

# Matemática Elemental



## **UNIVERSIDADE FEDERAL DA PARAÍBA**

### **Reitora**

MARGARETH DE FÁTIMA FORMIGA MELO DINIZ

### **Vice-Reitor**

EDUARDO RAMALHO RABENHORST



## **EDITORA DA UFPB**

### **Diretora**

IZABEL FRANÇA DE LIMA

### **Vice-Diretor**

JOSÉ LUIZ DA SILVA

### **Supervisão de Editoração**

ALMIR CORREIA DE VASCONCELLOS JÚNIOR

### **Supervisão de Produção**

JOSÉ AUGUSTO DOS SANTOS FILHO

## **CONSELHO EDITORIAL**

**Prof Dr. Lucídio Cabral .....(UFPB)**

**Prof Dr. Danielle Rousy.....(UFPB)**

**Prof Ms Eduardo Santana.....(UFPB)**



**Hélio de Menezes Silva**

# Matemática Elementar

Editora da UFPB  
João Pessoa  
2013

Capa - Projeto gráfico: Renato Arrais e Eduardo Santana

Catálogo na publicação  
Universidade Federal da Paraíba  
Biblioteca Setorial do CCEN

S587s Silva, Hélio de Menezes.

Matemática elementar/ Hélio de Menezes Silva. – João Pessoa: Editora da UFPB, 2013.

119p. : il. –

Livro do aluno desta disciplina no Curso de Licenciatura em Computação. Unidade de Educação a distância Unidade Federal da Paraíba.

ISBN: 978-85-237-0698-2

1. Matemática. 2. Lógica matemática . 3. Matemática elementar. I.  
Título.

BS-CCEN

CDU 51

Todos os direitos e responsabilidades dos autores.

EDITORA DA UFPB  
Caixa Postal 5081 – Cidade Universitária  
João Pessoa – Paraíba – Brasil  
CEP: 58.051 – 970  
<http://www.editora.ufpb.br>

Impresso no Brasil  
*Printed in Brazil*

# **Matemática**

# **Elementar**

Prof. **Hélio de Menezes Silva**

1ª. edição (mar.2013)

Livro do aluno desta disciplina no  
Curso de **Licenciatura em Computação**

Unidade de Educação a Distância  
**Universidade Federal da Paraíba**  
UFPB Virtual

<http://portal.virtual.ufpb.br/wordpress/cursos/licenciatura-em-computacao/>

**Dedico** este livro a  
**Raquel,**  
**Sandra,**  
**Mauro,**  
**Airton e**  
**Sérgio,**

os cinco maravilhosos filhos que Deus deu de presente a mim e a Nira. Vocês são o maior tesouro e a maior causa de júbilo e alegria que recebemos sobre esta terra! Bem, sinto muita falta e saudades de Mauro, mas sei que qualquer dia desses vamos nos encontrar de novo, no céu, e, enquanto isso, eu e Nira queremos aproveitar mais e melhor nossos dias com nossos outros filhos, e netos.

**Agradeço** à minha esposa, *Valdenira Nunes de Menezes Silva*, por ter assumido muitas das minhas tarefas, a fim de me dar tempo para escrever este livro em curto prazo de tempo.

Agradeço aos professores *Rivanildo Garcia da Silva* e *José Miguel Aroztegui* por suas contribuições e revisões do cap. 1; *Joseluze de Farias Cunha*, cap. 2; *Lucídio dos Anjos Formiga Cabral*, cap. 6.

Agradeço ao alunos *Túlio Albuquerque Pascoal*, cap. 3. Os exemplos das falácias citadas no cap. 2 são adaptações de respostas por meus *alunos de Linguagens Formais*, em trabalho para casa, no período 2012.2.

Hélio de Menezes Silva, março 2013.

Salmo 8:3 ¶ Quando vejo os teus céus, obra dos teus dedos, a lua e as estrelas que preparaste;

4 Que é o homem mortal para que te lembres dele? e o filho do homem, para que o visites?

5 Contudo, pouco menor o fizeste do que os anjos, e de glória e de honra o coroaste.

6 Fazes com que ele tenha domínio sobre as obras das tuas mãos; tudo puseste debaixo de seus pés:

7 Todas as ovelhas e bois, assim como os animais do campo.

8 As aves dos céus, e os peixes do mar, e tudo o que passa pelas veredas dos mares.

9 Ó SENHOR, Senhor nosso, quão admirável é o teu nome sobre toda a terra! (LTT)

# **Apresentação da Disciplina**

Parabéns, meu aluno e amigo, pela sua decisão de estudar e fazer um curso superior, particularmente Licenciatura em Computação na UFPB, enquanto muitos se abandonam ao não fazer nada da vida. Parabéns. Sei que alguns de vocês trabalham, muitos moram onde não há muitos meios e oportunidades, por isso lhe dou pessoalmente parabéns pela garra e determinação em fazer este curso através do EAD.

