FUNDAMENTOS DE ÁLGEBRA I

Ana Cristina Vieira

FUNDAMENTOS DE ÁLGEBRA I

Belo Horizonte
Editora UFMG
2011

Vieira, Ana Cristina
V657f Fundamentos de Álgebra I / Ana Cristina Vieira. – Belo Horizonte : Editora UFMG, 2011.

75 p. : il. (Educação a Distância)

ISBN: 978-85-7041-842-5

1. Álgebra. 2. Matemática. I. Título. II. Série.

CDD: 512
CDU: 512

Elaborada pela DITTI – Setor de Tratamento da Informação
Biblioteca Universitária da UFMG

Este livro recebeu apoio financeiro da Secretaria de Educação a Distância do MEC.

ASSISTÊNCIA EDITORIAL Eliane Sousa e Euclídia Macedo
EDITORAÇÃO DE TEXTOS Maria do Carmo Leite Ribeiro
REVISÃO E NORMALIZAÇÃO Danivia Wolff
REVISÃO DE PROVAS Danivia Wolff
PROJETO GRÁFICO E CAPA Eduardo Ferreira
FORMATAÇÃO Sérgio Luz
PRODUÇÃO GRÁFICA Warren Marilac
IMPRESSÃO Imprensa Universitária da UFMG

EDITORA UFMG
Av. Antônio Carlos, 6.627 - Ala direita da Biblioteca Central - Térreo
Campus Pampulha - 31270-901 - Belo Horizonte - MG
Tel.: + 55 31 3409-4650 - Fax: + 55 31 3409-4768
www.editora.ufmg.br - editora@ufmg.br

PRÓ-REITORIA DE GRADUAÇÃO
Av. Antônio Carlos, 6.627 - Reitoria - 6º andar
Campus Pampulha - 31270-901 - Belo Horizonte - MG
Tel.: + 55 31 3409-4054 - Fax: + 55 31 3409-4060
www.ufmg.br - info@prograd.ufmg.br - educacaoadistancia@ufmg.br

A Educação a Distância (EAD) é uma modalidade de ensino que busca promover inserção social pela disseminação de meios e processos de democratização do conhecimento. A meta é elevar os índices de escolaridade e oferecer uma educação de qualidade, disponibilizando uma formação inicial e/ou continuada, em particular, a professores que não tiveram acesso a esse ensino.

Não se pode ignorar que é fundamental haver, sempre, plena conexão entre educação e aprendizagem. A modalidade a distância é um tipo de aprendizagem que, em especial na Universidade Federal de Minas Gerais (UFMG), já está concretizada como um ensino de qualidade. Hoje, a aprendizagem tornou-se, para todos os profissionais dessa universidade envolvidos no programa de Educação a Distância, sinônimo de esforço e dedicação de cada um.

Este livro visa desenvolver no curso a distância os mesmos conhecimentos proporcionados num curso presencial. Os alunos estudarão o material nele contido e muitos outros, que lhe serão sugeridos em bibliografia complementar. É importante terem em vista que essas leituras são de extrema importância para, com muita dedicação, avançarem em seus estudos.

Cada volume da coletânea está dividido em aulas e, em cada uma delas, trata-se de determinado tema, que é explorado de diferentes formas – textos, apresentações, reflexões e indagações teóricas, experimentações ou orientações para atividades a serem realizadas pelos alunos. Os objetivos propostos em cada uma das aulas indicam as competências e habilidades que os alunos, ao final da disciplina, devem ter adquirido.

Os exercícios indicados ao final de cada aula possibilitam aos alunos avaliarem sua aprendizagem e seu progresso em cada passo do curso. Espera-se que, assim, eles se tornem autônomos, responsáveis, críticos e decisivos, capazes, sobretudo, de desenvolver a própria capacidade intelectual. Os alunos não podem se esquecer de que toda a equipe de professores e tutores responsáveis pelo curso estará, a distância ou presente nos polos, pronta a ajudá-los. Além disso, o estudo em grupo, a discussão e a troca de conhecimentos com os colegas serão, nessa modalidade de ensino, de grande importância ao longo do curso.

Agradeço aos autores e à equipe de produção pela competência, pelo empenho e pelo tempo dedicado à preparação deste e dos demais livros dos cursos de EAD. Espero que cada um deles possa ser valioso para os alunos, pois tenho certeza de que vão contribuir muito para o sucesso profissional de todos eles, em seus respectivos cursos, na área da educação em geral do país.

Ione Maria Ferreira de Oliveira
Coordenadora do Sistema Universidade Aberta do Brasil
(UAB/UFMG)

Sumário

Introdução

Por *Teoria dos Números* entendemos a área da Matemática que se destina ao estudo de propriedades dos números inteiros. Euclides de Alexandria (360 a.C - 295 a.C - criador da famosa geometria euclidiana) foi o autor do mais antigo texto matemático (conhecido como *Os elementos*), dividido em um total de treze volumes (cada um deles denominado *Livro*). Os Livros VII, VIII e IX de *Os elementos* são sobre Teoria dos Números.

Neste texto, apresentamos uma introdução à Teoria dos Números, escrita em linguagem acessível a alunos a partir do segundo ano de graduação. Demonstramos resultados básicos que são muito importantes em diversos ramos da matemática, incluindo muitos dos teoremas clássicos provados por Euclides.

Vários resultados importantes são precedidos e seguidos de exemplos com o objetivo de ilustrar as ideias utilizadas nas demonstrações e motivar o leitor para a importância delas. Além dos problemas propostos, há um significativo número de problemas resolvidos.

Na Aula 1, apresentaremos o Princípio de Indução Matemática (PIM) em sua primeira forma, esclarecendo ao aluno a necessidade das demonstrações de afirmações a respeito de números naturais feitas a partir da indução após uma observação. Faremos isso cautelosamente já que o PIM é um dos princípios fundamentais na construção dos números naturais.

A segunda forma do PIM será apresentada na Aula 2, onde também apresentaremos o Princípio de Boa Ordem (PBO). Estes princípios serão ferramentas valiosíssimas em demonstrações nas aulas posteriores de resultados que envolvem números inteiros. Ainda nessa aula, introduziremos a importante sequência dos números de Fibonacci, cujas propriedades são interessantes e podem ser provadas com o uso do PIM e do PBO.

Na Aula 3, vamos demonstrar o Lema de Euclides tanto para números naturais quanto para inteiros. Este Lema é o carro-chefe da divisão de números inteiros, garantindo a existência do resto e do quociente em qualquer situação.

As propriedades elementares da divisibilidade no conjunto dos números inteiros serão estudadas na Aula 4, onde também vamos estabelecer alguns critérios de divisibilidade.

A Aula 5 é destinada ao estudo de números inteiros particulares: os números primos. Daremos a definição de primos e compostos e destacaremos a importância dos números primos na vida cotidiana. Vamos

ver resultados que dizem respeito à sua distribuição entre os naturais e faremos a demonstração da infinitude dos primos. Comentaremos alguns problemas em aberto sobre primos que são curiosamente estudados até hoje.

Daremos continuidade ao estudo de números primos na Aula 6, onde demonstraremos o Teorema Fundamental da Aritmética, que garante que todos os naturais a partir de 2 podem ser escritos como um produto de números primos. A unicidade desta fatoração implica em consequências interessantes na Teoria dos Números, conforme veremos.

Na Aula 7, nos ocuparemos do estudo de divisores comuns de dois inteiros, sendo destacado o máximo divisor comum (MDC). Veremos quais são as alternativas para calculá-lo e estudaremos suas principais propriedades.

Na Aula 8, introduziremos as chamadas equações diofantinas lineares, que se destinam a resolver problemas que tenham como soluções pares de números inteiros e veremos que a existência de tais soluções está relacionada com propriedades do MDC. Finalizaremos estudando o mínimo múltiplo comum (MMC) de dois inteiros e sua relação com o MDC.

Nas referências no fim deste texto destacamos alguns livros recentes em Teoria de Números que podem servir como bibliografia complementar para os estudantes. Lá também destacamos a página da web onde foram consultadas as informações históricas sobre os matemáticos citados no texto.

AULA 1

Princípio de Indução Matemática

OBJETIVOS
Vamos apresentar um dos postulados que caracterizam os números naturais: o Princípio de Indução Matemática. Em seguida, veremos como utilizá-lo para demonstrar afirmações a respeito desses números.

Na matemática, tal como numa ciência física, podemos utilizar a observação para descobrir leis gerais. Mas há uma diferença marcante. Nas ciências físicas, nem sempre há uma autoridade superior à observação, enquanto que na matemática essa autoridade existe: a prova rigorosa.

A prova (ou demonstração) de um resultado é feita, de maneira geral, utilizando-se outros resultados previamente estabelecidos, mas existem sentenças que não são provadas ou demonstradas e são consideradas como óbvias ou como um consenso inicial necessário para a construção ou aceitação de uma teoria.

Nesse contexto, usaremos *axioma*, *postulado* e *princípio* como sinônimos de uma hipótese inicial (que não será demonstrada) a partir da qual outros enunciados são logicamente derivados.

Aqui, vamos considerar o conjunto dos números naturais como o conjunto:

$$\mathbb{N} = \{0, 1, 2, \cdots\}.$$

O *Princípio de Indução Matemática*, que é um postulado baseado no último axioma de Giuseppe Peano (1858 - 1932), praticamente define este conjunto. Foi August de Morgan, que em 1883, descreveu o princípio cuidadosamente e deu a ele o nome de Indução Matemática.

Vamos entender como é este princípio e ver como utilizá-lo na demonstração de afirmações a respeito de números naturais.

Problema 1.1 O que é indução e o que é indução matemática?

Solução: A indução (ou dedução) é o processo de descoberta de leis gerais pela observação e combinação de exemplos particulares. É usada em todas as ciências, mesmo na matemática. A indução matemática é usada especificamente na matemática para provar teoremas de um certo tipo. Vamos ilustrar ambos os métodos por intermédio do mesmo exemplo.

Iniciamos observando que

$$1 + 8 = 9$$

e, reconhecendo os cubos e os quadrados, podemos dar ao fato observado a forma mais interessante:

$$1^3 + 2^3 = 3^2.$$

Como é que isto acontece? Será que, com frequência, uma tal soma de cubos sucessivos, a partir do número 1, é um quadrado? De fato,

$$1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36 = 6^2.$$

Em geral, será que é verdade que $1^3 + 2^3 + 3^3 + \cdots + n^3$ é um quadrado para todo natural n?

Fomos levados a esta pergunta pelos exemplos particulares $n = 2, 3$ e podemos investigar outros casos especiais. Os casos $n = 4$ e $n = 5$ são os próximos. Acrescentemos, para garantir um passo inicial, o caso $n = 1$. Arranjando elegantemente todos estes casos, obtemos:

$$\begin{aligned} 1^3 &= 1^2, \\ 1^3 + 2^3 &= 3^2, \\ 1^3 + 2^3 + 3^3 &= 6^2, \\ 1^3 + 2^3 + 3^3 + 4^3 &= 10^2, \\ 1^3 + 2^3 + 3^3 + 4^3 + 5^3 &= 15^2. \end{aligned} \tag{1.1}$$

É difícil acreditar que todas estas somas de cubos consecutivos sejam quadrados por mero acaso. De fato, uma pessoa que não esteja muito preocupada com formalismos teria poucas dúvidas de que a lei geral sugerida pelos casos especiais até então observados não seja correta e a consideraria provada por indução. O matemático expressa-se com maior reserva pois sente a necessidade de uma demonstração. Ele diria que o seguinte teorema é fortemente sugerido por indução:

A soma dos primeiros n cubos é um quadrado.

Vamos obsevar as bases dos quadrados que aparecem em (1.1): 1, 3, 6, 10, 15. Podemos ver aqui uma notável regularidade nestas bases:

$1 = 1$

$3 = 1+2$

$6 = 1+2+3$

$10 = 1+2+3+4$

$15 = 1+2+3+4+5$.

Se esta regularidade for geral (e o contrário é difícil de acreditar), a conjectura que fizemos toma uma forma mais precisa:

Para $n = 1, 2, 3, \cdots$ temos $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

A lei que acabamos de enunciar foi encontrada por indução. A indução tenta encontrar regularidade e coerência para além das observações. Mas, conforme já foi dito, é necessário uma demonstração formal para que um resultado em matemática seja aceito como verdadeiro.

Podemos fazer uma pequena simplificação no enunciado da nossa conjectura pois é fácil de verificar que

$$1+2+3+\cdots+n=\frac{n(n+1)}{2},\ \text{para todo } n=1,2,\cdots. \qquad (1.2)$$

Para ver isto, tomamos um retângulo com lados n e $n+1$ e fazemos o seguinte:

$\rightarrow$ Dividimos o retângulo em $n(n+1)$ quadrados de lados iguais a 1, como na Figura 1a que mostra o caso $n=4$ e temos 20 quadrados de lado 1.

$\rightarrow$ Preenchemos os quadrados com $*$ da seguinte maneira: o primeiro quadrado da primeira coluna, os dois primeiros quadrados da segunda coluna, os três primeiros quadrados da terceira coluna e assim por diante até preenchermos os n primeiros quadrados da n-ésima coluna, como na Figura 1b para $n=4$.

$\rightarrow$ Notamos que a área da região preenchida é igual a área da região não preenchida e é dada por $1+2+...+n$; para $n=4$ este valor é $1+2+3+4$ (ver Figura 1b).

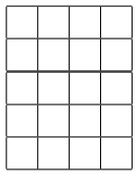


Figura 1a

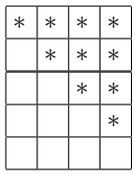


Figura 1b

Ora, a área total do retângulo é $n(n+1)$ da qual a área preenchida é metade. Isto prova a fórmula (1.2) acima.

Assim, podemos transformar o resultado que encontramos por indução em

$$1^3+2^3+3^3+\cdots+n^3=\left(\frac{n(n+1)}{2}\right)^2,\ \text{para todo } n=1,2,\cdots. \qquad (1.3)$$

Muito provavelmente, a fórmula é geralmente verdadeira, isto é, verdadeira para todos os valores de n.

Problema 1.2 Será que a afirmação continua verdadeira quando passamos de algum valor de n para o valor seguinte $n+1$?

Solução: Não sabemos ainda se (1.3) é verdadeira para um $n=k$ arbitrário, mas se soubéssemos que era verdade, teríamos

$$1^3+2^3+3^3+\cdots+k^3=\left(\frac{k(k+1)}{2}\right)^2$$

e poderíamos adicionar $(k+1)^3$ aos membros da equação obtendo

$$\begin{aligned}1^3+2^3+3^3+\cdots+k^3+(k+1)^3 &= \left(\tfrac{k(k+1)}{2}\right)^2+(k+1)^3\\ &= (k+1)^2\left[\tfrac{k^2+4(k+1)}{4}\right]\\ &= \left[\tfrac{(k+1)(k+2)}{2}\right]^2.\end{aligned}$$

Por virtude do que acabamos de dizer, a conjectura, ao ser verdadeira para $n = 6$, tem também de ser verdadeira para $n = 7$; ao ser verdadeira para $n = 7$, é verdadeira para $n = 8$; e assim sucessivamente. Ou seja, o resultado está provado em geral.

A prova precedente pode servir como padrão em muitos casos semelhantes. Se tivermos uma afirmação sobre números naturais que afirmamos ser verdadeira para todo natural n a partir de um natural a, podemos ser capazes de usar a experiência do exemplo anterior para concluir que a asserção será verdadeira se for provada para $n = a$ e se puder ser provada para $k + 1$, desde que seja admitida verdadeira para $n = k$.

Este processo é usado tantas vezes que merece um nome. Podíamos chamar-lhe "prova de n para $n+1$", mas o termo técnico aceito é *indução matemática*.

Em muitos casos, como no discutido acima em detalhes, a fonte é a indução, ou seja, a asserção é encontrada experimentalmente. Deste modo, a prova surge como um complemento matemático à indução; o que explica o nome.

Problema 1.3 Como fazer uma demonstração por indução?

Solução: A demonstração de uma afirmação a respeito de números naturais baseada no Princípio de Indução Matemática (PIM) é chamada uma *prova por indução*. Ela consiste de duas etapas:

• etapa 1: a demonstração de que a afirmação vale para um número natural inicial a (esta etapa é mais comumente chamada de *etapa inicial*);

• etapa 2: a demonstração de que a afirmação vale para o sucessor $k + 1$ de um número natural arbitrário $k > a$ depois de termos suposto que a afirmação vale para k. Esta suposição é chamada *hipótese de indução*.

Vamos agora estabelecer formalmente o PIM em sua forma mais simples.

PIM - primeira forma: Seja a um número natural. Suponha que para cada natural n, se tenha uma afirmativa $P(n)$ que satisfaça as seguintes propriedades:

(i) $P(a)$ é verdadeira (ou seja, a afirmativa vale para $n = a$);
(ii) se a afirmativa for verdadeira para um natural $k > a$ qualquer, então ela é verdadeira para o seu sucessor $k + 1$.

Então $P(n)$ é verdadeira para todo $n \geq a$.

É importante destacarmos que a indução matemática é constituída de duas etapas, cada uma de considerável importância, pois a primeira garante que estamos partindo de um fato verdadeiro para o natural inicial a; a segunda garante que ao assumir que a afirmação é verdadeira para um natural $k \geq a$ qualquer, então devemos garantir que ela é verdadeira para o seu sucessor; esta etapa consiste em demonstrar uma implicação.

Como um primeiro exercício, você pode observar que de fato provamos que (1.3) é verdadeira a partir do PIM - primeira forma.

Exemplo 1.1 Vamos provar por indução que a afirmação $P(n)$ abaixo é verdadeira:

$$(*) \quad 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}, \ \forall n \geq 1.$$

(a) Etapa inicial: verificar que vale $P(1)$. Mas isto é claro, pois $1 \cdot 2 = \frac{1(1+1)(1+2)}{3}$.

