo que lutou até a sua morte.

2. Inteiros Congruentes

Sejam $a, b \in \mathbb{Z}$ e o natural m. Dizemos que a é congruente a b módulo m se e somente se m divide a diferença $a - b$.

Usaremos a notação $a \equiv b mod m$ para indicar que a é congruente a b módulo m.

Em símbolos

$a \equiv b mod m \Leftrightarrow m \mid (a - b) \Leftrightarrow (\exists q \in \mathbb{Z}; a - b = m \cdot q)$.

Se m não divide a diferença $a - b$ então dizemos que a é incongruente a b módulo m e indica-se por $a \not\equiv b mod m$.

Exemplo: Trivialmente, $11 \equiv 3 mod 4$, pois $4 \mid 8 = (11 - 3)$. Mas $4 \nmid 6$ com $6 = 19 - 13$ logo $19 \not\equiv 13 mod 4$.

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

Hipótese: $a \equiv b mod m$ e r o resto da divisão de b por m, isto é, $b = mq + r, 0 \leq r < m$.

Tese: r é resto da divisão de a por m.

Prova: Por hipótese $a \equiv b mod m \Leftrightarrow (\exists k \in \mathbb{Z}; a - b = km)$ logo

$a = b + km = (mq + r) + km = m(q + k) + r$, isto é, r é resto da divisão de a por m.

Hipótese: $a = mq_1 + r, b = mq_2 + r, 0 \leq r < m$ e $q_1, q_2 \in \mathbb{Z}$

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

Prova: Ora, $a - b = (q_1 - q_2)m$ logo $m \mid (a - b) \Leftrightarrow a \equiv b mod m$

Exemplo: Sabendo que $1066 \equiv 1776 \text{mod} m$, ache todos os possíveis valores do módulo m.

Como $1066 \equiv 1776 \text{mod} m$, sejam $q_1 e q_2$ os quocientes das divisões de 1066 e 1776 por m e r o resto. Então $1066 \equiv q_1 m + r$ e $1776 \equiv q_2 m + r$ logo $1776 - 1066 = m(q_2 - q_1) \Leftrightarrow m \mid 710$ e assim m = 2, 5, 10, 142, 355, 710

Exemplo:

Se $k \equiv 1 \text{mod} 4$ então $6k + 5 \equiv 3 \text{mod} 4$.

Com efeito, se $k \equiv 1 \text{mod} 4$ então $k - 1 = 4q, q \in \mathbb{Z} \Rightarrow k = 4q + 1$.

Mas $6k + 5 = 6(4q + 1) + 5 = 4(6q + 2) + 3$, isto é, 3 é o resto da divisão de $6k + 5$ por 4 se, e somente se, $6k + 5 \equiv 3 \text{mod} 4$.

Exemplo: Mostre que todo primo $p (p \neq 2)$ é congruente $mod 4 a 1 ou 3$.

De fato, pelo algoritmo de Euclides $a = 4q + r, 0 \leq r < 4$ e

os possíveis restos são r = 0, 1, 2, 3,

Portanto

$a = 4q(par) ou a = 4q + 1 ou a = 4q + 2(par) ou a = 4q + 3.$

Se $p(p \neq 2)$ é primo então $p = 4q + 1 \Leftrightarrow p - 1 = 4q \Leftrightarrow p \equiv 1 \bmod 4$ ou $p = 4q + 3 \Leftrightarrow p - 3 = 4q \Leftrightarrow p \equiv 3 \bmod 4$.

Exemplo: Se $a \equiv b mod m$ então $mdc(a,m) = mdc(b,m)$.

Pois bem, como $a \equiv b mod m$ sejam $q_1, q_2 \in \mathbb{Z}$ os quocientes das divisões de a e b por m e r o resto. Então $a = mq_1 + r$ e $b = mq_2 + r$. Se $r = 0$ r = 0 então $a = mq_1$, logo $m \mid a$ daí $mdc(a,m) = m$. Também $b = mq_2$ logo m/b daí $mdc(b,m) = m$. Das duas identidades $mdc(a,m) = mdc(b,m)$.

Se $r \neq 0$ então

$mdc(a,m) = mdc(m,r) e mdc(b,m) = mdc(m,r) daí mdc(a,m) = mdc(b,m)$

Exemplo: Ache os naturais x, $0 < x \leq 15$ tais que $3x \equiv 6 mod 15$

Por definição, existe $y \in \mathbb{Z}$ tal que $3x - 6 = 15y \Leftrightarrow 3x - 15y = 6$. Mas $mdc(3,-15) = 3 \mid 6$ logo a equação diofantina $3x - 15y = 6$ possui solução.

Uma solução particular imediata é $x_0 = 7$, $y_0 = 1$ e as demais $(x = x_0 + \frac{b}{d}t = 7 - 5t, y = y_0 - \frac{a}{d}t = 1 - t) \in \mathbb{Z} \times \mathbb{Z}, t \in \mathbb{Z}$.