Tenho a firme convicção que, com sua disciplina e determinação amigo (isto será a chave!), a EAD pode formar profissionais de grande competência, EAD pode ser o futuro da educação, inclusive revertendo paradigmas seculares, <http://usatoday30.usatoday.com/life/people/story/2012-05-30/sal-khan-profile-khan-academy/55270348/1>. Sou um entusiasta da EAD, mas deixe-me avisá-lo, ela precisa de duas coisas básicas: autodisciplina e esforço. Se você não tiver essas qualidades e de modo nenhum as quiser desenvolver, deixe-me ser franco, dificilmente conseguirá muito na vida, em quase nada. Na EAD, você precisa ter a autodisciplina de diariamente dedicar várias horas ao estudo. Sozinho ou em grupo, você precisa fazer por si mesmo todos os exemplos e pelo menos 1/3 dos exercícios, saltando de três em três. Vou bater nessa mesma tecla em todas as unidades.

Quanto ao curso, minha aspiração é que ele lhe faça ainda mais um vencedor, em DUAS vertentes: a) tendo capacidade técnica para, se imposto pela vida, disputar corrida com os bacharéis em Ciência da Computação e cursos similares (por que não?); e b) sendo o profissional por excelência na nobre profissão de professor na educação básica e na técnico- profissionalizante, talvez fazendo pós-graduação e ensinando em universidades. Almejo e antevejo duas vertentes à sua disposição, para seu futuro.

Quanto à disciplina em si (Matemática Elementar) de que tomo como privilégio poder escrever este livro e lhe ensinar, é uma das primeiras e mais básicas para tudo o mais. Não é uma disciplina fácil, pois é muito densa, tem muito conteúdo em pouco tempo e espaço, mas tem que ser assim. Se, ao final dela, você não dominar seu assunto muito bem, provavelmente terá muita dificuldade para acompanhar as 3 outras disciplinas de Matemática, mais as 3 disciplinas Estrutura de Dados (que avançará em grafos), Teoria da Computação (que avançará em lógica e outros formalismos) e Agentes Inteligentes (idem).

O objetivo específico da disciplina é lhe capacitar plenamente nos assuntos da sua ementa: 1) Teoria dos Conjuntos: axiomas, operações elementares, relações, funções, ordenação, números naturais, conjuntos contáveis e incontáveis. 2) Introdução à Lógica Matemática. 3) Recorrência e Indução. 4) Noções básicas: proposições, provas/demonstrações. 5) Métodos de Enumeração: permutação, combinação e o teorema de Ramsey. 6) Grafos: terminologia básica, classes de grafos, grafos ponderados e orientados, ciclos e circuitos, árvores. Adicionei como um 7º tópico Teoria dos Números, ao invés de abordá-lo distribuído nos tópicos anteriores. Fica melhor assim.

Os livros-texto da disciplina, se você tiver acesso a eles em papel ou computador, são

- GERSTRING, J. L. Fundamentos Matemáticos para Ciência da Computação. Rio de Janeiro: LTC, 3 ed., 1995.
- ROSEN, K. H. Discrete Mathematics and its Applications. 4. ed. McGraw-Hill, 1999.
- IEZZI, G. et al. Fundamentos de Matemática Elementar: conjuntos e funções. 6 ed. São Paulo: Atual, Vol. 1, 1993..
- DAGHLIAN, J. Lógica e Álgebra de Boole. São Paulo: Editora Ática, 1990.

mas creio que este presente livro deverá ser suficiente para a maior parte da disciplina, você só precisando consultar os livros-texto se se interessar por maior aprofundamento em certos tópicos que despertem seu interesse. Também, espalhados por este livro, colocarei links para vários outros livros, notas de aula e artigos disponibilizados na internet, particularmente quando eu tiver extraído exemplos e problemas deles, ou quando eu quiser sugerir que você faça tais exercícios.

O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem). Mas, repito, o início de tudo, a chave, é você mesmo ser determinado e disciplinado, cada semana dedicando 4 a 8 horas para estudar este livro com todo afinho.

Sucesso, meu amigo. Começemos nossa jornada na Matemática Elementar. Que, ao final do seu esforço, mesmo duro, você a avalie como lhe tendo dado a satisfação de ter dominado o assunto, e eu a satisfação de lhe ter ajudado nisso.

Prof. *Hélio de Menezes Silva*, mar.2013.

DCC/ CI/ UFPB – Universidade Federal da Paraíba, Campus de João Pessoa.

.....