(b) Hipótese de indução: admitimos que vale $P(k)$, ou seja,

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}.$$

(c) Temos que provar que $P(k+1)$ é verdadeira. Para isto, somamos $(k+1)(k+2)$ em ambos os membros da igualdade acima (pois queremos a soma até $n = k+1$) e obtemos:

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) + (k+1)(k+2) &= \tfrac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= \tfrac{k(k+1)(k+2)+3(k+1)(k+2)}{3} \\ &= \tfrac{(k+1)(k+2)(k+3)}{3} \end{aligned}$$

e assim, o resultado está provado.

Cuidado: É extremamente importante que todas as etapas de indução sejam cumpridas para se evitar erros comuns entre os alunos, que chegam a "provar" conjecturas falsas pela falta do cumprimento dessa propriedade em suas demonstrações. Por exemplo, se não testamos a etapa inicial, corremos o risco de cometer este erro.

Exemplo 1.2 Vamos mostrar como é importante cumprir as etapas da indução através de um exemplo.

Se fizermos a seguinte afirmação:

$$1 + 2 + \cdots + n = \frac{1}{8}(2n+1)^2, \ \forall n \geq 1 \tag{1.4}$$

e iniciarmos uma demonstração por indução a partir da etapa 2, ignorando a etapa inicial, teremos como hipótese de indução que a afirmativa vale para $n = k$, ou seja, que

$$1 + 2 + \cdots + k = \frac{1}{8}(2k+1)^2$$

é verdadeira e a partir daí, somando $k+1$ em ambos os membros da igualdade, temos

$$1 + 2 + \cdots + k + (k+1) = \frac{1}{8}(2k+1)^2 + (k+1)$$

ou seja,

$$1 + 2 + \cdots + k + (k+1) = \frac{1}{8}(4k^2 + 4k + 1 + 8(k+1)) = \frac{1}{8}(2(k+1)+1)^2$$

e portanto a afirmação vale para $n = k+1$.

Teríamos de fato provado que (1.4) é verdadeira se tivéssemos garantida a etapa inicial. Mas para $n = 1$, em (1.4) temos $1 = \frac{1}{8}(2+1)^2$, o que é obviamente falso.

Logo, a afirmação (1.4) não é verdadeira.

Problema 1.4 Como demonstrar uma desigualdade usando PIM?

Solução: Devemos seguir as etapas da mesma forma como fizemos no Exemplo 1.1. Vamos provar o enunciado abaixo como exemplo:

$$2^n < n!, \ \forall n \geq 4.$$

(a) Etapa inicial: verificar que vale para $n = 4$. De fato vale, pois $2^4 = 16 < 24 = 4!$.

(b) Hipótese de indução: admitimos que vale para $n = k > 4$, ou seja, $2^k < k!$.

(c) Temos que provar que vale para $n = k + 1$. Observamos que

$$2^{k+1} = 2 \cdot 2^k$$

e usando a hipótese de indução, temos

$$2 \cdot 2^k < 2 \cdot k!$$

ou seja, $2^{k+1} < 2 \cdot k!$. Agora temos que comparar $2 \cdot k!$ com $(k + 1)!$ (que é onde queremos chegar).

Mas sabemos que $(k+1)! = (k+1) \cdot k!$ e como $2 < k+1$ (lembre que $k \geq 4$), multiplicando por $k!$ os dois lados da desigualdade (sem alterá-la) temos:

$$2 \cdot k! < (k + 1) \cdot k!$$

o que mostra que $2^{k+1} < (k + 1)!$.

O exemplo acima foi importante pois mostrou que muitas vezes temos que lançar mão de propriedades que não aparecem explicitamente para chegarmos a nossa conclusão.

No caso do exemplo, precisamos do fato "$2 < k + 1$" para terminarmos a demonstração. Em geral, esta necessidade surge naturalmente ao desenvolvermos a expressão que queremos provar. Portanto, você sempre deve observar atentamente o que precisa ser feito na etapa 2 do PIM em cada um dos exercícios.

Problema 1.5 Como fazer uma dedução?

Solução: Novamente, vamos resolver este problema através de um exemplo. Vamos deduzir a expressão geral que exprime de modo simplificado o produto:

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) ... \left(1 - \frac{1}{n^2}\right).$$

Note que não faz sentido considerarmos $n = 1$, já que começamos com $1 - \frac{1}{4}$. Assim, iniciamos com $n = 2$ e verificamos o que acontece para valores pequenos de n:

$$\text{Para} \ \ n = 2, \ \ \text{temos} \ \ 1 - \frac{1}{4} = \frac{3}{4}$$

$$\text{Para} \ \ n = 3, \ \ \text{temos} \ \ \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) = \frac{3}{4} \cdot \frac{8}{9} = \frac{2}{3}$$

Para $n = 4$, temos $\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right) = \frac{2}{3} \cdot \frac{15}{16} = \frac{5}{8}$

Para $n = 5$, temos $\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{25}\right) = \frac{5}{8} \cdot \frac{24}{25} = \frac{3}{5}$.

A princípio, parece que não há regularidade. Mas observando bem, parece que temos algo comum quando n é par.

Veja:

$$n = 2 \quad \rightarrow \quad \frac{3}{4} = \frac{2+1}{2 \cdot 2}$$

$$n = 4 \quad \rightarrow \quad \frac{5}{8} = \frac{4+1}{2 \cdot 4}$$

Note que é indicado deduzir que para n par o produto obtido corresponde a

$$\frac{n+1}{2n}.$$

Por outro lado, se observarmos bem, a expressão obtida para os casos em que n é ímpar nos dá:

$$n = 3 \quad \rightarrow \quad \frac{3+1}{2 \cdot 3} = \frac{4}{6} = \frac{2}{3}$$

$$n = 5 \quad \rightarrow \quad \frac{5+1}{2 \cdot 5} = \frac{6}{10} = \frac{3}{5}$$

ou seja, isto indica que o resultado também é verdadeiro para n ímpar. Deste modo, somos induzidos a acreditar que:

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) \ldots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}, \ \forall n \geq 2.$$

A demonstração de que a dedução é mesmo verdadeira, você fará no primeiro exercício da lista a seguir.

Exercícios

1 - Demonstre a dedução feita no Problema 1.5 por indução, para $n \geq 2$.

2 - Use indução matemática para provar que cada uma das afirmações abaixo é verdadeira para todo natural $n \geq 1$.

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

(b) $1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) $2 \cdot 2 + 3 \cdot 2^2 + 4 \cdot 2^3 + \cdots + (n+1)2^n = n2^{n+1}$.

(d) $2 \cdot 1 + 4 \cdot 3 + 6 \cdot 5 + \cdots + 2n(2n-1) = \frac{n(n+1)(4n-1)}{3}$.

3 - Use indução matemática para estabelecer cada desigualdade abaixo.

(a) $2^n > n^2$, para $n \geq 5$.

(b) $(1 + \frac{1}{2})^n \geq 1 + \frac{n}{2}$, para $n \in \mathbb{N}$.

(c) $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$, para $n \geq 2$.

4 - Considere $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(a) Calcule A^2 e A^3 para determinar uma fórmula possível para A^n, $n \geq 1$.

(b) Use indução para mostrar que a fórmula obtida em **(a)** é verdadeira.

5 - Encontre o erro na seguinte "prova": em qualquer grupo com n pessoas, todas elas têm a mesma idade.

Se um grupo consiste de uma pessoa, todas têm a mesma idade.

Suponha que em qualquer grupo com k pessoas, todas têm a mesma idade.

Sejam $a_1, a_2, ..., a_{k+1}$ as pessoas em um grupo com $k+1$ pessoas.

Desde que as pessoas $a_1, a_2, ..., a_k$ e $a_2, a_3, ..., a_{k+1}$ formam grupos com k pessoas, todas elas têm a mesma idade, por hipótese de indução.

Desde que a_2 está em cada um destes grupos, segue que todas as $k+1$ pessoas $a_1, a_2, ..., a_{k+1}$ têm a mesma idade.

6 - Encontre o erro na seguinte "prova", por indução matemática, que garante $2+4+6+...+2n = (n-1)(n+2)$, para todos os números naturais n.

Se assumimos que $2 + 4 + 6 + ... + 2k = (k-1)(k+2)$, para algum k, então

$$\begin{aligned} 2 + 4 + 6 + ... + 2(k+1) &= (k-1)(k+2) + 2(k+1) \\ &= k^2 + k - 2 + 2k + 2 \\ &= k(k+3) \\ &= [(k+1) - 1][(k+1) + 2], \end{aligned}$$

o que significa que sendo verdadeiro para k, é verdadeiro para $k+1$ e, portanto, é verdadeiro para todos os naturais.

7 - O que está errado com o seguinte argumento que afirma que *qualquer dívida de n dólares, $n \geq 4$, pode ser paga com notas de apenas 2 dólares*?

Logicamente a afirmação é válida para $n = 4$.

Considerando $k > 4$, suponhamos que a afirmação seja verdadeira para todo l, $4 \leq l < k$.

Devemos provar que a afirmação é verdadeira para $n = k$. Para isto, aplicamos a hipótese de indução a $k - 2$ e vemos que uma dívida de $k - 2$ dólares pode ser paga com notas de apenas 2 dólares. Adicionando mais uma nota de 2 dólares, vemos que podemos pagar uma dívida de k dólares com notas de apenas 2 dólares, como desejamos.

AULA 2

PIM e PBO

OBJETIVOS
Vamos estabelecer a segunda forma do PIM e introduzir a sequência de Fibonacci, que é uma sequência de números naturais com propriedades bastante importantes. Além disso, vamos estabelecer o Princípio de Boa Ordem (PBO) e provar a equivalência entre o PIM e o PBO.

Vamos iniciar apresentando uma interessante sequência de números naturais que constantemente aparece em problemas de matemática. Esta sequência foi estudada por Leonardo de Pisa (conhecido como *Fibonacci = filius* Bonacci) matemático e comerciante da Idade Média que, em 1202, escreveu um livro (*Liber abacci*) contendo uma grande quantidade de assuntos relacionados com a aritmética e álgebra da época e que realizou um papel importante no desenvolvimento matemático na Europa nos séculos seguintes, pois, através desse livro, os europeus vieram a conhecer os algarismos arábicos.

Um dos problemas que está nesse livro é o *problema dos pares de coelhos*:

> Um homem tem um casal de coelhos jovens em um ambiente inteiramente fechado. Desejamos saber quantos casais de coelhos podem ser gerados deste casal em um ano, se de um modo natural a cada mês ocorre a produção de um casal e um casal começa a produzir coelhos quando completa dois meses de vida.

Começando com um casal jovem, eles continuam jovens nos dois primeiros meses. Como o casal adulto produz um casal novo a cada 30 dias, no terceiro mês existirão dois casais de coelhos: 1 casal adulto + 1 casal recém-nascido.

No quarto mês, o casal adulto produzirá de novo mais um casal enquanto que o casal jovem terá completado 1 mês de vida e ainda não estará apto a produzir, assim no quarto mês existirão três pares de coelhos, sendo: 1 casal adulto + 1 casal com 1 mês de idade + 1 casal recém-nascido.

No quinto mês, existirão dois casais adultos sendo que cada um já produziu um novo casal e um casal novo que completou 1 mês, logo teremos 5 casais: 2 adultos + 1 com 1 mês + 2 recém-nascidos.

Tal processo continua através dos diversos meses até completar um ano. Observa-se esta formação na sequência numérica conhecida como a *sequência de Fibonacci*, que indica o número de casais a cada mês:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots$$

Considerando F_n o n-ésimo termo da sequência de Fibonacci, observamos que estes termos obedecem a uma regra de formação:

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad \text{para} \ \ n \geq 3$$

ou seja, os dois primeiros termos sao iguais a 1 e a partir do terceiro termo, cada termo é a soma dos dois termos anteriores (desta forma, esta sequência é *recursivamene definida*, pois conhecemos cada termo a partir dos anteriores).

Com esta observação, muitas são as propriedades da sequência de Fibonacci que podem ser provadas por indução.

Exemplo 2.1 Os termos da sequência de Fibonacci satisfazem:

$$F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$$

Devido à formação da sequência, a etapa inicial de indução deve ser testada para $n = 1$ e $n = 2$, em seguida usamos a recursividade. Assim, temos que a etapa inicial é válida pois:

$$F_1 = 1 = 2-1 = F_3-1 = F_{1+2}-1 \quad \text{e} \quad F_1+F_2 = 1+1 = 3-1 = F_4-1 = F_{2+2}-1.$$

Agora assumimos, por hipótese de indução, que vale para $n = k > 2$, ou seja, $F_1 + F_2 + \cdots + F_k = F_{k+2} - 1$. Vamos ter:

$$\begin{aligned} F_1 + F_2 + \cdots + F_k + F_{k+1} &= \overbrace{F_{k+2}} - 1 + \overbrace{F_{k+1}} \\ &= F_{k+3} - 1. \end{aligned}$$

Logo, vale para $n = k + 1$ e o resultado está provado.

Devido à recursividade da sequência de Fibonacci, em alguns casos não conseguimos provar resultados a respeito de seus termos diretamente a partir da primeira forma do PIM.

Para estes casos, existe uma forma alternativa que deve ser usada sempre que a prova para $P(k+1)$ não puder ser obtida diretamente da validade de $P(k)$, mas puder ser obtida a partir da validade de

$$P(a), P(a+1), \cdots, P(k).$$

Ou seja, quando pudermos provar que a afirmação é verdadeira para $k+1$ se assumirmos verdadeira para todos os naturais m entre a e k.

Para esta situação, vamos usar a segunda forma do princípio de indução matemática, enunciado abaixo.

PIM - segunda forma: Seja a um número natural. Suponha que para cada natural n, se tenha uma afirmativa $P(n)$ que satisfaça as seguintes propriedades:

(i) $P(a)$ é verdadeira;
(ii) se $P(m)$ for verdadeira para todo natural m com $a \leq m \leq k$ então $P(k+1)$ é verdadeira.

Então $P(n)$ é verdadeira para todo $n \geq a$.

Exemplo 2.2 Prove por indução que $F_n < \left(\frac{7}{4}\right)^n$, para todo $n \geq 1$.

Considerando que $P(n)$ é a nossa afirmação, temos:

(i) $P(1)$ e $P(2)$ são verdadeiras pois $1 < \frac{7}{4}$.

(ii) Usamos a segunda forma do princípio, tomando $k > 2$ e assumindo que:

$$P(m) \text{ é verdadeira para todo } 2 \leq m \leq k.$$

Desta forma, precisamos mostrar que $P(k+1)$ é verdadeira.

Como $k + 1 > 3$ temos, a partir da recursividade e da hipótese de indução:

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \\ &< \left(\tfrac{7}{4}\right)^k + \left(\tfrac{7}{4}\right)^{k-1} \\ &= \left(\tfrac{7}{4}\right)^{k-1}\left(\tfrac{7}{4} + 1\right) \\ &= \left(\tfrac{7}{4}\right)^{k-1}\left(\tfrac{11}{4}\right) \\ &< \left(\tfrac{7}{4}\right)^{k-1}\left(\tfrac{7}{4}\right)^2 \\ &= \left(\tfrac{7}{4}\right)^{k+1}. \end{aligned}$$

E temos válido o resultado.

Note que no exemplo anterior foi necessário usar a segunda forma do PIM pois precisamos de informações sobre $n = k$ e $n = k - 1$.

Agora vamos ver que a segunda forma do PIM pode ser demonstrada a partir da primeira forma do PIM.

Demonstração da segunda forma do PIM: Seja a um número natural. Suponha que para cada natural n, se tenha uma afirmativa $P(n)$ tal que:
(i) $P(a)$ é verdadeira;
(ii) se $P(m)$ for verdadeira para todo natural m com $a \leq m \leq k$ então $P(k+1)$ é verdadeira.

Queremos mostrar que $P(n)$ é verdadeira para todo natural $n \geq a$. Para isto, consideremos o seguinte conjunto:

$$A = \{n \in \mathbb{N} \mid n \geq a,\ P(a), P(a+1), \cdots, P(n) \text{ são verdadeiras }\}.$$

Pela condição (i), temos $a \in A$. Agora vamos mostrar que se $k \in A$ então $k + 1 \in A$ pois desta maneira, usando a primeira forma do PIM, todos os naturais $n \geq a$ estarão em A.

De fato, como $k \in A$ temos $k \geq a$, e $P(a), P(a+1), \cdots, P(k)$ são verdadeiras. Portanto, pela condição (ii) garantimos que $P(k+1)$ é verdadeira, ou seja, $k + 1 \in A$. Desta forma, A é formado de todos os naturais $n \geq a$, o que termina a demonstração.

□

Como uma última observação a respeito da sequência de Fibonacci, notamos que os termos desta sequência crescem indefinidamente, mas existe um fato interessante: tomando as razões (divisões) de cada termo pelo seu antecessor, obtemos uma outra sequência numérica cujo termo geral é dado por:

$$A_n = \frac{Fn + 1}{F_n}$$

e notamos que

$$A_1 = 1/1 = 1,$$
$$A_2 = 2/1 = 2,$$
$$A_3 = 3/2 = 1.5,$$
$$A_4 = 5/3 = 1.666...,$$
$$A_5 = 8/5 = 1.6,$$
$$A_6 = 13/8 = 1.625, \cdots .$$

As razões vão se aproximando de um valor particular, conhecido como *Número Áureo*, que é frequentemente representado pela letra grega ϕ e dado por

$$\phi = \frac{\sqrt{5}+1}{2}$$

ou seja,

$$\lim_{n\to\infty} A_n = \phi.$$

Note que ϕ é uma das raízes da equação $x^2 - x - 1 = 0$, ou seja, $\phi^2 = \phi + 1$.

Problema 2.1 Mostre por indução que

$$\phi^{n-2} \leq F_n \leq \phi^{n-1}, \quad \forall n \geq 2.$$

Solução: Vamos provar que $F_n \leq \phi^{n-1}$, $\forall n \geq 2$. Para o passo inicial de indução, temos $n = 2$:

$$\phi^{2-1} = \phi = \frac{\sqrt{5}+1}{2} > \frac{2+1}{2} > 1 = F_2$$

ou seja, é verdade que $F_2 \leq \phi^{2-1}$.