Como queremos soluções inteiras e positivas deve-se fazer $0 < x = 7 - 5t \leq 15$, isto é, $7 - 5t > 0 \Leftrightarrow t < \frac{7}{5}$ e $7 - 5t \leq 15 \Leftrightarrow t \geq \frac{-8}{5}$. Os valores inteiros de t são $t = 0, \pm 1$ logo $x = 2,7,12$

3. Propriedades dos Inteiros Congruentes

Sejam $a, b, c, d \in \mathbb{Z}$ e o natural m. São verdadeiras as seguintes propriedades:

P. 1 $a \equiv b mod m$.

Prova: Ora, $m \mid 0 = (a - a) \Leftrightarrow a \equiv a mod m$

P.2 Se $a \equiv b mod m$ então $b \equiv a mod m$.

Prova: Se $a \equiv b mod m$ então existe $q \in \mathbb{Z}$ tal que

$a - b = m \cdot q \Leftrightarrow b - a = m(-q) \Leftrightarrow b \equiv a mod m$.

P. 3 Se $a \equiv b mod m$ e se $b \equiv c mod m$ então $a \equiv c mod m$.

Prova: Se $a \equiv b mod m$ então existe $q_1 \in \mathbb{Z}$ tal que $a - b = mq_1$ e se $b \equiv c mod m$ então existe $q_2 \in \mathbb{Z}$ tal que $b - c = mq_2$.

Portanto,

$a - c = (a - b) + (b - c) = mq_1 + mq_2 = m(q_1 + q_2) \Leftrightarrow a \equiv c mod m$

P. 4 Se $a \equiv b mod m$ e se $c \equiv d mod m$ então $a \pm c \equiv (b \pm d) mod m$ e $ac \equiv bd mod m$.

Prova: Se $a \equiv b mod m$ então existe $q_1 \in \mathbb{Z}$ tal que $a - b = mq_1$ e se

$c \equiv dmodm$ existe $q_2 \in \mathbb{Z}$ tal que $c - d = mq_2$.

Portanto,

$(a + c) - (b + d) = (a - b) + (c - d) = mq_1 + mq_2 = m(q_1 + q_2) \Leftrightarrow a + c \equiv (b + d)modm$.

Como

$a - b = mq_1 \Leftrightarrow c(a - b) = ca - cb = m(cq_1) \Leftrightarrow ca \equiv cbmodm$.

P. 5 Se $a \equiv bmodm$ então $a \pm c \equiv (b \pm c)modm$ e $ac \equiv bcmodm$.

Prova: Se $a \equiv bmodm$ e como $c \equiv cmodm$ por P.4 $a \pm c \equiv (b \pm c)modm$.

P. 6 Se $a \equiv bmodm$ então $\mathrm{a}^n \equiv \mathrm{b}^n modm, n \in \mathbb{N}$.

Prova: (Indução sobre n)

É insofismável que para $n = 1$ a afirmação é verdadeira. Suponha verdadeira para $n = k$, isto é, $\mathrm{a}^k = \mathrm{b}^k modm$ é verdadeira, para provar que para $n = k + 1$ também o é.

Ora $a \equiv bmodm$, por hipótese indutiva $\mathrm{a}^k = \mathrm{b}^k modm$ e por P.4 $\mathrm{a}^k \cdot a \equiv \mathrm{b}^k \cdot bmodm \Leftrightarrow \mathrm{a}^{k+1} \equiv \mathrm{b}^{k+1} modm$. Portanto P.6 é verdadeira para todo n.

Exemplo: Mostre que 11 divide $10^{200} - 1$.

Com efeito, $10 \equiv -1\mathrm{mod}11$ logo

$10^{200} \equiv (-1)^{200} mod11 \Leftrightarrow 10^{200} \equiv 1\mathrm{mod}11 \Leftrightarrow 11 \mid (10^{200} - 1)$

Exemplo: Prove que $100 \mid (11^{10} - 1)$

De fato, $11^2 = 121 \equiv 21\mathrm{mod}100$ logo

$(11^2)^2 \equiv (21^2) mod100 \Leftrightarrow 11^4 \equiv 441\mathrm{mod}100$ e como

$441 \equiv 41\mathrm{mod}100$ segue-se que $11^4 \equiv 41\mathrm{mod}100$.

Ademais, $(11^4)^2 = (41^2) mod100 \Leftrightarrow 11^8 \equiv 1681\mathrm{mod}100$,

$1681 \equiv 81\mathrm{mod}100$ e assim $11^8 \equiv 81\mathrm{mod}100$. Portanto

$11^2 \cdot 11^8 \equiv 21 \cdot 81 mod100 \Leftrightarrow 11^{10} \equiv 1701\mathrm{mod}100$ e sendo

$1701 \equiv 1\mathrm{mod}100$ ocorre que

$11^{10} \equiv 1\mathrm{mod}100 \Leftrightarrow 100 \mid (11^{10} - 1)$.