# Conteúdo

(da disciplina *Matemática Elementar [e Discreta]*)

## Conteúdo

1. CONJUNTOS, RELAÇÕES, FUNÇÕES .....	7
1.1. Axiomas e Definições sobre Conjuntos. Relações entre Conjuntos .....	8
1.2. Operações com Conjuntos .....	9
1.3. Relações.....	11
1.4. Funções.....	12
1.5. Ordenação.....	14
1.6. Números Naturais, Inteiros, Racionais, Reais .....	16
1.7. Conjuntos Contáveis e Não-Contáveis.....	16
Problemas sobre toda a Unidade: .....	18
Recapitulando a unidade .....	20
2. Introdução à LÓGICA MATEMÁTICA .....	21
2.1. Motivação. Lógica. Porque só Veremos a Lógica Proposicional .....	21
2.2. A Linguagem $\mathcal{L}$ da Lógica Proposicional .....	22
2.2.1. A Sintaxe de $\mathcal{L}$ .....	23
2.2.2. A Semântica de $\mathcal{L}$ .....	25
2.3. Regras de Inferência sobre $\mathcal{L}$ . Sistemas Formais. Sistema Natural de Inferência.....	27
2.4. Sanidade, Completude, Consistência. Os Problemas da Satisfatibilidade e da Tautologia (são Decidíveis, mas NP-Completo). Modelo e Teoria .....	31
Problemas sobre toda a Unidade: .....	32
Recapitulando a Unidade.....	32
Apêndice à Unidade II: Falácias Lógicas .....	33
3. EQUAÇÕES DE RECORRÊNCIA e PROVAS POR INDUÇÃO MATEMÁTICA.....	39
3.1. Equações de Recorrência. Determinação Delas. Fórmulas Fechadas (Conjecturas) .....	39
3.2. Provas pelo Princípio da Indução Matemática Simples (ou Fraca) .....	42
3.3. Provas pelo Princípio de Indução Matemática Completa (ou Forte) .....	47
Problemas sobre toda a Unidade: .....	49
Recapitulando a unidade .....	50
4. PROVAS DEDUTIVAS .....	51
4.1. INTRODUÇÃO (Definição de Prova (ou Demonstração) Matemática) .....	52
4.2. DESEMARANHANDO AS DEFINIÇÕES (Começando a Prova) .....	53
4.3. PROVANDO/ DISPROVANDO AFIRMAÇÕES UNIVERSAIS "SE-ENTÃO" ("Se P, então Q") .....	54
4.3.1. Provas Diretas .....	54
4.3.2. Provas Indiretas.....	58
4.4. PROVAS "SE- E- SOMENTE- SE" (baseadas em Larry W. Cusick) .....	62
4.5. PROVANDO PROPOSIÇÕES EXISTENCIAIS .....	63
4.5.1. Achando Exemplo ("Adivinhando" o Elemento).....	63
4.5.2. Prova Construtiva de Existência .....	63
4.5.3. Prova Não- Construtiva de Existência .....	64
4.6. QUE SIGNIFICA "BEM DEFINIDO"? .....	65
4.7. O PRINCÍPIO DAS CASAS DE POMBO [ou Princípio das Gavetas de Dirichlet] .....	66
4.8. ERROS COMUNS NAS [pseudo] "PROVAS" .....	67
Recapitulando a unidade .....	68
5. Introdução à ANÁLISE COMBINATÓRIA .....	69
5.1. Técnicas Básicas de Contagem. Permutações, Arranjos, Combinações .....	69
5.2. Relações de Recorrência.....	74
5.3. Coeficientes Binomiais .....	75
5.4. Outras Sequências de Contagem.....	76
5.5. Teorema de Ramsey .....	78
PROBLEMAS PROPOSTOS (com respostas) .....	79
Recapitulando a unidade .....	81
6. Introdução a GRAFOS E ÁRVORES.....	83
6.1. Motivação e Introdução .....	83
6.2. Conceitos Básicos de Grafos e Digrafos .....	84
6.3. Percursos em Grafos em Geral e em Cliques .....	89
6.4. Árvores e Árvores Geradoras.....	91
Recapitulando a Unidade.....	94
7. Introdução à TEORIA DOS NÚMEROS.....	97
7.0. DEFINIÇÃO: A TEORIA DOS NÚMEROS ... ..	97

7.1. NÚMEROS PRIMOS.....	98
7.1.1. Testando Primalidade de $n$ : .....	99
7.1.2. Contando os Primos .....	101
7.1.3. Mais Algumas Poucas Coisas Sobre os Primos .....	101
7.2. DIVISIBILIDADE .....	104
7.2.1. Máximo Divisor Comum (mdc) .....	104
7.2.2. Mínimo Múltiplo Comum (mmc) .....	109
7.3. ARITMÉTICA MODULAR.....	110
7.3.1. – Problema 374 do ACM Programming Contest (BigMod).....	111
7.4. CONGRUÊNCIAS .....	113
7.4.1. Operações Sobre Congruências.....	113
7.4.2. Resolvendo Congruências Lineares.....	114
7.4.3. Equações Diofantinas .....	115
7.5. TRIPLAS PITAGÓRICAS: .....	115
Recapitulando a unidade .....	117

.....