Suponhamos que para qualquer $2 < m \leq k$, seja verdade que $F_m \leq \phi^{m-1}$. Vamos ver o que ocorre quando $n = k + 1$:

$$\begin{aligned} F_{k+1} &= \underbrace{F_k} + \underbrace{F_{k-1}} \\ &< \phi^{k-1} + \phi^{k-2} \\ &= \phi^{k-2}\underbrace{(\phi+1)}_{\phi^2} \\ &= \phi^{k-2}\ \phi^2 \\ &= \phi^k. \end{aligned}$$

Com isso, provamos a primeira desigualdade. Agora, prove você a desigualdade $F_n \geq \phi^{n-2}$, $\forall n \geq 2$.

Problema 2.2 O que é o Princípio da Boa Ordem?

Solução: Para finalizar a aula, vamos introduzir este princípio e estabelecer sua equivalência com o PIM.

Antes de mais nada, observemos que para quaisquer dois números reais, podemos estabelecer uma comparação no sentido que

$$a < b \quad \text{ou} \quad a > b \quad \text{ou} \quad a = b,$$

isto é, o conjunto dos números reais $\mathbb{R}$ é bem ordenado.

Definição 2.1 *Dizemos que um subconjunto $S \subset \mathbb{R}$ é limitado inferiormente por um elemento $a \in \mathbb{R}$ se*

$$a \leq x, \quad \forall x \in S.$$

E neste caso, dizemos que é a uma cota inferior de S.

Exemplo 2.3 (i) O conjunto $S_1 = \{-1, 0, 1\}$ é limitado inferiormente por -1 (mas também é limitado inferiormente por qualquer real < -1).

(ii) O intervalo aberto $S_2 = (0, 1)$, ou seja, $S_2 = \{x \in \mathbb{R} \mid 0 < x < 1\}$ é limitado inferiormente por 0.

Note que nos exemplos acima, temos que $a_1 = -1$ é uma cota inferior de S_1 e $a_1 \in S_1$ mas $a_2 = 0$ é uma cota inferior de S_2 que não pertence a S_2.

Definição 2.2 *Se a for uma cota inferior de um conjunto S e $a \in S$ então dizemos que a é o menor elemento de S.*

Portanto, pelo exemplo acima, alguns subconjuntos de $\mathbb{R}$ não possuem menor elemento. De fato, o conjunto $S_2 = (0, 1)$ não possui menor elemento, pois se $a \in S_2$ fosse menor elemento de S_2 então teríamos

$$0 < a < 1 \quad \text{e} \quad a \leq x, \ \forall x \in S_2,$$

o que não é possível, pois $\frac{a}{2} < a$ e $\frac{a}{2} \in S_2$ (já que $0 < \frac{a}{2} < \frac{1}{2} < 1$).

Problema 2.3 Quando podemos garantir que um subconjunto de $\mathbb{Z}$ possui menor elemento?

Solução: A resposta vem com o PBO, que garante que um subconjunto S de inteiros tem menor elemento quando ele é não vazio e limitado inferiormente. O PBO será enunciado abaixo como um teorema, pois pode ser demonstrado usando a segunda forma do PIM.

Teorema 2.1 (Princípio da Boa Ordem - PBO) *Todo subconjunto $S \subset \mathbb{Z}$ não vazio e limitado inferiormente possui menor elemento.*

Demonstração: Suponhamos que $S \subset \mathbb{Z}$ seja um conjunto não vazio e limitado inferiormente por $a \in \mathbb{Z}$ e suponhamos, por absurdo, que S não possui menor elemento.

Vamos provar que S é vazio. Para isto, observamos primeiramente que $a \notin S$ pois, caso contrário, a seria o menor elemento de S. Agora, vamos assumir que

$$a, a+1, a+2, \cdots, a+k$$

não estejam em S e vamos provar que $a + (k+1) \notin S$. Desta maneira, pela segunda forma do PIM, vamos concluir que $b \notin S$ para todo $b \geq a$ e como todos os elementos em S são maiores ou iguais a a (pois a é cota inferior de S), vamos ter $S = \emptyset$.

De fato, se $a + (k+1) \in S$, então $a + (k+1)$ será o menor elemento de S, pois todos os inteiros maiores que a e menores que $a + (k+1)$ estão fora de S. Isto nos diz que $a + (k+1) \notin S$, o que garante que S é vazio. Este absurdo prova o resultado, ou seja, S possui menor elemento.

□

A resposta para o Problema 2.3 vem a partir do PBO, ou seja, quando temos um subconjunto de $\mathbb{Z}$ que é não vazio e limitado inferiormente, garantimos que ele tem menor elemento. Em particular, se $S \subset \mathbb{N}$ for um conjunto não vazio então S tem menor elemento (pois neste caso S é um subconjunto de $\mathbb{Z}$ limitado inferiormente por 0).

Problema 2.4 Como provar resultados a respeito dos números naturais usando o PBO?

Solução: Vamos resolver o problema fazendo um exemplo.

Exemplo 2.4 Vamos mostrar, usando PBO, que para todo $n \geq 1$ temos:

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

Você pode notar que esta é exatamente a afirmação (1.2) que, na primeira aula, provamos através de um argumento geométrico.

Vamos agora prová-lo por absurdo através do PBO. Para isto, queremos garantir que o conjunto dos naturais $n \geq 1$ para os quais não vale a igualdade acima é vazio.

Assumimos que o conjunto

$$S = \left\{ n \in \mathbb{N}, \quad n \geq 1 \ \mid \ 1 + 2 + 3 + \cdots + n \neq \frac{n(n+1)}{2} \right\}$$

é diferente de vazio.

Usando o PBO, S tem um menor elemento, ou seja, existe um elemento $a \in S$ tal que $a \leq x, \ \ \forall x \in S$. Antes de mais nada, note que $a \neq 1$ pois

$$\frac{1}{2} = \frac{1}{1+1} \ \text{ e assim } \ 1 \notin S.$$

Temos $a \geq 2$ e com isso, $a-1 \geq 1$ e $a-1 \notin S$ (pois $a-1 < a$). Deste modo,

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

isto é,

$$1 + 2 + 3 + \cdots + (a-1) = \frac{(a-1)a}{2}.$$

Assim, somando a aos membros da igualdade acima, temos:

$$1 + 2 + 3 + \cdots + (a-1) + a = \frac{(a-1)a}{2} + a,$$

o que implica em

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

Mas isto é um absurdo pois como $a \in S$ temos:

$$1 + 2 + 3 + \cdots + (a-1) + a \neq \frac{a(a+1)}{2}.$$

Esta contradição aconteceu pois admitimos que $S \neq \emptyset$. Logo, vale o contrário, quer dizer, $S = \emptyset$ e portanto $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \ \ \forall n \geq 1$.

Lembre que usando a primeira forma do PIM, provamos a segunda forma do PIM. No Teorema 2.1, usamos a segunda forma do PIM para provar o PBO. Agora vamos ver que usando o PBO podemos provar a primeira forma do PIM. Isto significa que ao aceitar cada um dos princípios como verdadeiro podemos provar os outros e, neste caso, dizemos que os princípios de indução (primeira e segunda formas) e o Princípio de Boa Ordem são equivalentes:

$$PIM \ \ (primeira \ forma) \Leftrightarrow PIM \ \ (segunda \ forma) \Leftrightarrow PBO.$$

Demonstração da primeira forma do PIM usando PBO: Vamos começar com as hipóteses da primeira forma do PIM, ou seja, temos a um número natural e uma afirmativa $P(n)$ para cada natural n que satisfaz as seguintes propriedades:

(i) $P(a)$ é verdadeira (ou seja, a afirmativa vale para $n = a$);
(ii) se $P(k)$ for verdadeira para um natural $k > a$ qualquer, então $P(k+1)$ é verdadeira para o seu sucessor $k+1$.

Queremos mostrar que $P(n)$ é verdadeira para todo $n \geq a$ e para isto vamos usar o PBO.

Neste caso, devemos mostrar que o conjunto dos naturais $n \geq a$ para os quais $P(n)$ é falsa é um conjunto vazio. Vamos supor o contrário, ou seja,

$$S = \{n \in \mathbb{N} \mid n \geq a, \quad P(n) \ \text{ é falsa } \} \neq \emptyset.$$

Pelo PBO, existe um elemento $s_0 \in S$ que é o menor elemento de S, ou seja,

$$P(s_0) \quad \text{é falsa} \quad \text{e} \quad s_0 \leq n, \ \forall n \in S.$$

Mas é claro que $s_0 \neq a$, pois $P(a)$ é verdadeira pela condição (i). Logo, $s_0 > a$ e assim, $s_0 - 1 \geq a$.

Como $s_0 - 1 < s_0$, devemos ter $s_0 - 1 \notin S$ (pois s_0 é o menor elemento de S). Portanto, $P(s_0 - 1)$ é verdadeira e, usando a condição (ii), isto implica que $P(s_0)$ é verdadeira, o que é absurdo.

Deste modo, $S = \emptyset$ e assim, garantimos a validade do resultado.

□

Exercícios

1 - Use o PIM para provar as propriedades abaixo entre os termos da sequência de Fibonacci, para todo natural $n \geq 1$.

(a) $F_1 + F_3 + \cdots + F_{2n-3} + F_{2n-1} = F_{2n}$.

(b) $F_2 + F_4 + \cdots + F_{2n-2} + F_{2n} = F_{2n+1} - 1$.

(c) $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.

2 - Termine a solução do Problema 2.1, ou seja, prove a desigualdade

$$F_n \geq \phi^{n-2}, \ \forall n \geq 2.$$

3 - Note que:

$$2 < 2^2$$
$$2^2 < 3^2$$
$$2^3 < 4^2$$
$$2^4 < 5^2.$$

Dedução: $2^n < (n+1)^2$, para todo $n \geq 1$.

Se a dedução for verdadeira, então demonstre por indução. Se for falsa, explique porque.

4 - Prove, utilizando indução, que o número de subconjuntos de um conjunto com n elementos é 2^n, $n \geq 1$.

5 - Considere $n, p \in \mathbb{Z}$ com $0 \leq p \leq n$ e o número binomial definido por

$$\left(\begin{array}{c} n \\ p \end{array} \right) = \frac{n!}{p!(n-p)!},$$

onde $n! = n.(n-1)...3.2.1$ e $0! = 1$.

(a) Demonstre a relação de Stiefel: $\left(\begin{array}{c} n \\ p \end{array} \right) = \left(\begin{array}{c} n-1 \\ p-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ p \end{array} \right)$, para $n, p \geq 1$.

(b) Mostre que $\left(\begin{array}{c} n \\ p \end{array} \right)$ é um número natural, para todos n, p nas condições da definição.

(c) Mostre a fórmula do binômio de Newton por indução:

$$(x+a)^n = \sum_{p=0}^{n} \left(\begin{array}{c} n \\ p \end{array} \right) a^p x^{n-p}, \quad n \in \mathbb{N}.$$

6 - Refaça o Exercício (2) da Aula 1 usando PBO.

7 - Defina o que é um *subconjunto limitado superiormente* de números reais. Defina o que é *cota superior* e o que é *maior elemento* de um conjunto.

8 - Use PBO para provar o seguinte: *se $S \subset \mathbb{Z}$ é não vazio e limitado superiormente, então S tem um maior elemento.*

AULA 3

Lema de Euclides

OBJETIVO
Vamos apresentar nesta aula o lema da divisão de Euclides, que já nos é bastante familiar e que é um ótimo exemplo de como podemos usar indução para fazer uma demonstração.

Euclides de Alexandria (360 a.C - 295 a.C) foi professor, matemático platônico de origem desconhecida e o maior responsável pelo desenvolvimento da famosa geometria euclidiana. Teria sido educado em Atenas e frequentado a Academia de Platão, em pleno florescimento da cultura helenística. O mais antigo texto matemático, *Os elementos*, é de sua autoria e nele foi incorporado praticamente todo o conhecimento matemático acumulado por seus antecessores em um total de 13 volumes (cada um deles denominado *Livro*).

Os Livros VII, VIII e IX de *Os elementos* são sobre teoria de números, sendo que por *número* os antigos gregos entendiam o que hoje denominamos número natural. Nestes Livros também são encontrados resultados sobre os números inteiros com demonstrações que são utilizadas até hoje e que, obviamente, foram reescritas em uma notação moderna.

Lembremos que o conjunto dos números naturais é formado de números inteiros não negativos $\mathbb{N} = \{0, 1, 2, \cdots\}$. O que o lema de Euclides basicamente faz é uma espécie de comparação entre dois números naturais. Vejamos abaixo.

Lema 3.1 (Euclides) Dados dois números naturais a e b, com $b \neq 0$, existem naturais q (quociente) e r (resto), unicamente determinados, tais que $a = bq + r$, onde $0 \leq r < b$.

Demonstração: A demonstração será feita por indução sobre a.

É claro que se $a = 0$ então tomamos $q = 0$ e $r = 0$, ou seja, a etapa inicial é verdadeira. Vamos assumir como hipótese de indução que vale para $a > 0$, ou seja, que existem q e r tais que $a = bq + r$, onde $0 \leq r < b$.

Agora vamos mostrar que vale para $a + 1$, exibindo um quociente q' e um resto r' tais que

$$a + 1 = bq' + r', \quad \text{com} \quad 0 \leq r' < b. \tag{3.1}$$

Usando a hipótese de indução temos:

$$a + 1 = bq + r + 1, \quad \text{com} \quad 1 \leq r + 1 < b + 1.$$

Deste modo, $r+1 \leq b$. Se $r+1 < b$, basta tomar $q' = q$ e $r' = r+1$ e temos (3.1).

Mas se $r+1 = b$, teremos $a+1 = bq+b = b(q+1)$ e portanto tomamos $q' = q+1$ e $r' = 0$, também garantindo (3.1).

Para provar a unicidade, suponhamos que temos dois pares de naturais (q_1, r_1) e (q_2, r_2) tais que

$$a = bq_1 + r_1 \quad \text{e} \quad a = bq_2 + r_2 \ , \quad \text{com} \quad 0 \leq r_1 < b \quad \text{e} \quad 0 \leq r_2 < b.$$

Queremos mostrar que $q_1 = q_2$ e $r_1 = r_2$. Suponhamos que isto não ocorra, ou seja, suponhamos que $q_1 \neq q_2$. Se são diferentes, então um deve ser maior ou menor que o outro. Podemos assumir, sem perda de generalidade, que $q_2 > q_1$. Neste caso, como $bq_1 + r_1 = bq_2 + r_2$, temos

$$r_1 - r_2 = b(q_2 - q_1) > b \quad (\text{pois} \quad q_2 - q_1 > 0),$$

o que não é possível já que $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Portanto, $q_1 = q_2$ e, assim,

$$r_1 = a - bq_1 = a - bq_2 = r_2$$

e o lema está provado.

□

Uma observação muito importante que podemos fazer após a demonstração do lema de Euclides é que existe uma maneira única de se escrever um número natural quando comparado com um outro natural. Ou seja, se a e b forem naturais não nulos, então a é de uma das formas (excludentes) abaixo com relação a b:

$$a = bq \ \text{ ou } \ a = bq+1 \ \text{ ou } a = bq+2 \cdots \text{ou } \ a = bq+(b-2) \ \text{ ou } \ a = bq+(b-1),$$

bastando para isto considerar os possíveis restos na divisão de a por b:

$$0, 1, 2, \cdots, b-1.$$

Quando o resto é zero, dizemos que a é um *múltiplo* de b, ou seja, a é múltiplo de b quando existe $q \in \mathbb{N}$ tal que $a = bq$.

Problema 3.1 Mostre que se $a \in \mathbb{N}$ então a^2 é da forma $3k$ ou $3k+1$, com $k \in \mathbb{N}$.

Solução: Pelo que observamos acima a é de uma das formas:

$$\text{ou} \quad (i)\ a = 3q \quad \text{ou} \quad (ii)\ a = 3q+1 \quad \text{ou} \quad (ii)\ a = 3q+2.$$

Deste modo, analisando cada caso:

$$\text{ou} \ \ (i)\ a^2 = (3q)^2 = \underbrace{3(3q^2)}_{forma\ 3k}$$

$$\text{ou} \ \ (ii)\ a^2 = (3q+1)^2 = \underbrace{3(3q^2+2q)+1}_{forma\ 3k+1}$$

$$\text{ou} \ \ (ii)\ a^2 = (3q+2)^2 = \underbrace{3(q^2+4q+1)+1}_{forma\ 3k+1}.$$

Problema 3.2 Dados 3 números naturais consecutivos, um (e somente um) deles é múltiplo de 3.

Solução: Os números dados podem ser escritos como

$$a, \quad a+1 \ \text{ e } \ a+2.$$

Mas o número a pode ser dividido por 3 deixando um (e somente um) resto, ou seja existe $q \in \mathbb{N}$ tal que $a = 3q + r$, onde $0 \leq r < 3$.

O resto r pode ser 0 ou 1 ou 2.

(i) Se $r = 0$ então temos $a = 3q$, ou seja, a é múltiplo de 3.

(ii) Se $r = 1$ então temos $a = 3q + 1$. Assim, $a + 2 = 3q_3 = 3(q + 1)$, ou seja, $a + 2$ é múltiplo de 3.

(iii) Se $r = 2$ então temos $a = 3q + 2$. Assim, $a + 1 = 3q_3 = 3(q + 1)$, ou seja, $a + 1$ é múltiplo de 3.

Observe que apenas uma das possibilidades (i), (ii) ou (iii) pode ocorrer, pela unicidade do resto na divisão euclidiana.

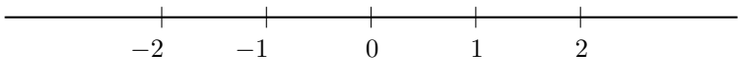
Problema 3.3 Mostre que dados n números naturais consecutivos, um, e somente um, deles é múltiplo de n.

Solução: Faça!

O Lema 3.1 pode ser generalizado para o conjunto dos números inteiros

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

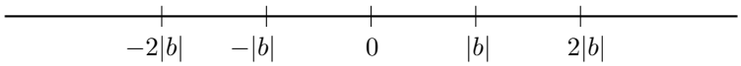
Sabemos que este conjunto pode ser representado sobre uma reta escolhendo um ponto arbitrário como zero e associando pontos à direita deste para serem os números positivos, e os da esquerda para serem os negativos.