Exemplo: Verifique que $2^{20} \equiv 1\mathrm{mod}41$

Ora, $2^7 = 128 \equiv 5\mathrm{mod}41$ e $2^6 = 64 \equiv 23\mathrm{mod}41$ logo

$2^7 . 2^7 . 2^6 \equiv 5.5.23\mathrm{mod}41 \Leftrightarrow 2^{20} \equiv 575\mathrm{mod}41$ e sendo $575 \equiv 1\mathrm{mod}41$segue-se que $2^{20} \equiv 1\mathrm{mod}41$.

Exemplo: Verifique se $-2 \equiv 2\mathrm{mod}8$

Ora, $-2 \equiv 2\mathrm{mod}8 \Leftrightarrow 8 \mid (-2 - 2)$. Como $8 \nmid (-4)$ então $-2 \not\equiv 2mod8$, isto é, não é verdade que $-2 \equiv 2mod8$.

Exemplo: Se a é um inteiro impar então $a^2 \equiv 1 mod 8$

Pois bem, na divisão de a por $b = 4$ encontramos $a = 4q + r, 0 \leq r < 4$ e os possíveis restos são $r = 0,1,2,3$.

Portanto *a = 4q (par) ou a = 4q + 1 (ímpar) ou a = 4q + 2(par) ou a = 4q + 3(ímpar)*

Se $a = 4q + 1$ então $a^2 = 8(2q^2 + q) + 1$, isto é, "a" deixa resto 1 quando dividido por 8 logo $a^2 \equiv 1 mod 8$. Se $a = 4q + 3$ então $a^2 = 8(2q^2 + 3q) + 1$, ou seja, "a" deixa resto 1 quando dividido por 8 logo $a^2 \equiv 1 mod 8$.

4. Critério de divisibilidade por 11

Temos $10 \equiv -1 mod 11$ logo $10^r \equiv -1 mod 11$ se r é ímpar e

$10^r \equiv 1 mod 11$ se *r* é par. Portanto

$a_0 \equiv a_0 mod 11$

$10a_1 \equiv -a_1 mod 11$

$10^2 a_2 \equiv a_2 mod 11$

.

.

.

$10^r a_r \equiv (-1^r) a_r mod 11$ e assim

$$a = a_0 + a_1 10 + a_2 10^2 + \ldots + a_r 10^r \equiv [a_0 - a_1 + a_2 - \ldots (-1^r) a_r] mod 11$$

.

Pelo Teorema de 5.2 "a" e $[a_0 - a_1 + a_2 - \ldots + (-1^r) a_r]$ deixam o mesmo resto quando divididos por 11.

Portanto "a" é divisível por 11 se, só se, 11 divide

$[a_0 - a_1 + a_2 - \ldots + (-1^r) a_r]$.

Síntese do Capítulo

Neste quinto e último capítulo estudamos a congruência entre dois números inteiros. Primeiramente definimos dois inteiros congruentes e estabelecemos propriedades para essa relação entre inteiros. Concluímos esta unidade demonstrando um critério de divisibilidade por 11, que ainda não conhecíamos.

Atividades de avaliação

1. Determine o valor lógico de cada uma das proposições seguintes:

$a) 17 \equiv 9 \bmod 2$ $\quad b) 1 \equiv 0 \bmod 7$

$c) 3+5+7 \equiv 5 \bmod 10$ $\quad d) 11^2 \equiv 1 \bmod 3$

$e) a \equiv 3 \bmod 5 \Rightarrow a \in \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

2. Ache todos os naturais x tais que:

$a)\ 0 < x \leq 200$ e $x \equiv -1 \bmod 7$.

$b)\ 0 < x \leq 100$ e $x \equiv 5 \bmod 8$

$c) 0 < x < 15$ e $3x \equiv 6 \bmod 15$

$d) 1 \leq x \leq 100$ e $x \equiv 7 \bmod 17$

3. Mostre que todo primo $p (p \neq 2,3)$ é congruente módulo 6 a 1 ou 5.

4. Provar:

$a)\ 89 \mid (2^{44} - 1)$ $\quad b)\ 97 \mid (2^{48} - 1)$

5. Se $a \in \mathbb{Z}$ então $a^3 \equiv 0, 1 ou 8 \bmod 9$

6. Mostrar que :

a) Se $a \equiv b mod m$ então $-a \equiv -b mod m$

b) Se $a + b = c mod m$ então $a \equiv (c - b) mod m$

c) Se $ac \equiv bc mod m$ e se $mdc(c, m) = d$ então $a \equiv b mod \frac{m}{d}$

d) Se $ac = bc mod mem dc(c, m) = 1$ então $a \equiv b mod m$

e) Se $ac \equiv bc mod mp$, p primo, e se $p \nmid c$ então $a \equiv b mod p$

7. O número $3145.253.9^9$ é divisível por 11 ?

Referências

ALENCAR FILHO, Edgard de. **Teoria elementar dos números.** São Paulo. Nobel, 1992.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números.** Rio de Janeiro. IMPA, 2009.

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

FIGUEIREDO, D. G. **Números irracionais e transcendentes.** Rio de Janeiro. Sociedade Brasileira de Matemática, 1985.

Sobre o autor

Francisco César Aires: é mestre em Matemática (UFC) e professor da UECE no curso de licenciatura em Matemática.