## UNIDADE I

# 1. CONJUNTOS, RELAÇÕES, FUNÇÕES

(Como você, com suficiente carga horária e profundidade, já estudou este assunto no ensino médio e para o recente vestibular, e como estaremos apenas fazendo uma revisão dele, então vamos andar algo sumária e rapidamente, sem provas de fórmulas e teoremas, para que sobre tempo de estudo e espaço no livro para explicarmos melhor os assuntos realmente novos para você.)

**Nosso objetivo, nesta unidade,** é, ao final dela, você <sup>(voltar a)</sup> dominar as mais básicas noções e propriedades dos conjuntos, das relações e operações entre eles; da ordenação entre os seus elementos; dos conjuntos de números naturais, de inteiros, de racionais e de reais; dos conjuntos contáveis e não contáveis.

Lembre-se: *estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, **cada semana dedicando 4 a 8 horas para estudar este livro**, entender e reter os exemplos, resolver sozinho pelo menos 1/3 dos exercícios propostos, sumariar em sua mente os principais pontos desta unidade. Sem determinação de firme propósito, sem disciplina e esforço honesto, então talento e boa vontade não bastam para nenhuma vitória na nossa vida, não é?*

### Conteúdo desta unidade:

- 1.1. Axiomas e Definições sobre Conjuntos. Relações entre Conjuntos
- 1.2. Operações com Conjuntos
- 1.3. Relações entre Conjuntos
- 1.4. Funções
- 1.5. Ordenação
- 1.6. Conjuntos dos Números Naturais, e dos Inteiros, e dos Racionais, e dos Reais
- 1.7. Conjuntos Contáveis e Não Contáveis



Se você quiser ver o assunto mais explicada e profundamente, não precisará de mais que os livros textos da ementa da disciplina.

Mas, para escrever esta unidade, além deles também usamos (mais como esqueleto mestre e plano geral e ordem de apresentação) partes do livro *Matemática Elementar* que se encontra disponível em [http://pt.wikibooks.org/wiki/Matem%C3%A1tica\\_elementar](http://pt.wikibooks.org/wiki/Matem%C3%A1tica_elementar). Não o copiamos de cabo a rabo, somente "pegamos mais o jeito" dele. Assim fizemos por causa de sua concisão e objetividade, mas acrescentamos "carne" baseada nos livros-texto e em outros, omitimos algumas partes, modificamos muitas outras, acrescentamos exemplos, etc. Os exemplos e problemas propostos foram-nos gentilmente sugeridos pelo Prof. *Rivanildo Garcia da Silva*, e o Prof. *José Miguel Aroztegui* revisou todo o texto

### Símbolos para esta unidade:

$\in$ : pertence	$\notin$ : não pertence
$\subseteq$ : está contido (podendo ser igual)	

$\Rightarrow$ : implica logicamente que; se então	$\Leftrightarrow$ : equivale logicamente a; se, e somente se
$\exists$ : existe	$\nexists$ : não existe

$\subset$ : está contido propriamente (não podendo ser igual)	$\not\subset$ : não está contido propriamente (nem é igual)
$\supseteq$ : contém (podendo ser igual)	
$\subsetneq$ : contém propriamente (não podendo ser igual)	$\not\supseteq$ : não contém propriamente
$\emptyset$ : conjunto vazio	$ $ : tal que

$\forall$ : para todo (ou qualquer que seja)	
<b>N</b> : conjunto dos números naturais	<b>Z</b> : conjunto dos números inteiros
<b>Q</b> : conjunto dos números racionais	<b>R</b> : conjunto dos números reais

## 1.1. Axiomas e Definições sobre Conjuntos. Relações entre Conjuntos

Em Matemática, conjunto, elemento e relação de pertinência são conceitos primitivos, isto é, que não podem ser formalmente definidos em função de conceitos mais simples, portanto são aceitos sem definição formal. Mas, informalmente, podemos dizer que um **conjunto** é uma coleção de objetos (chamados de **elementos**). Os elementos podem representar qualquer coisa (até mesmo outros conjuntos). Um conjunto possui como única propriedade os elementos que contém, portanto dois conjuntos que têm os mesmos elementos são **conjuntos iguais**. A relação básica entre um elemento e um conjunto é a relação de pertinência: quando um objeto  $x$  é um dos elementos que compõem o conjunto  $A$ , dizemos que  $x \in A$  (leia "x pertence a A"), senão dizemos que  $x \notin A$  (leia "x não pertence a A").