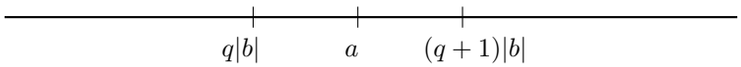
Recordemos ainda que o *valor absoluto* de um inteiro b é definido por

$$|b| = \begin{cases} b, & \text{se } \ b \geq 0 \\ -b, & \text{se } \ b < 0. \end{cases}$$

Observe ainda que, para qualquer inteiro b, o número $|b|$ é natural e $|b| = |-b|$. Assim, ao considerar $b \neq 0$, podemos dividir a reta de números inteiros considerando, a partir do zero, segmentos de comprimento $|b|$ como abaixo:



É importante notar que dados dois inteiros a e b com $b \neq 0$, podemos ter a como um múltiplo de b ou podemos localizar a entre dois múltiplos consecutivos de b:



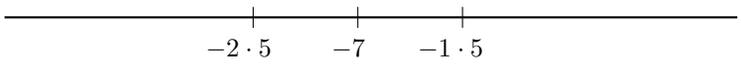
Esta informação pode ser expressa de duas maneiras:

$$a = q|b| + r, \quad \text{com} \quad 0 \leq r < |b| \tag{3.2}$$

ou

$$a = (q+1)|b| + r, \quad \text{com} \quad -|b| < r < 0. \tag{3.3}$$

Exemplo 3.1 Para $a = -7$ e $b = 5$ temos $q = -2$ e



ou seja:

$$-7 = \underbrace{-2}_{q} \cdot 5 + \underbrace{3}_{r_1}, \quad 0 < r_1 < |5|$$

ou

$$-7 = \underbrace{-1}_{q+1} \cdot 5 \underbrace{-2}_{r_2}, \quad -|5| < r_2 < 0.$$

Para não dar margem a dúvidas, escolhemos sempre o resto na forma (3.2) acima.

Desta maneira, assim como no caso dos naturais, vamos provar que temos dois inteiros: q (quociente) e r (resto), que serão unicamente determinados desde que escolhamos o resto para ser não negativo.

Agora, podemos generalizar o Lema 3.1 no seguinte:

Lema 3.2 (Euclides) Dados dois inteiros a e b, com $b \neq 0$, existem inteiros q e r unicamente determinados, tais que $a = bq + r$, onde $0 \leq r < |b|$.

Demonstração: A prova da existência de q e r será feita considerando os quatro casos possíveis abaixo:

Caso 1: $a \geq 0$ e $b > 0$.

Caso 2: $a \geq 0$ e $b < 0$.

Caso 3: $a < 0$ e $b > 0$.

Caso 4: $a < 0$ e $b < 0$.

Claramente não é necessário provar o caso 1 pois este é exatamente o Lema 3.1.

Para o caso 2, observamos que $|b| = -b > 0$ e recorremos novamente ao Lema 3.1. Deste modo, existem naturais q_1 e r_1 tais que:

$$a = (-b)q_1 + r_1, \quad \text{onde} \quad 0 \leq r_1 < -b.$$

Tomamos $r = r_1$ e $q = -q_1$, obtemos $a = bq + r$ dentro das condições exigidas, ou seja, $0 \leq r < |b|$.

No caso 3 temos $-a > 0$ e assim:

$$-a = bq_1 + r_1, \quad \text{com} \quad 0 \leq r_1 < b.$$

Logo, $a = -bq_1 - r_1$ e deste modo, se $r_1 = 0$, tomamos $r = 0$ e $q = -q_1$. Mas se $0 < r_1 < b$ então $0 < b - r_1 < b$. Tomamos $r = b - r_1$ e $q = -q_1 - 1$ pois, deste modo,

$$a = -bq_1 - r_1 + b - b = b(-q_1 - 1) + (b - r_1) = bq + r, \quad \text{onde} \quad 0 \leq r < |b|.$$

Finalmente, para o caso 4, temos $|a| = -a > 0$ e $|b| = -b > 0$ e, assim, ao usar o Lema 3.1, sabemos que existem naturais q_1 e r_1 tais que:

$$-a = (-b)q_1 + r_1, \quad \text{onde} \quad 0 \leq r_1 < -b$$

e portanto $a = bq_1 - r_1$. Novamente, se $r_1 = 0$ tomamos $r = 0$ e $q = q_1$. Mas se $0 < r_1 < -b$ então $0 < -b - r_1 < -b$. Deste modo, tomamos $r = -b - r_1$ e $q = q_1 + 1$ pois com isso temos

$$a = bq_1 - r_1 - b + b = b(q_1 + 1) + (-b - r_1) = bq + r, \quad \text{onde} \quad 0 \leq r < |b|.$$

Após garantir a existência do quociente e do resto na divisão euclidiana, vamos garantir a unicidade supondo que podemos escrever

$$a = |b|q_1 + r_1 \quad \text{e} \quad a = |b|q_2 + r_2, \quad \text{com} \quad 0 \leq r_1, r_2 < |b|.$$

Primeiramente, como r_1 e r_2 são ambos ≥ 0, note que

$$|r_1 - r_2| < |r_1| = r_1 < |b|.$$

Por outro lado, temos $|b|q_1 + r_1 = |b|q_2 + r_2$ e assim, $r_1 - r_2 = |b|(q_2 - q_1)$.

Portanto

$$|r_1 - r_2| = |b||q_2 - q_1|$$

Mas assim, $|r_1 - r_2|$ é um múltiplo de $|b|$ e é menor que $|b|$, consequentemente $|r_1 - r_2| = 0$. Logo $r_1 = r_2$ e $q_1 = q_2$, como queríamos mostrar.

□

Exemplo 3.2 Explicitamos o quociente e o resto da divisão em cada caso abaixo:

$$\begin{aligned}
\text{Para} \quad a = -17, b = 5: \quad & -17 = -4 \cdot 5 + 3, \\
\text{quociente} = -4, \quad & \text{resto} = 3 \\
\text{Para} \quad a = 17, b = -5: \quad & 17 = (-3) \cdot (-5) + 2, \\
\text{quociente} = -3, \quad & \text{resto} = 2 \\
\text{Para} \quad a = -17, b = -5: \quad & -17 = 4 \cdot (-5) + 3, \\
\text{quociente} = 4, \quad & \text{resto} = 3
\end{aligned}$$

Problema 3.4 Se a for um número inteiro, então mostre que exatamente um dos números a^2 ou $a^2 + 2$ é múltiplo de 3.

Solução: De fato, o Problema 3.1 também é verdadeiro quando $a \in \mathbb{Z}$ e assim, a^2 é da forma

$$3k \quad \text{ou} \quad 3k + 1, \quad \text{para algum inteiro} \quad k.$$

Assim, se $a^2 = 3k$ temos a^2 múltiplo de 3 enquanto que $a^2 + 2$ não é múltiplo de 3.

Mas se $a^2 = 3k + 1$ então $a^2 + 2 = 3(k + 1)$ é múltiplo de 3 e a^2 não o é.

Exercícios

1 - Na divisão de dois inteiros positivos, o quociente é 16 e o resto é o maior possível. Se a soma do dividendo e do divisor for 125, determine o resto.

2 - Mostre que se $a \in \mathbb{N}$ então $a^2 = 8c$ ou $a^2 = 8c + 1$ ou $a^2 = 8c + 4$, com $c \in \mathbb{N}$.

3 - Se $a \in \mathbb{Z}$, prove que exatamente um dos números $a,\ a + 9,\ a + 18$, ou $a + 27$ é múltiplo de 4.

4 - Mostre que o cubo de um natural n mais o seu dobro é sempre divisível por 3.

5 - Mostre que se $a, b \in \mathbb{Z}$ forem tais que $a^2 + ab + b^2$ deixa resto 0 na divisão por 3 então a e b deixam o mesmo resto na divisão por 3.

6 - Suponha que a seja um inteiro que é simultaneamente um quadrado e um cubo (por exemplo, para $a = 64$ temos $a = 8^2 = 4^3$). Prove que a é da forma $7k$ ou $7k + 1$, para algum inteiro k.

7 - Suponha que quando você divide um número ímpar a por 3, o resto seja igual a 1. Qual será o resto da divisão de a por 6?

8 - Quantos são os números naturais n, maiores que 0 e menores que 2006, tais que a expressão $\dfrac{n^3 - n}{6n - 6}$ é um número natural?

9 - Os restos das divisões de 247 e 315 por x são 7 e 3, respectivamente. Determine o maior valor possível para x.

AULA 4

Divisibilidade

OBJETIVOS
Trataremos mais cuidadosamente da condição "ser divisível por" e estudaremos as propriedades da divisibilidade de inteiros. Vamos também estudar alguns critérios de divisibilidade.

Como vimos, o resto dado pela divisão euclidiana é único. Euclides observou que o caso em que este resto é zero merece particular atenção. Vamos estudá-lo agora.

Definição 4.1 *Dados dois inteiros a e b dizemos que b divide a se existe um inteiro q tal que $a = bq$.*

Usaremos a notação: $b \mid a$ para indicar que b divide a.

Observação importante: Preste muita atenção: $b \mid a$ informa que "b divide a", não quer dizer "b dividido por a", ou seja, não indica o número racional $\frac{b}{a}$. Por exemplo, $2 \mid 6$ pois $6 = 2 \cdot 3$ e não expressa o racional $\frac{2}{6} = \frac{1}{3}$.

Portanto,

$$b \mid a \text{ se, e somente se, } \exists\, q \in \mathbb{Z} \text{ tal que } a = bq.$$

Isto equivale a dizer que o resto da divisão de a por b é zero. Neste caso, dizemos que b é um *divisor* de a ou que a é *divisível* por b, ou ainda que a é um *múltiplo* de b (como já foi usado no caso dos números naturais).

Outra observação importante: Quando demos a Definição 4.1, não nos preocupamos se os inteiros a e b eram nulos ou não. Note que, com a nossa notação, temos o seguinte:

Para $a = 0,\ b \neq 0$: $\quad b \mid 0$ é verdade, pois existe um inteiro $q = 0$ tal que

$$\underbrace{0}_{a} = b \cdot \underbrace{0}_{q}.$$

Para $a \neq 0,\ b = 0$: $\quad 0 \mid a$ é falso, pois não existe um inteiro q tal que

$$a = \underbrace{0}_{b} \cdot q.$$

O caso mais estranho ocorre quando $a = 0$ e $b = 0$. Será que podemos escrever $0 \mid 0$? Olhando para nossa definição, parece que sim pois para qualquer inteiro q temos:

$$\underbrace{0}_{a} = \underbrace{0}_{b} \cdot q$$

Novamente, neste último caso, temos que tomar cuidado pois o que informamos não foi que é possível escrever $\frac{0}{0}$ e sim que é possível usar a notação $0 \mid 0$. Vamos evitar estes casos estranhos considerando os inteiros como não nulos.

Proposição 4.1 *Se $a, b, c \in \mathbb{Z}$ forem não nulos então:*

(1) Se $a \mid b$ e $b \mid c$ então $a \mid c$.

(2) Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$ e $a \mid (b - c)$.

(3) Se $a \mid b$ então $a \mid bz$, para todo $z \in \mathbb{Z}$.

(4) Se $a \mid b$ e $a \mid c$ então $a \mid (bz + ct)$ para quaisquer $z, t \in \mathbb{Z}$.

Demonstração: A propriedade (1) garante a transitividade e isto é claro pois se $a \mid b$ e $b \mid c$ então

$$\exists\ q \in \mathbb{Z} \text{ tal que } \ b = aq \quad \text{e} \quad \exists\ \ k \in \mathbb{Z} \text{ tal que } \ c = bk.$$

Assim, $c = aqk$ com $qk \in \mathbb{Z}$ e portanto c é um múltiplo de a, ou seja, $a \mid c$.

Para provar a propriedade (2), basta ver que se $a \mid b$ e $a \mid c$ então

$$\exists\ q \in \mathbb{Z} \text{ tal que } \ b = aq \quad \text{e} \quad \exists\ \ k \in \mathbb{Z} \text{ tal que } \ c = ak.$$

Portanto, $b \pm c = aq \pm ak = a(q \pm k)$, o que garante que $a \mid (b \pm c)$.

A propriedade (3) é óbvia e a propriedade (4) decorre de (2) e (3).

□

Problema 4.1 Como decidir se um dado natural é divisível por outro?

Solução: Em algumas situações, é importante ter condições para responder a esta questão e isto é feito através dos *critérios de divisibilidade*. Vamos determinar alguns deles a partir de agora.

Quando escrevemos um número inteiro $a = a_n a_{n-1} \cdots a_1 a_0$, estamos expressando que

$$a = a_n \cdot 10^n + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0,$$

onde cada a_i é um algarismo entre 0 e 9, ou seja, a representação posicional considerada está num *sistema de numeração de base 10*. Por exemplo,

$$1358 = 1 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 8 \cdot 10^0.$$

Para as demonstrações dos critérios de divisibilidade que faremos nesta seção, estaremos sempre considerando que o número em questão está representado na base 10.

Proposição 4.2 (Divisibilidade por 2): *Um número natural a é divisível por 2 se, e somente se, o algarismo das unidades de a for divisível por 2.*

Demonstração: Escrevemos

$$a = a_n \cdot 10^n + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \quad \text{onde} \quad 0 \leq a_i \leq 9.$$

Assim,

$$a = 10(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) + a_0$$

ou seja, a é da forma $10k + a_0$. Deste modo, se $2 \mid a$ então como $2 \mid 10k$ vamos ter

$$2 \mid \underbrace{(a - 10k)}_{a_0}.$$

Reciprocamente se $2 \mid a_0$ então $a_0 = 2q$ para algum $q \in \mathbb{Z}$ e assim,

$$\begin{aligned} a &= 10(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) + 2q \\ &= 2\underbrace{[5(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) + q]}_{m}, \quad \text{com} \quad m \in \mathbb{Z}. \end{aligned}$$

e portanto $2 \mid a$.

□

Para garantir o critério de divisibilidade por 3, primeiramente provamos um lema.

Lema 4.1 Para todo natural $n \geq 1$, 10^n é da forma $3q + 1$.

Demonstração: Vamos provar este resultado por indução. Claramente vale para $n = 1$ pois $10 = 3 \cdot 3 + 1$. Suponhamos que vale para $n = k > 1$. Agora vamos mostrar que vale para $n = k + 1$. Temos:

$$10^{k+1} = 10^k \cdot 10 = (3q + 1) \cdot 10 = 30q + \underbrace{10}_{9+1} = 3\underbrace{(10q + 3)}_{m} + 1.$$

□

Proposição 4.3 (Divisibilidade por 3): *Um número natural a é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.*

Demonstração: Escrevemos

$$a = a_n \cdot 10^n + \cdots + a_2 10^2 + a_1 \cdot 10 + a_0, \quad \text{onde} \quad 0 \leq a_i \leq 9$$

e usamos o lema anterior, reescrevendo

$$\begin{aligned} a &= a_n \cdot (3q_n + 1) + \cdots + a_2 \cdot (3q_2 + 1) + a_1 \cdot (3q_1 + 1) + a_0 \\ &= 3\underbrace{(a_n \cdot q_n + \cdots + a_2 \cdot q_2 + a_1 \cdot q_1)}_{c} + \underbrace{(a_n + \cdots + a_2 + a_1 + a_0)}_{s}, \end{aligned}$$

isto é, $a = 3c + s$ e claramente, $3 \mid a$ se, se somente se, $3 \mid s$.

□

Proposição 4.4 (Divisibilidade por 9): *Um número natural é divisível por* 9 *se, e somente se, a soma dos seus algarismos for um número divisível por* 9.

Demonstração: A prova é análoga a que fizemos para garantir a divisibilidade por 3, usando o seguinte resultado (que você pode provar facilmente como foi feito no Lema 4.1):

$$\text{Para todo natural } n \geq 1, \text{o inteiro } 10^n \text{ é da forma } 9q+1.$$

□

Antes de enunciar o critério de divisibilidade por 11, vamos provar um lema parecido com o Lema 4.1.

Lema 4.2 Para todo natural $n \geq 1$, 10^n é da forma $11q + (-1)^n$.

Demonstração: Usaremos indução para provar este resultado. Claramente vale para $n = 1$ pois $10 = 11 - 1$. Vamos supor que vale para $n = k > 1$ e vamos mostrar que vale para $n = k + 1$. Temos:

$$\begin{aligned} 10^{k+1} &= 10^k \cdot 10 \\ &= (11q + (-1)^k) \cdot 10 \\ &= 11q \cdot 10 + (-1)^k \cdot \underbrace{10}_{11-1} \\ &= 11 \cdot 10q + 11 \cdot (-1)^k + (-1)(-1)^k \\ &= 11 \underbrace{(10q(-1)^k)}_{m} + (-1)^{k+1}. \end{aligned}$$

□

Proposição 4.5 (Divisibilidade por 11): *Um natural* $a = a_n a_{n-1} \cdots a_1 a_0$ *é divisível por* 11 *se, e somente se, a soma alternada dos seus algarismos*

$$a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$$

for um número divisível por 11.

Demonstração: Temos:

$$a = a_n \cdot 10^n + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \quad \text{onde} \quad 0 \leq a_i \leq 9$$

e usando o lema anterior, escrevemos:

$$\begin{aligned} a &= a_n \cdot (11q_n + (-1)^n) + \cdots + a_2 \cdot (11q_2 + (-1)^2) + a_1 \cdot (11q_1 + (-1)) + a_0 \\ &= 11 \underbrace{(a_n \cdot q_n + \cdots + a_2 \cdot q_2 + a_1 \cdot q_1)}_{k} + \underbrace{(a_0 - a_1 + a_2 - \cdots + (-1)^n a_n)}_{t}, \end{aligned}$$

isto é, $a = 11k + t$ e claramente, $11 \mid a$ se, se somente se, $11 \mid t$.

□

Problema 4.2 Fica como exercício a demonstração dos critérios abaixo e a pesquisa por outros que não foram citados.

Divisibilidade por 4: Um número natural é divisível por 4 se, e somente se, o número formado pelos seus dois últimos algarismos for divisível por 4.

Divisibilidade por 5: Um número natural é divisível por 5 se, e somente se, o seu último algarismo é 0 ou 5.

Divisibilidade por 6: Um número natural é divisível por 6 se, e somente se, ele é par e a soma de seus algarismos é divisível por 3.

Exercícios

1 - Algumas das afirmações abaixo são falsas (F) e outras são verdadeiras (V). Em todas elas, a, b, c, d são inteiros não nulos. Argumente convenientemente para verificar quais são (V) e quais são (F).

(a) Se $d \mid a$ e $d \mid b$ então $d^2 \mid ab$.

(b) $a \mid c$ e $b \mid d$ então $(a+b) \mid (c+d)$.

(c) $a \mid c$ e $b \mid d$ então $ab \mid cd$.

(d) $(a+b) \mid (c+d)$ então $a \mid c$ e $b \mid d$.

(e) $d \mid a$ e $d \mid b$ então $d \mid (a^2+b^2)$.

(f) $d \mid (a^9-b)$ e $d \mid a$ então $d \mid b$.

2 - Mostre que se a for um inteiro a^2-2 não é divisível por 4.

3 - Prove que se $a \in \mathbb{N}$ não for divisível por 2 e também não for divisível por 3 então a^2-1 é divisível por 24.

4 - Demonstre os critérios de divisibilidade por 4, por 5 e por 6.

5 - Determine critérios de divisibilidade por 7, por 8 e por 10.

6 - Mostre que um número natural com três algarismos, todos eles iguais, é divisível por 37.

7 - Mostre que para todo $n \geq 1$, $8 \mid 3^{2n}-1$ (sugestão: use PIM).

8 - Mostre que se a for um inteiro que deixa resto 3 na divisão por 6 então $72 \mid a^2-9$.

AULA 5

Números primos

OBJETIVOS
Nesta aula, nos preocuparemos com alguns números que são especiais: os números primos. Veremos como estes se distribuem na sequência de números naturais e a importância destes números na vida moderna.

No Livro VII de *Os elementos* de Euclides encontra-se a definição de números primos. Claramente, dado qualquer número inteiro n, os números 1, n, -1 e $-n$ são divisores inteiros de n. Vamos nos preocupar apenas com os divisores positivos de n. A pergunta é se existem outros além de 1 e n.

Definição 5.1 *Um número inteiro $n > 1$ é primo se seus únicos divisores positivos são 1 e n.*

Assim:

$$n \text{ é primo} \iff \text{se } a \mid n,\ a > 0 \text{ então } a = 1 \text{ ou } a = n.$$

Caso o número $n > 1$ não seja primo, dizemos que ele é *composto*, ou seja,

$$n \text{ é composto} \iff \text{existe } a \mid n,\ a > 0 \text{ tal que } a \neq 1 \text{ e } a \neq n.$$

Neste caso, $n = ab$, onde a e b são inteiros e $1 < a, b < n$. Note que o número 1 não é classificado nem como primo, nem como composto.

Claro que 2 é um número primo e é o único primo que é par. Não é difícil dar outros exemplos de números primos, podemos listar os iniciais

$$2, 3, 5, 7, 11, 13, 17, 19, \cdots$$

e chegar até certo ponto sem problemas, mas podemos questionar se é possível determinar uma fórmula para gerar números primos, ou seja:

Problema 5.1 É possível determinar uma função f, tal que dado um número natural não nulo n, $f(n)$ seja um número primo?

Solução: Vamos responder a esta questão considerando as situações em que isto pode ocorrer ou não.

O célebre matemático Pierre de Fermat (1601-1665) saiu em busca de uma fórmula para primos e conjecturou que todos os números da forma

$$F(n) = 2^{2^n} + 1$$

onde n é um inteiro positivo, são primos. Por exemplo: $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, $F(4) = 65537$ são todos primos.

Porém, em 1732, Leonhard Euler (1707-1783) mostrou que $F(5)$ (um inteiro de 10 algarismos) é divisível por 641 e portanto não é primo.

Um resultado bem conhecido da álgebra afirma que **não existe um polinômio, com coeficientes racionais, que produza somente números primos**. Embora estabeleça uma limitação para a geração de números primos, este resultado não exclui a existência de:

a) funções polinomiais em uma variável que gere números primos, mas não todos;
b) funções não polinomiais que gerem números primos, todos ou não;
c) funções polinomiais em mais de uma variável que produzam números primos, todos ou não.

Muitos professores e estudantes de matemática desconhecem o fato de que existem funções com cada uma das características acima, como nos seguintes exemplos.

a) Considere a função $f(n) = n^2 - n + 41$, com n sendo um número natural. Já sabemos que esta fórmula não pode produzir todos os primos pois é um polinômio em uma variável com coeficientes inteiros. Mas o fato curioso é que para $n = 1, 2, 3, ..., 40$, temos $f(n)$ primo, enquanto que para $n = 41$ tem-se $f(41) = 41^2$, ou seja, não é primo.

b) Um exemplo do segundo tipo é a função dada em 1971 pelo matemático J. M. Gandhi, que fornece o n-ésimo número primo em função dos $n - 1$ primos anteriores:

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d|A_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor$$

onde p_n é o n-ésimo número primo, $A_{n-1} = p_1 p_2 ... p_{n-1}$ é o produto dos $n-1$ primeiros primos, $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x e μ é função de Möbius dada por $\mu(n) = (-1)^m$ caso n seja igual ao produto de m primos distintos $q_1, \cdots, q_m$, e $\mu(n) = 0$ caso contrário.

c) Exemplo em: http://www.mat.puc-rio.br/~nicolau/papers/mersenne/node18.html.

Problema 5.2 Qual o menor divisor positivo diferente de 1 de $a = 235$? E de $b = 344$? E de $c = 91$?

Solução: Note que as respostas são $d_1 = 5$ para a, $d_2 = 2$ para b e $d_3 = 7$ para c. Em qualquer caso, foi um número primo. De fato, temos que:

Teorema 5.1 *Se $n \geq 2$ for um número natural então n possui um divsor que é um número primo.*

Demonstração: Para provar este resultado, usamos a segunda forma do PIM. Se $n = 2$, é claro que o resultado vale.

Suponhamos que $k > 2$ e que o resultado vale para $2 \leq m < k$, ou seja, dado qualquer natural m entre 2 e k, m possui um divisor primo.

Vamos provar que vale para $n = k + 1$. Se $k + 1$ for primo, não temos nada a fazer. Caso contrário, $k+1$ tem um divisor d tal que $1 < d < k+1$. Deste modo, usando a hipótese de indução, d possui um divisor primo e como este será também divisor primo de $k + 1$, o resultado está demonstrado.

□

Problema 5.3 Existe uma maneira de testar se um número é primo?

Solução: Existe uma grande quantidade de *testes de primalidade* que garantem se um determinado número é primo ou não. Podemos exemplificar um destes testes com o resultado abaixo.

Proposição 5.1 *Se n for um número natural composto, então n possui (pelo menos) um divisor primo $p \leq \sqrt{n}$.*

Demonstração: Para um número composto n existem divisores $1 < a, b < n$ tais que $n = ab$. Além disso, não podemos ter simultaneamente $a > \sqrt{n}$ e $b > \sqrt{n}$ (caso contrário $n = ab > \sqrt{n}\sqrt{n} = n$, o que é absurdo). Logo, pelo menos um dos divisores (digamos que seja a) tem que ser $\leq \sqrt{n}$. Mas, pela proposição anterior, a possui um divisor primo e assim concluímos que n possui um divisor primo $\leq \sqrt{n}$.

□

Desta forma, o resultado anterior nos informa que para um dado número natural $n \geq 2$, se constatarmos que todos os primos $p \leq \sqrt{n}$ não são divisores de n, então podemos concluir que n é primo.

O inconveniente do teste acima é que se o número for muito grande, determinar todos os primos anteriores a ele pode ser uma tarefa extremamente difícil. De fato, mais a frente veremos como é o comportamento da função que dá a quantidade de primos até um inteiro fixado.

Uma lista de números primos: Segundo a tradição, a primeira tabela de números primos foi criada pelo matemático grego Eratóstenes (c. 285-194 a.C.), o terceiro bibliotecário-chefe da Biblioteca de Alexandria. Ele desenvolveu um procedimento que, mais tarde, passou a se chamar de *crivo de Eratóstenes*.

Vamos exemplificar o crivo, determinando a lista de números primos entre 1 e 100.

Inicialmente, determina-se o maior número a ser checado. Ele corresponde à raiz quadrada do valor limite, arredondado para baixo de acordo com a Proposição 5.1. No nosso caso, a raiz de 100, que é 10. Em seguida, faça o seguinte:

• Crie uma lista de todos os números inteiros de 2 até o valor limite: $2, 3, \cdots, 99, 100$.

• Encontre o primeiro número da lista. Ele é um número primo, 2.

• Remova da lista todos os múltiplos do número primo encontrado (exceto o próprio número). No nosso exemplo, a lista fica formada de 2 seguido de todos os ímpares até 99.

• O próximo número da lista é primo, 3. Repita o procedimento, removendo seus múltiplos; a lista fica: 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97. O próximo número, 5, também é primo; repetindo o processo sucessivamente até o último número a ser checado (ou seja, até 10), a lista contendo todos os primos até 100 será:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

No Livro IX dos Elementos, Euclides provou um importante resultado sobre a quantidade de primos existentes.

Teorema 5.2 *Existem infinitos números primos.*

Demonstração: Uma simples demonstração pode ser dada por absurdo, considerando que temos um número finito de números primos e que $p_1, p_2, ..., p_k$ sejam todos os primos existentes.

O inteiro $m = p_1 \cdot p_2 \cdots p_k + 1$ não é primo pois não é igual a nenhum dos listados. Portanto, pelo Teorema 5.1, possui um divisor primo. Porém, este divisor não é nenhum dos primos já considerados, pois caso seja algum dos p_i temos $p_i \mid p_1 \cdot p_2 \cdots p_k + 1$ mas como $p_i \mid p_1 \cdot p_2 \cdots p_k$ chegaríamos ao absurdo que $p_i \mid 1$. Com este argumento, garantimos que existem infinitos números primos.

□

Problema 5.4 Como os números primos se distribuem entre os naturais?

Solução: O problema da distribuição dos primos entre os naturais foi considerado por Gauss (1777-1855), que estudou o comportamento de uma função que fornece a quantidade de primos até um fixado inteiro x. Ele fez uma conjectura sobre esta função que foi provada por Hadamard e Poussin em 1896.

Teorema 5.3 *Se $\pi(x)$ denota o número de primos menores ou iguais a um dado inteiro x, então:*

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

Pelo teorema, se x for muito grande temos :

$$\pi(x) \approx \frac{x}{\log x}.$$

Exemplo 5.1 Vamos ver como se comportam os primos no intervalo $(10^{100}, 10^{101})$. Para determiná-los, fazemos o seguinte:

→ Geramos um ímpar $b \in (10^{100}, 10^{101})$.

→ Verificamos se ele é primo. Se não for, testamos $b+2$ e assim por diante, até encontrarmos um primo.

A questão é: em média, quantos serão os números testados até encontrarmos um número primo?

Pelo Teorema 5.3 temos

$$\pi(10^{100}) \approx \frac{10^{100}}{\log 10^{100}} \qquad \pi(10^{101}) \approx \frac{10^{101}}{\log 10^{101}}.$$

Logo, a probabilidade de um b ímpar no intervalo ser primo é:

$$\pi(10^{100}) - \pi(10^{101}) \approx \frac{210^{-2}}{\log 10} \approx \frac{1}{115},$$

ou seja, deverão ser gerados cerca de 115 números ímpares no intervalo antes que um primo seja encontrado.

Problema 5.5 Para que precisamos determinar primos tão grandes?

Solução: Atualmente, os fatores primos de números monstruosos são usados como chaves de criptografia (*kryptos* = oculto, *graphos* = escrever) que fazem parte da segurança nacional de muitos países. Isto porque, ao multiplicarmos dois primos tremendamente grandes, podemos considerar uma mensagem criptografada cuja quebra do sigilo consiste em fatorar o número obtido, e o processo de fatoração neste caso pode ser praticamente impossível.

Exemplo 5.2 O número $2^{193} - 1$ é um número gigantesco. Seus fatores primos são:

$$p = 13.821.503,$$

$$q = 61.654.440.233.248.340.616.559;$$

$$r = 14.732.265.321.145.317.331.353.282.383.$$

Para um número da ordem de 10^{130}, um computador comum levaria 50 anos para efetuar a sua fatoração. E para um número da ordem de 10^{308}, mesmo com os esforços combinados de 100 milhões de computadores, seriam necessários mais de 1000 anos!

Problema 5.6 Mostre que dado um número natural n, existe uma sequência de n naturais consecutivos todos compostos.

Solução: Este problema parece incrível pois quando o número n é muito grande, temos uma sequência enorme de números consecutivos onde nenhum deles é primo.

O problema pode ser resolvido ao verificarmos que os n números consecutivos

$$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4, \cdots, (n+1)!+n, (n+1)!+(n+1)$$

são todos compostos, pois 2 divide $(n+1)!+2$, 3 divide $(n+1)!+3, \cdots, n$ divide $(n+1)!+n$ e $n+1$ divide $(n+1)!+(n+1)$.

Números de Mersenne: Marin Mersenne (1588-1648) estudou os números da forma

$$M_n = 2^n - 1$$

sendo n um número primo. Esses números são chamados de números de Mersenne. São conhecidos números de Mersenne tanto primos, como compostos. Por exemplo,

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$$

são números primos, enquanto

$$M_{11} = 23 \cdot 89$$

é composto.

Atualmente o maior número primo conhecido é o primo de Mersenne

$$2^{43.112.609} - 1,$$

descoberto no dia 23 de agosto de 2008, num projeto de computação distribuído pela internet, o GIMPS, que usa o tempo ocioso do processador de computadores pessoais, procurando por números primos específicos, do tipo $2^p - 1$, em que p é primo. O último primo encontrado é o primo de Mersenne de número 46 e tem 12.978.189 dígitos.

Problemas a respeito de números primos encantam a humanidade há muitos séculos, muitos deles ainda estão em aberto, ou seja, não foram provados até hoje. Vejamos alguns exemplos.

Definição 5.2 *Dois números primos dizem-se gêmeos se a sua diferença for* 2*.*

Os primeiros pares de números primos gêmeos são

$$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43),$$

$$(59,61), (71,73), (101,103), (107,109)$$

(sequência A001097 na OEIS - veja Moreira; Saldanha (1999)). Os maiores números primos gêmeos conhecidos são

$$2.003.663.613 \cdot 2^{195.000} \pm 1,$$

descobertos em janeiro de 2007.

Problema 5.7 (em aberto): Existe uma infinidade de números primos gêmeos? Este problema é muito antigo, tendo Euclides conjecturado que sim. Esta conjectura é chamada de conjectura dos primos gêmeos.

Definição 5.3 *Um número de Fermat* $F(n) = 2^{2^n} + 1,\ n \in \mathbb{N}$, *que é primo, é dito um primo de Fermat.*

Até hoje são conhecidos apenas cinco números primos de Fermat:

$$F(0), F(1), F(2), F(3), F(4).$$

Todos os números de Fermat $F(n)$ para $5 \leq n \leq 23$, assim como números enormes tais como $F(23288)$ e $F(23471)$, são comprovadamente compostos.

Problema 5.8 (em aberto): Serão finitos os números primos de Fermat? Se forem finitos, quantos são?

Exercícios

1 - Encontre todos os primos p e q tais que $p - q = 3$.

2 - Três naturais ímpares consecutivos são primos. Mostre que estes números são 3, 5 e 7.

3 - Verifique se 38.567 é um número primo.

4 - Mostre que $n^4 + 4$ é sempre um número composto quando $n \in \mathbb{Z}$ e $|n| \neq 1$.

5 - Verifique se é verdadeiro ou falso, justificando.
(a) Se a e b forem ímpares então $a + b$ não é primo.
(b) Se $a + b$ for um primo > 2 então a e b não podem ser simultaneamente ímpares.
(c) Se a e b forem dois primos e $a + b$ também é primo então $a = 2$ e $b = 3$.

6 - Mostre que se a soma de dois primos gêmeos for igual a 24 então um dos primos é 13.

7 - Determine primos gêmeos p e q tais que $p^2 + q^2 = 34$.

8 - Mostre que a soma de dois primos gêmeos p e $p + 2$, com $p > 3$, é um múltiplo de 12.

9 - Se $a > 1$ e $a^2 + 2$ for um número primo, então mostre que a é um múltiplo de 3.

AULA 6

Teorema Fundamental da Aritmética

OBJETIVOS
Vamos demonstrar o Teorema Fundamental da Aritmética, que é um dos principais teoremas a respeito de números primos. Vamos apresentar também importantes aplicações que podemos fazer com o uso deste.

Os gregos foram os primeiros a perceber que qualquer número natural, exceto o 0 e o 1, pode ser gerado pela multiplicação de números primos, os chamados "blocos de construção". Ou seja, um número natural $n \geq 2$ pode ser escrito como um produto de primos e, é claro, a ordenação dos primos neste produto não modifica o resultado.

A demonstração deste fato foi dada por Euclides, que provou apenas a existência da fatoração de um natural em primos. Acredita-se que Euclides conhecesse a unicidade desta fatoração e que não fez sua demonstração pela dificuldade em estabelecer uma notação adequada.

No próximo teorema, provaremos a existência e a unicidade da fatoração de um natural em primos utilizando o Princípio de Indução Matemática.

Teorema 6.1 (Teorema Fundamental de Aritmética - TFA): *Dado um número natural $n \geq 2$, existem primos distintos $p_1, p_2, \cdots, p_k$ tais que*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

onde os expoentes α_i são naturais, $1 \leq i \leq k$.

Além disso, se $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$, onde q_j são primos distintos, $1 \leq j \leq t$, então $t = k$ e todo q_j é igual a algum p_i.

Demonstração: Usaremos a segunda forma do PIM para garantir a existência da fatoração. Para $n = 2$ existe uma decomposição trivial em números primos, já que 2 já é um número primo. Consideremos $k > 2$ e suponhamos que existe uma fatoração para todo natural m tal que $2 \leq m \leq k$.