Nos conjuntos, a ordem e a quantidade de vezes que os elementos estão listados na coleção não é relevante. Em contraste, uma coleção de elementos na qual a multiplicidade, mas não a ordem, é relevante, é chamada **multiconjunto** [Knuth, Donald E. (1998). *The Art of Computer Programming – Vol. 2: Seminumerical Algorithms* Addison Wesley. p. 694]. Exemplos: conjunto  $\{1,5,2,4,3\}$ ; multiconjunto  $\{1,1,1,5,2,4,3,3\}$ .

É possível descrever o mesmo conjunto de três maneiras diferentes, por meio de uma:

- lista dos seus elementos (ideal para conjuntos pequenos e finitos);
- definição de uma propriedade de seus elementos;
- representação gráfica (recorde-se dos diagramas de Venn, nos livros do ensino médio).

A notação padrão em Matemática lista os elementos separados por vírgulas e delimitados por chaves. Um conjunto  $A$ , por exemplo, poderia ser representado como:  $A = \{1,2,3\}$

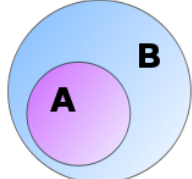
Como a ordem não importa em conjuntos, isso é equivalente a escrever, por exemplo,  $A = \{1,2,2,1,3,2\}$

Um conjunto  $A$  também fica definido (ou determinado, ou caracterizado) quando se dá uma regra que permita decidir se um objeto arbitrário pertence ou não a  $A$ . Por exemplo, a frase "B é o conjunto dos triângulos retângulos" define perfeitamente o conjunto  $B$ , já que permite decidir se um objeto qualquer é ou não é um elemento de  $B$ . O mesmo conjunto  $A$  do parágrafo anterior poderia ser representado por uma regra:

$$A = \{x \mid x \text{ é um número inteiro maior que } 0 \text{ e menor que } 4\}$$

ou ainda:

$$A = \{x : x \text{ é um número natural tal que } 1 \leq x \leq 3\}$$

	<p>Se <math>A</math> e <math>B</math> são conjuntos e todo o elemento <math>x</math> pertencente a <math>A</math> também pertence a <math>B</math>, então o conjunto <math>A</math> é dito um <b>subconjunto</b> do conjunto <math>B</math>, o que é denotado por <math>A \subseteq B</math>. Note que esta definição inclui o caso em que <math>A</math> e <math>B</math> possuem os mesmos elementos, ou seja, <math>A = B</math>. Se <math>A \subseteq B</math> e ao menos um elemento pertencente a <math>B</math> não pertence a <math>A</math>, então <math>A</math> é chamado de <b>subconjunto próprio</b> de <math>B</math>, o que é denotado por <math>A \subset B</math>.</p>
---	--

Todo conjunto é subconjunto dele mesmo ( $A \subseteq A$ ), entretanto não se enquadra na definição de subconjunto próprio, portanto ( $A \not\subset A$ ) e é chamado de **subconjunto impróprio**.

Todo conjunto também possui como subconjunto o **conjunto vazio** [o conjunto que não tem nenhum elemento] representado por  $\{\}$  ou  $\emptyset$  (a letra “phi”, leia “fí”). Como todos os conjuntos vazios são iguais uns aos outros, é permissível falar de um único conjunto sem elementos.

Ao conjunto da totalidade de elementos que consideramos possíveis [para o assunto de que estivermos tratando] chamamos de **conjunto universo**, usualmente representado pelo símbolo  $U$ . Por exemplo, se estivermos tratando das siglas dos estados do Brasil,  $U = \{AC, AL, AP, \dots, TO\}$

EXERCÍCIO: Você mesmo reveja seus livros, dê o nome exato, e defina formalmente as relações entre elemento e conjunto  $\in, \notin$ . E as relações entre dois conjuntos:  $\subseteq, \subset, \supseteq, \supset, \not\subseteq, \not\subset, =, \neq$ . Dê um exemplo para cada relação usando diagramas de Venn, outro usando a notação  $\{\}$ , outro definindo os conjuntos por suas propriedades.

Se um conjunto  $A$  tem  $n$  elementos, onde  $n$  é um número natural (possivelmente 0), então diz-se que o conjunto é um conjunto finito com uma **cardinalidade** de  $n$ , [e denotamos isto como  $|A| = n$ , que você deve ler como “a cardinalidade de  $A$  é  $n$ ”]. Mesmo se o conjunto não possui um número finito de elementos, pode-se definir a cardinalidade graças ao trabalho desenvolvido pelo matemático Georg Cantor. Mais sobre isso na seção 1.7 (Conjuntos Contáveis e Não Contáveis)