Mostraremos agora que também vale para $k + 1$ e, como consequência, teremos que o resultado vale para todo $n \geq 2$.

Se $k+1$ for primo, admite a decomposição trivial. Caso contrário, $k+1$ pode ser escrito como

$$k+1 = ab, \quad \text{onde} \quad 1 < a < k+1 \quad \text{e} \quad 1 < b < k+1.$$

Assim, $2 \leq a \leq k$ e $2 \leq b \leq k$, e pela hipótese de indução a e b podem ser escritos como produtos de primos. Logo, o resultado também vale para $k+1$.

Para provar a unicidade, devemos garantir que um natural $n \geq 2$ não admite mais de uma fatoração em produto de fatores primos. Esta demonstração também será feita usando a segunda forma do PIM.

Claro que $n = 2$ possui uma única fatoração. Vamos considerar $k > 2$ e assumir que qualquer natural m tal que $2 \leq m \leq k$ tem uma fatoração única como produto de primos.

Agora suponhamos que $k+1$ tenha duas fatorações distintas como produto de primos (os primos não são necessariamente distintos):

$$k+1 = p_1 \cdots p_r = q_1 \cdots q_s. \tag{6.1}$$

Reordenando os primos, se necessário, podemos supor que

$$p_1 \leq \cdots \leq p_r \qquad \text{e} \qquad q_1 \leq \cdots \leq q_s.$$

Note que $p_1 \neq q_1$ pois se tivéssemos $p_1 = q_1$ então o natural $\frac{k+1}{p_1} \leq k$ teria duas fatorações distintas com produto de primos, contrariando a hipótese de indução.

Se assumimos, sem perda de generalidade, que $p_1 < q_1$ e considerarmos o inteiro

$$m = (k+1) - (p_1 q_2 \cdots q_s),$$

então $m < k+1$ e a partir de (6.1) temos que m se escreve como

$$m = p_1 p_2 \cdots p_r - p_1 q_2 \cdots q_s$$

e também como

$$m = q_1 q_2 \cdots q_s - p_1 q_2 \cdots q_s.$$

Deste modo:

$$m = p_1(p_2 \cdots p_r - q_2 \cdots q_s) \tag{6.2}$$

e

$$m = (q_1 - p_1)(q_2 \cdots q_s). \tag{6.3}$$

Por (6.2), temos $m \geq 2$ pois $p_1 \mid m$ e assim já que $2 \leq m \leq k$, por hipótese de indução, m tem fatoração única em primos.

Deste modo, o primo p_1 deve estar presente no produto em (6.3) (pois está presente em (6.2)) e como $p_1 < q_1 \leq \cdots \leq q_s$, devemos ter p_1 como fator de $q_1 - p_1$, ou seja, $p_1 \mid q_1 - p_1$. Portanto, existe $c \in \mathbb{Z}$ tal que

$$q_1 - p_1 = cp_1$$

e, com isso, $q_1 = (c+1)p_1$, o que é absurdo pois p_1 e q_1 são primos distintos.

Com esta contradição, concluímos que $k+1$ não possui duas fatorações distintas como produto de primos, o que mostra que qualquer natural $n \geq 2$ tem uma fatoração única como produto de primos, de acordo com a segunda forma do PIM.

□

Problema 6.1 Mostre que não existe um primo cujo dobro seja igual a um quadrado perfeito menos 1.

Solução: Para resolver, suponhamos que exista um primo p tal que $2p = n^2 - 1$. Mas então $2p = (n-1)(n+1)$ e, assim, usando o TFA:

$$(1) \quad \begin{matrix} n+1 = 2 \\ n-1 = p \end{matrix} \qquad \text{ou} \qquad (2) \quad \begin{matrix} n-1 = 2 \\ n+1 = p \end{matrix}$$

Se (1) ocorre então $n = 1$ e $p = 0$, o que é um absurdo. Se (2) ocorre, então $n = 3$ e, assim, $p = 4$, o que é igualmente um absurdo. Logo tal primo não existe.

Problema 6.2 A quarta potência de um natural é igual ao triplo de um primo p mais 1. Que primo é este?

Solução: Neste caso, temos $n^4 = 3p + 1$ e assim, $3p = n^4 - 1$, ou seja, $3p = (n^2 - 1)(n^2 + 1)$. Pelo TFA, devemos ter:

$$(1) \quad \begin{matrix} n^2+1 = 3 \\ n^2-1 = p \end{matrix} \qquad \text{ou} \qquad (2) \quad \begin{matrix} n^2-1 = 3 \\ n^2+1 = p \end{matrix}$$

No caso (1) temos $n^2 = 2$, o que já é um absurdo. No caso (2) temos $n^2 = 4$, ou seja, $n = 2$ e consequentemente $p = 5$.

Se não prestarmos atenção quando analisarmos certas questões sobre divisibilidade, poderemos cometer erros. Por exemplo, dados naturais a, b e c, é verdade que

$$\text{se } \; c \mid ab \; \text{ então } \; c \mid a \quad \text{ou} \quad c \mid b? \tag{6.4}$$

Isto não é sempre verdade. Tomemos como exemplo, $c = 12$, $a = 6$ e $b = 4$. Claro que $\underbrace{12}_{c}$ divide $\underbrace{24}_{ab}$ mas $\underbrace{12}_{c}$ não divide $\underbrace{6}_{a}$ e $\underbrace{12}_{c}$ não divide $\underbrace{4}_{b}$.
Como consequência do TFA, temos que (6.4) vale quando $c = p$ é um primo.

Corolário 6.1 Se p é primo tal que $p \mid ab$ então $p \mid a$ ou $p \mid b$.

Demonstração: Se $p \mid ab$ então p é um primo que aparece na fatoração de ab. Quando fatoramos a e b em primos, o primo p tem que aparecer em pelo menos uma das fatorações, devido à unicidade garantida pelo TFA. Ou seja, $p \mid a$ ou $p \mid b$.

□

Corolário 6.2 Se p for um primo tal que $p \mid ab$ mas p não divide a então $p \mid b$.

Exercícios

1 - Determine se é verdadeiro (V) ou falso (F). Justifique:

(a) Se p é um primo tal que $p^3 \mid ab$ e $p^2 \mid a$ então $p \mid b$.

(b) Se um primo $p \mid a^2 + b^2$ e $p \mid a$ então $p \mid b$.

(c) Se um primo $p \mid a + b$ então $p \mid a$ e $p \mid b$.

(d) Se a divide um primo p então a é primo.

2 - Responda com justificativa: O triplo de um número primo p é igual ao quadrado de um inteiro n menos 16. Que primo é este?

3 - Seja n um número natural > 1. Mostre que se n divide $(n-1)! + 1$ então n é um número primo.

4 - Seja $n \geq 5$ um número composto. Mostre que $n \mid (n-1)!$.

5 - Mostre que se o triplo de um número primo p é igual ao quadrado de um número natural n menos 4 então p só pode ser o primo 7.

6 - Mostre que todo inteiro positivo da forma $3k + 2$ tem um fator primo da mesma forma.

7 - Mostre que:

(a) Todo número natural ímpar é da forma $4k + 1$ ou $4k - 1$, onde $k \in \mathbb{N}$.

(b) Todo número da forma $4k - 1$ possui pelo menos um divisor primo desta mesma forma.

(c) Existem infinitos primos da forma $4k - 1$.

8 - Seja $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ onde $p_1, p_2, \cdots, p_k$ são primos distintos e os expoentes α_i são naturais, $1 \leq i \leq k$.

(a) Mostre que todos os divisores positivos b de a são da forma $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ em que $0 \leq \beta_i \leq \alpha_i$, para todo $1 \leq i \leq k$.

(b) Conclua que o número dos divisores positivos de a (incluindo 1 e a) é dado pelo produto

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

9 - Se p_n denota o n-ésimo primo então prove que não existe $x \in \mathbb{Z}$ tal que $p_1 p_2 ... p_n + 1 = x^2$.

10 - Suponha que p seja o menor fator primo de um inteiro n e que $p > \sqrt{n/p}$. Prove que n/p é primo.

AULA 7

Máximo divisor comum

OBJETIVOS
Estudaremos os divisores comuns de dois inteiros e veremos como calcular o maior dentre estes divisores: o máximo divisor comum (MDC). Destacaremos as diversas propriedades do MDC entre dois inteiros.

Quando temos dois inteiros a e b, podemos nos perguntar sobre seus divisores e múltiplos comuns, ou seja, divisores simultâneos de a e b e múltiplos simultâneos de a e b.

Claro que 1 é um divisor comum de a e b, a questão é se existem outros e qual é o maior destes divisores. Também podemos notar que ab é um múltiplo comum de a e b e novamente nos perguntamos qual é o menor destes múltiplos.

Foi no Livro VII de *Os elementos* que Euclides definiu o máximo divisor comum de dois inteiros, conforme abaixo.

Definição 7.1 *Dados dois inteiros a e b, não simultaneamente nulos, dizemos que um inteiro d é o máximo divisor comum de a e b (e escrevemos $d = mdc(a, b)$) se:*

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

(ii) Se existe um inteiro c tal que $c \mid a$ e $c \mid b$ então $c \leq d$.

Uma consequência imediata da definição acima é que $mdc(a, b) > 0$ (o MDC é o maior divisor comum e é claro que se x é divisor de a e b então $-x$ também o é). Além disso, $mdc(a, b) = mdc(b, a)$, pois não faz diferença se trocamos a por b na Definição 7.1.

Definição 7.2 *Quando a e b são inteiros tais que $mdc(a, b) = 1$, então dizemos que a e b são primos entre si (ou relativamente primos).*

Exemplo 7.1 Se p e q forem primos distintos então eles são relativamente primos. Isto é claro pois os divisores (positivos) de p são 1 e p e os divisores (positivos) de q são 1 e q. Como p e q são distintos, com certeza p não divide q (e vice-versa) e portanto $mdc(p, q) = 1$.

Problema 7.1 Se a for um inteiro não nulo, qual é o $mdc(a, 0)$?

Solução: Um divisor comum de a e 0 é a (lembre que $a \mid 0$ pois $0 = a \cdot 0$). Como $mdc(a, 0) > 0$, devemos ter $mdc(a, 0) =\mid a \mid$.

Problema 7.2 Se p for um primo e $a \neq 0$ é inteiro, quais os possíveis valores para $mdc(a, p)$?

Solução: Neste caso, $mdc(a, p) = 1$ ou $mdc(a, p) = p$ pois este deve ser um divisor de p (que é primo).

Como consequência, se p não divide a então $mdc(a, p) = 1$.

Problema 7.3 Devemos nos preocupar com números negativos?

Solução: Vamos ver que não, através deste exemplo:

Divisores de 12 = Divisores de -12

$$-1, -2, -3, -4, -6, -12, 1, 2, 3, 4, 6, 12.$$

Divisores de 18 = Divisores de -18

$$-1, -2, -3, -6, -9, -18, 1, 2, 3, 6, 9, 18.$$

Com isso, temos

$$mdc(12, 18) = mdc(-12, 18) = mdc(12, -18) = mdc(-12, -18) = 6.$$

O problema anterior pode ser resolvido geralmente com o resultado abaixo.

Proposição 7.1 *Se a e b forem inteiros não nulos então:*

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

(2) $mdc(a, b) \leq min\{|a|, |b|\}$.

Demonstração: A prova do item (1) é trivial pois os divisores comuns de a e b são os mesmos divisores comuns de $\mid a \mid$ e $\mid b \mid$. Além disso, se $d = mdc(a, b)$, então d é positivo e, como divide $\mid a \mid$ e também divide $\mid b \mid$, com certeza vamos ter $d \leq \mid a \mid$ e $d \leq \mid b \mid$, provando o item (2).

□

Para calcular o máximo divisor comum de dois inteiros podemos utilizar a fatoração de cada um deles em primos dada pelo TFA. Vejamos como isto pode ser feito no próximo resultado.

Proposição 7.2 *Se*

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} r_1^{\gamma_1} \cdots r_t^{\gamma_t},$$

e

$$b = p_1^{\beta_1} \cdots p_k^{\beta_k} s_1^{\lambda_1} \cdots s_l^{\lambda_l},$$

onde $p_1, \cdots, p_k, r_1, \cdots, r_t, s_1, \cdots, s_l$ são primos distintos e os expoentes $\alpha_i, \gamma_j, \beta_i, \lambda_v$ são naturais, $1 \leq i \leq k$, $1 \leq j \leq t$, $1 \leq v \leq l$ então

$$mdc(a, b) = p_1^{\theta_1} \cdots p_k^{\theta_k}$$

onde $\theta_i = min\{\alpha_i, \beta_i\}$, para $i = 1, \cdots, k$.

Demonstração: Vamos mostrar que o inteiro $d = p_1^{\theta_1} \cdots p_k^{\theta_k}$, com $\theta_i = \min\{\alpha_i, \beta_i\}$, $i = 1, \cdots, k$, satisfaz os itens (i) e (ii) da Definição 7.1.

Como para todo $i = 1, \cdots, k$, $\theta_i \leq \alpha_i$ e $\theta_i \leq \beta_i$, temos $\alpha_i - \theta_i \geq 0$ e $\beta_i - \theta_i \geq 0$ e assim os números

$$a_1 = p_1^{\alpha_1 - \theta_1} \cdots p_k^{\alpha_k - \theta_k} \quad \text{e} \quad b_1 = p_1^{\beta_1 - \theta_1} \cdots p_k^{\beta_k - \theta_k}$$

são naturais e, além disso,

$$a = a_1 d \quad \text{e} \quad b = b_1 d,$$

ou seja, $d \mid a$ e $d \mid b$, o que garante o item (i).

Agora, para provar o item (ii), consideramos um inteiro c tal que $c \mid a$ e $c \mid b$. Desta forma, a e b são múltiplos de c e, assim, pelo Teorema Fundamental da Aritmética, os primos que aparecem na fatoração de c devem estar presentes tanto na fatoração de a quanto na fatoração de b.

Como os únicos primos comuns nas fatorações de a e b são os p_i', teremos:

$$c = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}, \quad \text{com} \quad 0 \leq \varepsilon_i \leq \min\{\alpha_i, \beta_i\}, \quad i = 1, \cdots, k,$$

portanto $\varepsilon_i \leq \theta_i$, o que mostra que $c \leq d$ e finaliza a demonstração deste resultado.

□

Exemplo 7.2 Temos $1508 = 2^2 \cdot 13 \cdot 29$ e $442 = 2 \cdot 13 \cdot 17$. Neste caso, $mdc(1508, 422) = 2 \cdot 13$ pois o máximo divisor comum é dado pelos primos comuns com menor expoente.

O método acima não é sempre conveniente, pois, como já observamos na Aula 5, a fatoração pode ser muito difícil quando trabalhamos com números grandes.

Existe um procedimento prático que permite o cálculo do máximo divisor comum de dois inteiros, sem passar pela fatoração em primos, que está presente em *Os elementos* de Euclides e é conhecido como *algoritmo de Euclides*.

Primeiramente vamos ver um exemplo.

Exemplo 7.3 Temos $221 = 2 \cdot 91 + 39$, ou seja, o resto da divisão de 221 por 91 é 39 e notamos também que $mdc(221, 91) = mdc(91, 39) = 13$.

No exemplo anterior vimos que o máximo divisor comum de $a = 221$ e $b = 91$ é igual ao máximo divisor comum de b e o resto da divisão de a por b. Isto ocorre de maneira geral.

Proposição 7.3 *Se $a = bq + r$ onde $0 \leq r < b$ então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Suponhamos que $d = mdc(a, b)$. Queremos mostrar que $d = mdc(b, r)$. Usando a definição de mdc, já temos que $d \mid a$ e $d \mid b$. Desta forma, como $r = a - bq$, vamos ter $d \mid r$.

Logo, já concluímos que d é um divisor comum de b e r, precisamos garantir agora que ele seja o maior de todos os divisores.

Se c é um outro divisor de b e r, temos $c \mid b$ e $c \mid r$. Mas então, como $a = bq + r$ teremos que $c \mid a$. Assim, c é um divisor comum de a e b e portanto deve ser menor ou igual a $mdc(a, b)$, ou seja, $c \leq d$.

□

Exemplo 7.4 Vamos calcular $mdc(754, 221)$ com base no resultado anterior.

Dividindo sucessivamente, temos:

(1) $754 = 3 \cdot 221 + 91$ e $mdc(754, 221) = mdc(221, 91)$

(2) $221 = 2 \cdot 91 + 39$ e $mdc(221, 91) = mdc(91, 39)$

(3) $91 = 2 \cdot 39 + 13$ e $mdc(91, 39) = mdc(39, 13)$

(4) $39 = 3 \cdot 13 + 0$ e $mdc(39, 13) = 13$

(5) $mdc(13, 0) = 13$ e a partir daqui isto se repete.

Assim, $mdc(754, 221) = mdc(221, 91) = mdc(91, 39) = mdc(39, 13) = 13$.

Em geral, podemos obter $mdc(a, b)$ pelo *método das divisões sucessivas.*

Teorema 7.1 (Algoritmo de Eulides) *Sejam a e b naturais não nulos, com $a \geq b$. Dividindo sucessivamente, obtemos:*

$$a = bq_1 + r_1,\ 0 < r_1 < b \Rightarrow mdc(a, b) = mdc(b, r_1)$$

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1 \Rightarrow mdc(b, r_1) = mdc(r_1, r_2)$$

$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2 \Rightarrow mdc(r_1, r_2) = mdc(r_2, r_3)$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n,\ 0 < r_n < r_{n-1} \Rightarrow mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n)$$

$$r_{n-1} = r_nq_{n+1} \Rightarrow mdc(r_{n-1}, r_n) = r_n.$$

Portanto, $mdc(a, b) = r_n$, ou seja, é o último resto não nulo encontrado no processo de divisões sucessivas. Claro que se $r_1 = 0$ então $mdc(a, b) = b$.

Demonstração: Como a e b são naturais, é claro que se $a = bq_1$ então $mdc(a, b) = b > 0$. Portanto, vamos considerar o caso geral e provar que podemos calcular o MDC usando indução sobre o número de passos do algoritmo de Euclides (AE).

Para isto, o que queremos provar é que a seguinte afirmação é verdadeira: se, ao aplicarmos o AE a dois naturais a e b, obtivermos o primeiro resto nulo após $n + 1$ passos, então $mdc(a, b)$ é igual ao último resto não nulo obtido, ou seja, o resto obtido no passo n.

É claro que para $n = 1$ a afirmação é verdadeira, pois se o primeiro resto nulo é obtido no passo 2 então

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

$$b = r_1q_2,$$

assim, de acordo com a Proposição 7.3, temos $mdc(a, b) = mdc(b, r_1) = r_1$ e, neste caso, o MDC é o resto obtido no passo $n = 1$.

Agora suponhamos que a afirmativa seja verdadeira para $n = k$, ou seja, para obter o primeiro resto nulo precisamos de $k + 1$ passos.

Vamos ver que a afirmativa também é verdadeira para $n = k + 1$, ou seja, quando precisarmos de $k + 2$ passos para chegar no primeiro resto nulo:

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

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + r_k,\ 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1} + r_{k+1}$$

$$r_k = r_{k+1}q_{k+2}.$$

Queremos mostrar que $mdc(a, b) = r_{k+1}$, ou seja, o resto não nulo obtido no passo $k + 1$.

Mas note que ao aplicarmos o AE aos números b e r_1, o primeiro resto nulo foi encontrado após $k + 1$ passos e então, por hipótese de indução, $mdc(b, r_1) = r_{k+1}$. Mas, novamente usando a Proposição 7.3, temos

$$mdc(a, b) = mdc(b, r_1) = r_{k+1},$$

o que garante o resultado.

□

Já vimos que se $a \neq 0$ então $mdc(a, 0) = |a|$. Neste caso, podemos escrever:

$$mdc(a, 0) = |a| = \underbrace{(\pm 1)}_{x} a + \underbrace{0}_{y} b.$$

De maneira geral, podemos perguntar se isto ocorre quando a e b são simultaneamente não nulos, ou seja,

$$existem\ \ inteiros\ \ x\ e\ \ y\ \ tais\ \ que\ \ mdc(a, b) = ax + by?$$

Isto é verdade e dizemos que o máximo divisor comum é uma combinação linear inteira de a e b. É claro que podemos provar este fato apenas para o caso em que a e b são inteiros positivos, pois já sabemos que $mdc(a, b) = mdc(|a|, |b|)$.

Teorema 7.2 *Se a e b forem naturais e $d = mdc(a, b)$, então existem inteiros x e y tais que $d = ax + by$.*

Demonstração: Inicialmente notamos que se $b \mid a$ então:

$$mdc(a, b) = b = \underbrace{0}_{x} \cdot a + \underbrace{1}_{y} \cdot b.$$

Portanto, vamos considerar o caso em que b não divide a. Neste caso, calculamos $d = mdc(a, b)$ pelo Teorema 7.1 e vamos mostrar que d é uma combinação linear inteira de a e b usando indução sobre o número de passos do algoritmo de Euclides.

É claro que se são necessários $n = 2$ passos para calcularmos o MDC então

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

$$b = r_1q_2,$$

ou seja, temos $mdc(a,b) = mdc(b,r_1) = r_1 = a - bq_1$ e, neste caso, $x = 1$ e $y = -q_1$.

Agora suponhamos que a afirmativa seja verdadeira sempre que necessitarmos de $n = k$ passos para o cálculo do MDC (ou seja, para obter o primeiro resto nulo no processo de divisões sucessivas).

Vamos ver que também é verdadeira quando precisarmos de $n = k + 1$ passos:

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

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + r_k,\ 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1},$$

ou seja, o que temos aqui é que $mdc(a,b) = r_k$, obtido após $k + 1$ passos.

Mas note que $mdc(b,r_1) = r_k$ e necessitamos de k passos para obtê-lo. Logo, por hipótese de indução, existem inteiros x' e y' tais que

$$r_k = bx' + r_1y'.$$

Mas como $a = bq_1 + r_1$ temos $r_1 = a - bq_1$ e, portanto,

$$mdc(a,b) = r_k = bx' + (a - bq_1)y' = a\underbrace{y'}_{x} + b\underbrace{(x' - q_1y')}_{y}$$

e isto finaliza a demonstração.

□

Problema 7.4 Como determinar os inteiros x e y?

Solução: Considerando o cálculo que fizemos no Exemplo 7.4, temos o seguinte:

$$\begin{array}{lrcl} \text{De (3)} & 13 & = & 91 - 2 \cdot 39 \\ \text{De (2)} & & = & 91 - 2 \cdot (221 - 2 \cdot 91) \\ & & = & 5 \cdot 91 - 2 \cdot 221 \\ \text{De (1)} & & = & 5 \cdot (754 - 3 \cdot 221) - 2 \cdot 221 \\ & & = & 5 \cdot 754 - 17 \cdot 221 \end{array}$$

Concluímos que

$$13 = 5 \cdot 754 - 17 \cdot 221,$$

isto é, os inteiros $x = 5$ e $y = -17$ são tais que

$$13 = 754x + 221y.$$

A partir do próximo resultado, temos uma maneira de verificar quando dois inteiros são relativamente primos.

Proposição 7.4 *Sejam $a, b \in \mathbb{Z}$. Temos $mdc(a,b) = 1$ se, e somente se, existem inteiros x e y tais que $1 = ax + by$.*

Demonstração: Pelo Teorema 7.2, está claro que se $mdc(a,b) = 1$ então existem inteiros x e y tais que $1 = ax + by$.

Por outro lado, se existem tais inteiros e $d = mdc(a,b)$ então $d \mid a$ e $d \mid b$, mas, assim,

$$d \mid (ax + by), \quad \text{ou seja,} \quad d \mid 1.$$

Deste modo, $d = 1$ e a demonstração está feita.

□

Problema 7.5 Se a, b e d são inteiros tais que $d = ax + by$, com $x, y \in \mathbb{Z}$ então é verdade que $d = mdc(a,b)$?

Solução: Isto não é sempre verdadeiro. Por exemplo, para $a = 3$, $b = 2$ e $d = 9$ temos

$$9 = 3x + 2y,$$

onde $x = 1$ e $y = 3$ e claramente $mdc(3,2) \neq 9$.

Portanto, devemos tomar cuidado com a recíproca do Teorema 7.2. Ela vale quando $d = 1$, como visto na proposição anterior.

Proposição 7.5 *Sejam $a, b, c, d \in \mathbb{Z}$. Valem as seguintes propriedades do máximo divisor comum:*

(1) se $mdc(a,b) = d$ então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$;

(2) se $a \mid bc$ e $mdc(a,b) = 1$ então $a \mid c$.

Demonstração: Para provar (1), usamos o Teorema 7.2 e escrevemos $d = ax + by$. Então, como $d \mid a$ e $d \mid b$ temos que os números $\frac{a}{d}$ e $\frac{b}{d}$ são naturais e, além disso,

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

Assim, pela proposição anterior, concluímos que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Agora, se $a \mid bc$ e $mdc(a,b) = 1$ então existem inteiros q, x e y tais que

$$aq = bc \quad \text{e} \quad 1 = ax + by. \tag{7.1}$$

Para garantir que $a \mid c$, devemos mostrar que existe $k \in \mathbb{Z}$ tal que $c = ak$. Para obter esta informação, multiplicamos a segunda equação em (7.1) por c:

$$c = axc + \underbrace{bc}_{aq} y$$

ou seja,

$$c = a\underbrace{(xc + qy)}_{k}, \quad \text{com} \quad k \in \mathbb{Z},$$

o que prova a proposição.

□

Problema 7.6 É verdade que se $a \mid c$ e $b \mid c$ então temos $ab \mid c$?

Solução: Devemos tomar cuidado pois temos exemplos onde a e b dividem c e o produto ab não divide c. Isto acontece com $a = 3$, $b = 6$ e $c = 24$.

A resposta da questão anterior é positiva é quando $mdc(a, b) = 1$, como abaixo.

Proposição 7.6 *Se $a, b, c, d \in \mathbb{Z}$ então vale o seguinte:*

(1) se $a \mid c$, $b \mid c$ e $mdc(a, b) = d$ então $\dfrac{ab}{d} \mid c$;

(2) se $a \mid c$, $b \mid c$ e a e b são relativamente primos então $ab \mid c$.

Demonstração: Basta provar o item (1), pois o segundo é um consequência imediata deste. Temos:

$$a \mid c \Rightarrow \exists\ q \in \mathbb{Z} \text{ tal que } \ c = aq$$

$$b \mid c \Rightarrow \exists\ k \in \mathbb{Z} \text{ tal que } \ c = bk$$

$$mdc(a, b) = d \Rightarrow \exists\ x,\ y \in \mathbb{Z} \text{ tais que } \ d = ax + by.$$

Assim, ao multiplicar a última equação por c, obtemos:

$$dc = ax\underbrace{c}_{bk} + by\underbrace{c}_{aq},$$

ou seja,

$$dc = ab\underbrace{(xk + yq)}_{m}, \quad \text{com} \quad m \in \mathbb{Z}.$$

Mas como $\dfrac{ab}{d} \in \mathbb{Z}$, logo

$$c = \frac{ab}{d}m, \quad \text{isto é,} \quad \frac{ab}{d} \mid c.$$

□

Quando enunciamos a Definição 7.1 do máximo divisor comum de a e b, nos preocupamos apenas em dizer que ele é o maior divisor dos dois números. Na verdade, existe uma outra maneira de dizer que um inteiro d é o máximo divisor comum de a e b, garantindo que este é um divisor comum positivo que é múltiplo de todos os outros divisores comuns de a e b, conforme provaremos agora.

Proposição 7.7 *Sejam a e b dois inteiros não simultaneamente nulos. O inteiro d é o máximo divisor comum de a e b se, e somente se, d satisfaz as propriedades abaixo:*

(i) $d > 0$;

(ii) $d \mid a$ e $d \mid b$;

(iii) se c é um inteiro tal que $c \mid a$ e $c \mid b$ então $c \mid d$.

Demonstração: Se $d = mdc(a, b)$ então claramente d satisfaz as propriedades (i) e (ii) do enunciado. Agora, temos que mostrar que também satisfaz (iii). Para isto, considere c um inteiro tal que $c \mid a$ e $c \mid b$. Usando o Teorema 7.2, escrevemos $d = ax + by$, com $x, y \in \mathbb{Z}$ e, portanto, basta usar o item (4) da Proposição 4.1 para concluir que $c \mid d$.

Para mostrar a recíproca, consideramos d um inteiro satisfazendo os itens $(i), (ii)$ e (iii) acima. Vamos mostrar que de fato, d é o máximo divsor comum de a e b. Para isto, temos que garantir que d também satisfaz os itens da Definição 7.1.

Claro que só temos que mostrar o último item e, para fazer isto, tomamos um inteiro c tal que

$$c \mid a \qquad \text{e} \qquad c \mid b.$$

Pelo item (iii) acima, temos $c \mid d$ e, assim, existe $c \in \mathbb{Z}$ tal que

$$d = cq = |c||q|, \quad \text{pois} \quad d > 0.$$

Logo, $c \leq |c| \leq d$, como queríamos mostrar.

□

Problema 7.7 Mostre que $mdc(a, b) = mdc(a - b, b)$.

Solução: Para provar a igualdade acima, consideramos $d = mdc(a, b)$ e vamos mostrar que também temos $d = mdc(a - b, b)$ usando a proposição anterior.

É claro que o item (i) é verdadeiro e como já temos que $d = mdc(a, b)$ então $d \mid a$ e $d \mid b$, o que implica que $d \mid (a - b)$. Logo d é divisor de $a - b$ e de b.

Falta apenas mostrar que se c é um inteiro tal que $c \mid (a - b)$ e $c \mid b$ então $c \mid d$. Mas isto também já é verdade, pois

$$c \mid (a - b) \;\text{ e }\; c \mid b \Rightarrow \quad c \mid [(a - b) + b],$$

isto é, $c \mid a$, e como $c \mid b$, usamos novamente a proposição anterior e concluímos que $c \mid d$.

Exercícios

1 - Encontre os possíveis valores de $a \in \mathbb{Z}$ tal que $mdc(20 + a, a) = 4$.

2 - Se p é um primo e $mdc(a, b) = p$, quais são os possíveis valores de $mdc(a^2, b)$? E de $mdc(a^2, b^2)$?

3 - Seja n um número natural tal que $mdc(n, 6) = 1$. Mostre que $n^2 - 1$ é múltiplo de 12.

4 - Determine o $mmc(a, b)$ de dois números positivos a e b cujo produto é $2^5 \cdot 3^3$ e sendo $mdc(a, b) = 2^2 \cdot 3$.

5 - Considere a, b, c inteiros tais que $a \mid bc$. Mostre que se $mdc(a, b) = d$ então $a \mid dc$.

6 - Sejam $a, b, c \in \mathbb{Z}$ não nulos. Prove que:

(a) Se $mdc(a, c) = 1$ e $b \mid c$, então mostre que $mdc(a, b) = 1$.

(b) Se $mdc(a, c) = 1$ então $mdc(a, bc) = mdc(a, b)$.

(c) Se $mdc(a, b) = 1$ então $mdc(a + b, a - b) = 1$ ou 2.

(d) $mdc(a, b) = 1 \Leftrightarrow mdc(a + b, a^2 + ab + b^2) = 1$.

7 - Considerando $a, b \in \mathbb{Z}$ e p um número primo nas afirmativas abaixo, verifique se estas são verdadeiras ou falsas. Justifique convenientemente.

(a) Se $a + mdc(a, b)$ é par então $a + b$ é par.

(b) Se $a + mdc(a, b)$ é ímpar então $a + b$ é ímpar.

(c) Se $d = mdc(a, a^2 + b^2)$ então $d \mid (a - b)^2$.

8 - Sejam a e b inteiros não nulos primos entre si. Mostre que $mdc(a^n, b^n) = 1, \ \forall n \geq 1$.

AULA 8

Equações diofantinas lineares e MMC

OBJETIVOS
Introduziremos as chamadas equações diofantinas lineares, que são utilizadas na solução de problemas envolvendo números inteiros. Vamos ver que suas soluções dependem fortemente de uma condição envolvendo o MDC. Além disso, vamos tratar dos múltiplos comuns de dois inteiros, destacando o principal deles: o mínimo múltiplo comum.

O matemático grego Diofanto de Alexandria viveu no século 3 da era cristã. Ele expôs uma série de problemas a respeito de números inteiros que despertaram interesse entre os árabes. Um deles passou à história da matemática, graças a Pierre de Fermat, no século 17. É o problema expresso pela equação

$$x^n + y^n = z^n,$$

e a pergunta é se existem números inteiros x, y e z que sejam soluções desta equação.

Diofanto demonstrou que para $n = 2$ existem inúmeras soluções. De fato, você já conhece soluções clássicas dadas por números pitagóricos, tais como:

$$3^2 + 4^2 = 5^2.$$

Fermat, ao retomar o problema, estabeleceu o famoso "Último Teorema de Fermat", que diz que a equação não tem solução em números inteiros quando n é maior que 2.

Na verdade, Fermat não deixou registros sobre a prova deste teorema e a primeira demonstração pública para ele foi dada em 1993, por Andrew Wiles.

De modo geral, Diofanto se interessava por problemas que envolvessem equações cujas soluções se restringiam aos números inteiros e se preocupou particularmente com as chamadas *equações diofantinas lineares* com duas incógnitas, que são equações nas incógnitas x e y, que têm a forma:

$$ax + by = c, \quad \text{onde } a, b, c \in Z$$

com a e b não simultaneamente nulos.

As equações diofantinas lineares surgem naturalmente em problemas cotidianos, como no exemplo abaixo.

Exemplo 8.1 Um feirante vende maçãs e uvas por quilo. Cada quilo de maçã custa $R\$3,00$ e cada quilo de uva custa $R\$6,00$. Determine a equação que fornece a quantidade de quilos de maçãs e quilos de uvas vendidos após o feirante faturar $R\$21,00$.

Considerando que o feirante vendeu x quilos de maçãs e y quilos de uvas, a equação que estabelece os quilos vendidos é $3x + 6y = 21$.

Definição 8.1 *Um par de inteiros (x_0, y_0) tais que $ax_0 + by_0 = c$ é uma solução inteira (ou simplesmente uma solução) da equação diofantina linear $ax + by = c$.*

Exemplo 8.2 Considerando a equação diofantina linear $3x + 6y = 21$, temos:

$$3.(7) + 6.(0) = 21, \quad 3.(9) + 6.(-1) = 21 \quad 3.(-1) + 6.(4) = 21.$$

Logo, os pares de inteiros $(7, 0), (9, -1)$ e $(-1, 4)$ são exemplos de soluções.

Problema 8.1 Toda equação diofantina linear possui solução?

Solução: Não, existem equações diofantinas lineares com duas incógnitas que não têm solução. Por exemplo, a equação diofantina linear

$$2x + 4y = 7 \tag{8.1}$$

não tem solução, porque $2x + 4y$ é um inteiro par quaisquer que sejam os valores inteiros de x e y, enquanto que 7 é um inteiro ímpar.

Observe que na equação (8.1) temos $mdc(2, 4) = 2$ não divide 7. De modo geral, a equação diofantina linear $ax+by = c$ não tem solução todas as vezes que $d = mdc(a, b)$ não divide c, conforme provaremos no próximo teorema.

Teorema 8.1 *A equação diofantina linear $ax + by = c$ tem solução se, e somente se, d divide c, onde $d = mdc(a, b)$.*

Demonstração: Suponha que a equação $ax + by = c$ tem uma solução, isto é, que existe um par de inteiros (x_0, y_0) tais que

$$ax_0 + by_0 = c.$$

Considerando $d = mdc(a, b)$, existem inteiros k e q tais que

$$a = dk \quad \text{e} \quad b = dq$$

e, assim, temos:

$$c = ax_0 + by_0 = dkx_0 + dqy_0 = d(kx_0 + qy_0).$$

E como $kx_0 + qy_0$ é um inteiro, segue-se que d divide c.

Reciprocamente, suponhamos que d divide c, isto é, que $c = dt$, onde t é um inteiro.