O conjunto de todos os subconjuntos de um conjunto dado  $A$  é chamado de **conjunto potência** (ou **conjunto das partes**) de  $A$ , denotado por  $P(A)$ . O conjunto potência é uma álgebra booleana (ver Unidade II) sobre as operações de união e interseção. Sendo o conjunto dado  $A$  finito, com  $n$  elementos, prova-se que o número de subconjuntos (ou seja, o número de elementos do conjunto potência, ou seja, o conjunto das partes de  $A$ ) é  $2^n$ , ou seja, a cardinalidade do conjunto das partes de  $A$  é igual a  $2^n$ . Exemplo: o conjunto  $A = \{1, 2\}$  tem 4 subconjuntos, são eles: o próprio  $A$ ,  $\{1\}$ ,  $\{2\}$  e  $\emptyset$ . Veja que  $n = |A| = 2$  e há  $2^2 = 4$  subconjuntos. Exercício: Entenda e explique porque  $P(\emptyset)$  é  $\{\emptyset\}$  e não é  $\emptyset$ .

O **produto cartesiano** de dois conjuntos  $A$  e  $B$  é o conjunto de **pares ordenados** (relembre isso, por você mesmo):

$$A \times B = \{(a, b) : a \in A \text{ e } b \in B\}$$

O produto cartesiano é não-comutativo:  $A \times B \neq B \times A$

EXEMPLO 1: Sejam  $A = \{0, 2, 5\}$  e  $B = \{2, 3\}$ . Temos:  $A \times B = \{(0, 2), (0, 3), (2, 2), (2, 3), (5, 2), (5, 3)\}$  e  $B \times A = \{(2, 0), (3, 0), (2, 2), (3, 2), (2, 5), (3, 5)\}$ . Note que  $A \times B \neq B \times A$ , pois  $(x, y) \neq (y, x)$ , para todo  $x$  e para todo  $y$ .

EXEMPLO 2: Dados conjuntos  $A = \{x \mid x \text{ é número par primo}\}$  e  $B = \{x \mid x \text{ é divisor positivo de } 6\}$ , temos  $A \times B = \{(2, 1), (2, 2), (2, 3), (2, 6)\}$  e  $B \times A = \{(1, 2), (2, 2), (3, 2), (6, 2)\}$ . Note que  $A \times B \neq B \times A$

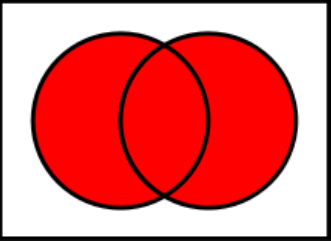
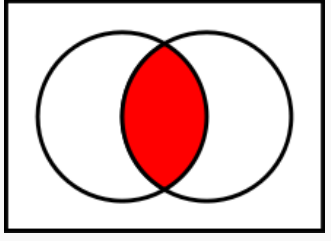
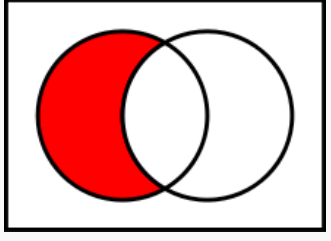
EXEMPLO 3: Considere os conjuntos  $C = \{1\}$ ,  $D = \{1, 2, 3\}$ ,  $E = \{1, 3, 5, 7, \dots\}$  e  $F = \{x \mid x \text{ é número primo}\}$ . Classifique as sentenças a seguir em verdadeira ou falsa.

- |                  |                          |                      |
|------------------|--------------------------|----------------------|
| a) $C \supset D$ | d) $D \not\subset E$     | g) $E = F$           |
| b) $C \subset E$ | e) $F \supset E$         | h) $C \not\subset F$ |
| c) $D \subset F$ | f) $\emptyset \subset C$ | i) $E \supset C$     |

Resposta: f v f v f v f v f v (respectivamente)

## 1.2. Operações com Conjuntos

Operação	Operador	Definição	Exemplo
----------	----------	-----------	---------

União	$\cup$	<p>A união (ou reunião) de dois conjuntos <math>A</math> e <math>B</math> é o conjunto <math>A \cup B</math> composto dos elementos que pertencem ao menos a um dos conjuntos <math>A</math> ou <math>B</math>. A união de <math>N</math> conjuntos <math>S = S_1 \cup S_2 \cup S_3 \cdots \cup S_N = \cup_{i=1}^N S_i</math> é o conjunto formado pelos os elementos que pertencem ao menos a um dos conjuntos <math>S_i</math>. A união entre dois conjuntos pode ser definida formalmente por <math>A \cup B = \{\forall x   x \in A \text{ ou } x \in B\}</math></p>	 <p><math>A \cup B</math></p>
Interseção	$\cap$	<p>A interseção de dois conjuntos <math>A</math> e <math>B</math> é o conjunto <math>A \cap B</math> composto dos elementos que pertencem simultaneamente aos dois conjuntos <math>A</math> e <math>B</math>.</p>	 <p><math>A \cap B</math></p>
Diferença	$\setminus$ ou $-$	<p>A diferença <math>A \setminus B</math> (ou <math>A - B</math>) entre dois conjuntos <math>A</math> e <math>B</math> é o conjunto dos elementos que pertencem a <math>A</math> e que não pertencem a <math>B</math>.</p>	 <p><math>A \setminus B</math></p>