Pelo Teorema 7.2, existem inteiros x' e y' tais que

$$d = ax' + by'.$$

Então:

$$c = dt = (ax' + by')t = a(tx') + b(ty'),$$

isto é, o par de inteiros

$$(tx', ty')$$

é uma solução da equação $ax + by = c$.

□

Problema 8.2 Se já sabemos que existem soluções, como são estas soluções?

Solução: Se $d = mdc(a, b)$ divide c, já sabemos que existe um par de inteiros (x_0, y_0) que é uma solução particular da equação diofantina linear $ax + by = c$. As outras soluções desta equação serão dadas por fórmulas envolvendo o par (x_0, y_0) e o máximo divisor comum d, conforme mostra o resultado seguinte.

Teorema 8.2 *Seja (x_0, y_0) uma solução particular da equação diofantina linear $ax + by = c$, onde $d = mdc(a, b)$ divide c. Então todas as demais soluções são dadas por:*

$x = x_0 + (b/d)k \quad e \quad y = y_0 - (a/d)k, \quad$ *onde k é um inteiro arbitrário.*

Demonstração: Suponhamos que o par de inteiros (x_0, y_0) é uma solução particular da equação

$$ax + by = c. \tag{8.2}$$

Claro que para qualquer intero k, o par

$$(x_0 + (b/d)k, y_0 - (a/d)k)$$

também é solução de (8.2), pois

$$a(x_0 + (b/d)k) + b(y_0 - (a/d)k) = \underbrace{ax_0 + by_0}_{c} + \underbrace{a(b/d)k - b(a/d)k}_{0} = c.$$

Agora considere (x_1, y_1) uma outra solução qualquer desta equação. Então, temos

$$ax_0 + by_0 = c = ax_1 + by_1$$

e portanto

$$a(x_1 - x_0) = b(y_0 - y_1).$$

Como $d = mdc(a, b)$, existem inteiros r e s tais que $a = dr$ e $b = ds$, com r e s primos entre si (veja item (1) da Proposição 7.5). Substituindo estes valores de a e b na igualdade anterior e cancelando o fator d, obtemos

$$r(x_1 - x_0) = s(y_0 - y_1).$$

Assim, $r \mid s(y_0 - y_1)$ e, como $mdc(r, s) = 1$, segue do item (2) da Proposição 7.5 que $r \mid (y_0 - y_1)$, isto é,

$$y_0 - y_1 = rk \quad \text{e} \quad x_1 - x_0 = sk, \text{ onde } k \text{ é um inteiro.}$$

Portanto, temos as fórmulas:

$$x_1 = x_0 + sk = x_0 + (b/d)k \quad \text{e} \quad y_1 = y_0 - rk = y_0 - (a/d)k$$

□

Como podemos ver, se $d = mdc(a, b)$ divide c então a equação diofantina linear $ax + by = c$ admite um número infinito de soluções, uma para cada valor do inteiro arbitrário k.

Problema 8.3 Como encontrar uma solução inicial para uma equação diofantina linear?

Solução: Uma solução da equação diofantina linear $ax + by = c$ se obtém por tentativa ou pelo Algoritmo de Euclides, pois através dele podemos escrever $d = mdc(a, b)$ como combinação linear de a e b: $d = ax' + by'$. Mas como $d \mid c$ temos $c = dm$, com m um inteiro e, assim, $c = ax'm + by'm$, fornecendo assim a solução inicial $(x'm, y'm)$.

Problema 8.4 Mostre que a equação $16x + 15y = 17$ não possui soluções positivas (x', y'), isto é, com $x' > 0$ e $y' > 0$.

Solução: Uma solução inicial é dada através do MDC. Temos $a = 16$, $b = 15$ e $d = mdc(a, b) = 1$ é tal que

$$16 \cdot 1 + 15 \cdot (-1) = 1.$$

Assim, uma solução inicial é dada por

$$16 \cdot 17 + 15 \cdot (-17) = 17,$$

ou seja, $x_0 = 17$ e $y_0 = -17$.

Portanto, soluções gerais são dadas por:

$$x' = 17 + 15k \quad \text{e} \quad y' = -17 - 16k.$$

Assim, soluções positivas são tais que $17 + 15k > 0$ e $-17 - 16k > 0$, isto é, devemos ter um inteiro k tal que

$$-\frac{17}{15} < k < -\frac{17}{16},$$

o que não é possível.

Exemplo 8.3 Considerando o Exemplo 8.1, quantos quilos de maçãs e quantos quilos de uvas o feirante vendeu ao faturar $R\$21,00$?

Note que queremos encontrar soluções (x', y') da equação $3x + 6y = 21$. Uma solução inicial já foi dada no Exemplo 8.2: $x_0 = 7$ e $y_0 = 0$. Como $mdc(3, 6) = 3$, as demais soluções são dadas por:

$$x' = 7 + 2k \quad \text{e} \quad y' = 0 - k.$$

Como queremos valores não negativos (pois representam quantidades), então devemos ter

$$7 + 2k \geq 0 \quad \text{e} \quad -k \geq 0$$

ou seja,

$$k \geq -\frac{7}{2} \quad \text{e} \quad k \leq 0.$$

devemos encontrar os valores para um inteiro k tal que $-3 \leq k \leq 0$, que são:

k	x'	y'
-3	1	3
-2	3	2
-1	5	1
0	7	0

Ou seja, o feirante pode ter vendido 1 quilo de maçãs e 3 quilos de uvas ou 3 quilos de maçãs e 2 quilos de uvas ou 5 quilos de maçãs e 1 quilo de uva ou 7 quilos de maçãs e nenhum quilo de uva.

Problema 8.5 Até agora nos preocupamos com divisores comuns. O que dizer sobre os múltiplos comuns de dois inteiros não nulos a e b?

Solução: A partir de agora, vamos trabalhar com esta questão e definir o mínimo múltiplo comum (MMC) de a e b como o menor múltiplo positivo dos dois números, como temos abaixo.

Definição 8.2 *Um número inteiro m é o mínimo múltiplo comum dos números não nulos a e b se:*

(i) $m > 0$;

(ii) $a \mid m$ e $b \mid m$;

(iii) se existe um inteiro $c > 0$ tal que $a \mid c$ e $b \mid c$ então $m \leq c$.

Denotaremos o mínimo múltiplo comum de a e b por $mmc(a, b)$ e observamos que na definição acima, exigimos que $mmc(a, b)$ seja um inteiro estritamente positivo. Como já sabemos, no cálculo do MDC, sempre trabalhamos com inteiros positivos. O que dizer do MMC? Vejamos no exemplo.

Exemplo 8.4 Devemos nos preocupar com números negativos? Vamos ver que não, através deste exemplo:

Múltiplos de 12 = Múltiplos de -12

$$0, \pm 12, \pm 24, \pm 36, \cdots$$

Múltiplos de 18 = Múltiplos de -18

$$0, \pm 18, \pm 36, \pm 54, \cdots$$

Com isso, temos

$$mmc(12, 18) = mmc(-12, 18) = mmc(12, -18) = mmc(-12, -18) = 36.$$

O exemplo anterior pode ser generalizado com o resultado abaixo, cuja demonstração é deixada como exercício.

Proposição 8.1 *Se a e b são inteiros não nulos então:*

(1) $mmc(a,b) = mmc(|a|,|b|)$;

(2) $mmc(a,b) \geq max\{|a|,|b|\}$.

Assim como fizemos com o máximo divisor comum, o mínimo múltiplo comum também pode ser calculado através da fatoração em primos.

Proposição 8.2 *Se*

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} r_1^{\gamma_1} \cdots r_t^{\gamma_t},$$

e

$$b = p_1^{\beta_1} \cdots p_k^{\beta_k} s_1^{\lambda_1} \cdots s_l^{\lambda_l},$$

onde $p_1, \cdots, p_k, r_1, \cdots, r_t, s_1, \cdots, s_l$ são primos distintos e os expoentes $\alpha_i, \gamma_j, \beta_i, \lambda_v$ são naturais, $1 \leq i \leq k$, $1 \leq j \leq t$, $1 \leq v \leq l$ então

$$mmc(a,b) = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k} r_1^{\gamma_1} \cdots r_t^{\gamma_t} s_1^{\lambda_1} \cdots s_l^{\lambda_l} \tag{8.3}$$

onde $\epsilon_i = max\{\alpha_i, \beta_i\}$.

Demonstração: Considere $m = mmc(a,b)$. Vamos mostrar que m tem de fato a fatoração dada em (8.3). Para isto, vamos mostrar como é a fatoração de um múltiplo comum c qualquer de a e b.

Temos $c = av, v \in \mathbb{N}$, e então todos os primos na fatoração de a aparecem na fatoração de c com expoentes maiores ou iguais aos respectivos expoentes. O mesmo acontece em relação aos primos na fatoração de b pois $c = bw, w \in \mathbb{N}$. Portanto,

$$c = h(p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}), \quad \text{onde} \quad \epsilon_i \geq \max\{\alpha_i, \beta_i\}.$$

Por outro lado, $r_1, r_2, \cdots, r_t$ aparecem em a e não em b e $s_1, s_2, \cdots, s_l$ aparecem em b e não em a, mas todos devem aparecer em c, ou seja,

$$c = (r_1^{\mu_1} r_2^{\mu_2} \cdots r_t^{\mu_t} s_1^{\upsilon_1} s_2^{\upsilon_2} \cdots s_l^{\upsilon_l})(p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}),$$

onde $\epsilon_i \geq \max\{\alpha_i, \beta_i\}$, $\mu_j \geq \gamma_j$ e $\upsilon_n \geq \lambda_n$. Como m é o menor múltiplo comum necessariamente, teremos:

$$m = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k} r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_t^{\gamma_t} s_1^{\lambda_1} s_2^{\lambda_2} \cdots s_l^{\lambda_l},$$

onde $\epsilon_i = \max\{\alpha_i, \beta_i\}$, e isto finaliza a prova do resultado.

□

Exemplo 8.5 Temos $754 = 2 \cdot 13 \cdot 29$ e $221 = 13 \cdot 17$. Neste caso, $mmc(754, 221) = 2 \cdot 13 \cdot 17 \cdot 29$ pois o mínimo múltiplo comum é dado pelos primos comuns e não comuns com maior expoente.

Na Proposição 7.7, demos uma alternativa para a definição do máximo divisor comum que era equivalente a Definição 7.1. Vamos ver que o mesmo ocorre com o MDC.

Proposição 8.3 *Sejam a e b dois inteiros não simultaneamente nulos. O inteiro m é o mínimo múltiplo comum de a e b se, e somente se, m satisfaz as propriedades abaixo:*

(i) $m > 0$;

(ii) $a \mid m$ *e* $b \mid m$;

(iii) se c é um inteiro tal que $a \mid c$ e $b \mid c$ então $m \mid c$.

Demonstração: Se $m = mmc(a,b)$ então claramente m satisfaz as propriedades (i) e (ii) do enunciado. Agora, temos que mostrar que também satisfaz (iii). Para isto, considere c um inteiro tal que $a \mid c$ e $b \mid c$. Usando o Lema de Euclides, dividimos c por m, encontrando:

$$c = mq + r, \quad \text{onde} \quad 0 \leq r < m.$$

Portanto, $r = c - mq$, e como c e m são ambos múltiplos de a e de b então r é múltiplo de a e de b. Deste modo, não podemos ter $r \neq 0$, pois, se isto acontecesse, r seria um múltiplo comum positivo de a e b, que é $< m$, um absurdo.

Logo $r = 0$ e $c = mq$, ou seja, $m \mid c$.

Reciprocamente, se m um inteiro satisfazendo os itens $(i), (ii)$ e (iii) acima, para garantir que m é o mínimo múltiplo comum de a e b, basta mostrar que se $c > 0$ é um inteiro tal que $a \mid c$ e $b \mid c$ então temos $m \leq c$. Mas isto é claro pois pela condição (iii), já temos $m \mid c$ e assim, $c = mk$.

Mas como $m > 0$ e $c > 0$ temos $k > 0$, isto é, $k \geq 1$, o que implica $c \geq m$, conforme desejávamos.

□

Por fim, vamos ver que existe uma relação estreita entre o MDC e o MMC de dois naturais a e b, como abaixo.

Teorema 8.3 *Se a e b são números naturais então* $mmc(a,b) = \dfrac{ab}{mdc(a,b)}$.

Demonstração: Para demonstrar este resultado, vamos considerar $d = mdc(a,b)$. Inicialmente observamos que, como $d \mid a$ e $d \mid b$, os números $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros e também o número $m = \frac{ab}{d}$ é inteiro.

Precisamos ver que m satisfaz as condições que definem o MMC de a e b. Para isto, ele deve ser positivo, o que é claro, deve ser um múltiplo comum de a e b e deve ser o menor de todos.

De fato, temos que m é múltiplo de a e de b, pois

$$m = a \cdot \underbrace{\frac{b}{d}}_{inteiro} \qquad \text{e} \qquad m = b \cdot \underbrace{\frac{a}{d}}_{inteiro}.$$

Agora, se tomamos um outro múltiplo positivo de a e b, ou seja, $c > 0$ tal que $a \mid c$ e $b \mid c$, então vamos ter que existem $k, q \in \mathbb{N}$ tais que

$$c = ak \quad \text{e} \quad c = bq.$$

Mas $d = mdc(a,b)$, portanto existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Assim, multiplicando esta igualdade por c, temos:

$$\begin{aligned} cd &= \overbrace{c}^{bq} ax + \overbrace{c}^{ak} by \\ &= bq\, ax + ak\, by \\ &= ab(qx + ky). \end{aligned} \tag{8.4}$$

Agora, já que $\dfrac{ab}{d}$ é inteiro, podemos considerar o número inteiro

$$c = \overbrace{\frac{ab}{d}}^{m} (qx + ky).$$

Com isso, c é múltiplo de $m = \dfrac{ab}{d}$ e o lema anterior garante que $m = mmc(a, b)$.

□

Exemplo 8.6 O produto de dois naturais a e b é igual a 100. Sabendo que $mmc(a, b) < 50$, determine os possíveis valores de a e b.

Pelo teorema acima, temos $ab = mmc(a, b)mdc(a, b)$ e assim,

$$2^2 \cdot 5^2 = mmc(a, b)mdc(a, b) < 2 \cdot 5^2 \cdot mdc(a, b).$$

Então $mdc(a, b) > 2$.

Assim, a e b têm fator comum > 2 e como $ab = 2^2 \cdot 5^2$, as possiblidades são:

$$a = 2 \cdot 5 \text{ e } b = 2 \cdot 5$$

ou

$$a = 5 \text{ e } b = 2^2 \cdot 5.$$

Exercícios

1 - A soma de dois naturais a, b é 120 e $mmc(a, b) = 144$.
Determine os possíveis valores de a e b.

2 - Determine todos os possíveis valores para os naturais a e b tais que $mdc(a, b) = 10$ e $mmc(a, b) = 100$.

3 - Considerando $a, b \in \mathbb{Z}$ e p um número primo nas afirmativas abaixo, verifique se estas são verdadeiras ou falsas. Justifique convenientemente.

(a) Se $mdc(a, b)$ é par então $mmc(a, b)$ é par.

(b) Se $mmc(a, b)$ é par então $mdc(a, b)$ é par.

(c) Se $mmc(a, b) = p^2$ então p^3 não divide a.

4 - Determine todos os múltiplos positivos de 3 e todos os múltiplos positivos de 5 cuja soma é igual a 60.

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

6 - Um lojista vende cada par de tênis a R$50,00 e cada par de sapatos a R$30,00. Qual o mínimo de pares de calçados vendidos para que o total arrecadado ao fim de um dia de venda seja R$700,00?

7 - Um certo número de "seis" e de "noves" são adicionados e a soma resultante é 126. Se o número de "seis" e o número de "noves" fossem permutados, a soma seria 114. Quantos "seis" e quantos "noves" foram somados?

8 - Sejam $a, b \in \mathbb{Z}$ e n um número natural não nulo. Prove que:

(a) $mdc(na, nb) = n\ mdc(a, b)$.

(b) $mmc(na, nb) = n\ mmc(a, b)$.

9 - Sejam $a, b \in \mathbb{Z}$ não nulos. Mostre que $mdc(a, b) = mmc(a, b)$ se, e somente se, $a = b$.

10 - Sejam $a, b \in \mathbb{Z}$ não nulos. Se $m = mmc(a, b)$ então mostre que $mdc(a + b, m) = mdc(a, b)$.

Referências

COUTINHO, S. C. *Números inteiros e criptografia RSA*. Rio de Janeiro: IMPA, 2005.

HEFEZ, A. *Curso de álgebra*. 3. ed. Rio de Janeiro: IMPA, 2002.

MILIES, F. C. P.; COELHO, S. P. *Números*: uma introdução à matemática. 3. ed. São Paulo: Editora da Universidade de São Paulo, 2003.

MOREIRA, G. C. T. de A.; SALDANHA, N. *Primos de Mersenne e outros primos muito grandes*. Rio de Janeiro: IMPA, 1999.

RIBENBOIM, P. *Números primos*: mistérios e recordes. Rio de Janeiro: IMPA, 2001.

SANTOS, J. P. de O. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2007.

VIDIGAL, A. *et al*. *Fundamentos de álgebra*. Editora UFMG, 2005.

WIKIPÉDIA. Disponível em http://pt.wikipedia.org/wiki/. Acesso em: 21 fev. 2010.

Sobre a autora

Ana Cristina Vieira possui graduação em Matemática pela Universidade Federal Fluminense (1988), mestrado em Matemática pela Universidade de Brasília (1991) e doutorado em Matemática também pela Universidade de Brasília (1997). Atualmente é professora associada da Universidade Federal de Minas Gerais. Tem experiência na área de Matemática, com ênfase em Teoria de Grupos e Teoria de Anéis, atuando principalmente nos seguintes temas: álgebras de grupos, grupos de automorfismos de árvores, representações de grupos e álgebras com identidades polinomiais.

Para obter mais
informações sobre
outros títulos da
EDITORA UFMG,
visite o site

www.editora.ufmg.br

A presente edição foi composta pela Editora UFMG, em caracteres Chaparral Pro e Optima Std, e impressa pela Imprensa Universitária da UFMG, em sistema offset 90g (miolo) e cartão supremo 250g (capa), em 2012.