Dado um universo  $U$ , diz-se **complementar de** um conjunto **A**, em relação ao universo **U**, o conjunto (denotado por  $A^c$ ) que contém todos os elementos presentes no universo e que não pertençam a  $A$ . Também define-se complementar para dois conjuntos, contanto que um deles seja subconjunto do outro. Nesse caso, diz-se, por exemplo, **complementar de B em relação a A** (sendo  $B$  um subconjunto de  $A$ ) — é o complementar relativo — e usa-se o símbolo  $\complement_A$ . Leia  $\complement_A^B$  como “o conjunto complementar de  $B$  em relação a  $A$ , que é seu superconjunto”. Matematicamente:

$$\complement_A^B = A - B = \{x \in A \mid x \notin B\}$$

EXEMPLO 4: Seja  $A = \{1,2,3,4\}$ ,  $B = \{x \mid x \text{ é número natural primo menor que } 6\}$  e  $C = \{1,2,3,4,5,6,7,8,9\}$ . Determine:

- a)  $A \cup B$                       b)  $A \cap C$   
 c)  $A - C$                       d)  $B - A$   
 e)  $C - A$

Respostas:

- a)  $\{1,2,3,4,5\}$                       b)  $\{1,2,3,4\}$   
 c)  $\emptyset$                               d)  $\{5\}$   
 e)  $\{5,6,7,8,9\}$

EXEMPLO 5: Dados os conjuntos  $A = \{0,2,4\}$ ,  $B = \{0,1,2,3,4,5\}$  e  $C = \{0,1,2,4,8\}$ , determine:

- a)  $\complement_B^A$                       a')  $B \setminus A$   
 b)  $\complement_B^C$                       b')  $B \setminus C$

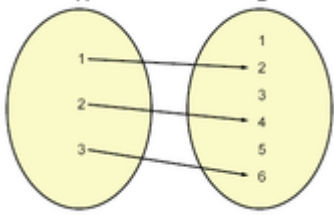
Respostas:

- a)  $\complement_B^A = B - A = \{1,3,5\}$ ;                      a')  $B \setminus A = B - A = \{1,3,5\}$ ;  
 b)  $\complement_B^C =$  não definido, pois  $C \not\subseteq B$ ;                      b')  $B \setminus C = B - C = \{3,5\}$

## 1.3. Relações

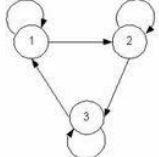


Uma **relação R do conjunto A para o conjunto B** (representada por  $R: A \rightarrow B$ ) é um qualquer subconjunto do produto cartesiano  $A \times B$ . Ou seja, é o conjunto de pares ordenados cujo primeiro elemento pertence a A e o segundo elemento pertence a B. O conjunto A é chamado de **domínio** da relação, o conjunto B é chamado de **contradomínio** da relação.

Relações podem ser **especificadas/ representadas**: por figuras dos dois conjuntos A, B, com setas indicando os pares ordenados; por listagem de todos os pares; ou por equação, inequação, ou qualquer forma matemática que possa representar a condição que os pares devem satisfazer. Por exemplo:

	$R = \{(1,2), (2,4), (3,6)\}$	$A = \{1,2,3\}$ $B = \{1,2,3,4,5,6\}$ $R = \{(x,y) \in A \times B \mid y = 2x = \text{dobro de } x\}$
---	-------------------------------	---

Existe um tipo especial de relação que é chamado **função**: é a relação na qual, para todo elemento do domínio, há correspondência de um (e somente um) elemento no contradomínio. A função normalmente é simbolizada por  $f(x)$  (sendo  $x$  uma variável, ou seja, um valor que pode representar qualquer elemento do conjunto domínio). Como consequência natural da correspondência de todo e cada elemento do domínio para exatamente um elemento do contradomínio, a função é sempre uma relação definida por uma equação (pois uma inequação associa um elemento do domínio a vários elementos do contradomínio). Funções serão estudadas com maiores detalhes na próxima seção (1.4).

**Relações de equivalência:** Seja  $R$  uma relação entre os conjuntos A e B, ou seja,  $R \subseteq A \times B$ . Denotaremos que um elemento  $a$  de A se relaciona com o elemento  $b$  de B, segundo a relação  $R$ , por  $aRb$ . Se uma relação  $R$  definida com domínio A e contradomínio A cumpre as seguintes propriedades:

		
$\forall a \in A: aRa$ (propriedade reflexiva),	$\forall a,b \in A: aRb \Leftrightarrow bRa$ (propriedade simétrica),	$\forall a,b,c \in A: aRb \wedge bRc \Rightarrow aRc$ (propriedade transitiva),

ela é dita relação de equivalência.

**Classes de equivalência:** Seja  $\bar{a} = \{x \in A \mid xRa\}$ .  $\bar{a}$  é denominada **classe de equivalência** de  $a$ . Alguns resultados importantes desta definição são (demonstrações nos livros-texto da disciplina):

Teorema: Se  $a \in \bar{a} \Rightarrow \bar{a} = \bar{a}$ .

Teorema: Se  $a \notin \bar{a}$ , então  $\bar{a} \cap \bar{a} = \emptyset$

Teorema: Se  $\bar{a} \neq \bar{b}$ , então  $\bar{a} \cap \bar{b} = \emptyset$

Uma **partição** de um conjunto X é um conjunto P tal que

$x \in P \Rightarrow x \subseteq X$

$x, y \in P \Rightarrow x \cap y = \emptyset$

$x \in X \Rightarrow \exists a \in P$  tal que  $x \in a$ .

Alguns resultados importantes desta definição são (demonstrações nos livros-texto da disciplina):

Teorema: Seja  $R$  uma relação de equivalência em A,  $P = \{\bar{a} \subseteq A \mid a \in A\}$  é uma partição de A.



**Teorema:** Seja  $P$  uma partição de  $A$ , a relação  $R$  dada por  $aRe \Leftrightarrow a \in \bar{e}$  é de equivalência. Disto sabemos que toda partição induz uma relação de equivalência e toda relação de equivalência induz uma partição.

**EXEMPLO 6:** Seja  $E = \{a, b, c\}$ . A relação  $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$  é uma relação de equivalência? Resposta: Sim, pois satisfaz as três propriedades definidas acima.

**EXEMPLO 7:** A relação  $S = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c)\}$  é uma relação de equivalência? Resposta: Não, pois  $aRc$  mas  $\neg(cRa)$  ( $c$  não está relacionado com  $a$ )

**EXEMPLO 8:** Seja a relação de equivalência  $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ . Determine as classes de equivalência  $\bar{a}$ ,  $\bar{b}$ ,  $\bar{c}$ .

Resposta:  $\bar{a} = \{a, b\}$ ;  $\bar{b} = \{a, b\}$ ;  $\bar{c} = \{c\}$

**EXEMPLO 9:** Seja  $A = \{1, 2, 3, 4\}$ . Determine uma partição desse conjunto.

Resposta:  $P = \{\{1\}, \{2, 3\}, \{4\}\}$  ou  $P = \{\{1, 2\}, \{3, 4\}\}$ , entre outras.

## 1.4. Funções

Uma **função** é uma relação especial, assim definida: sejam dois conjuntos  $A$  e  $B$  (não vazios), tais que para *todo* elemento  $x$  pertencente a  $A$  (chamado de **domínio**), haja uma **correspondência** de *um e somente um* elemento  $y$  (chamado imagem) pertencente a  $B$  (chamado de **contradomínio**). Essa correspondência é a função: a associação, definida de algum modo, entre todos os elementos de um conjunto e os elementos de outro conjunto. O subconjunto  $B'$  de  $B$  compreendendo todos os elementos que são realmente imagens de elementos de  $A$  também é chamado de **imagem**.

A função que associa um elemento  $x$  a outro valor pode ser indicada por  $f(x)$ .  $x$  é chamada de **variável independente** e  $f(x)$  (ou  $y$ ) é chamada de **variável dependente**. Matematicamente a função é assim definida:

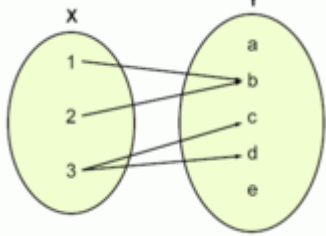
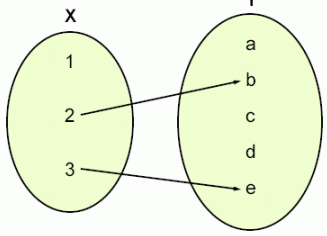
$$f: A \rightarrow B: x \rightarrow f(x),$$

Um exemplo de função: dado o conjunto dos números naturais, uma função pode associar cada número ao seu quadrado. Assim, essa função assumiria os valores:  $\{1, 4, 9, 16, \dots\}$ .

Note duas características de função, na definição:

- há **correspondência unívoca** entre um elemento e o valor associado a ele pela função: para cada valor assumido pela variável independente ( $x$ ) há um único valor da variável dependente ( $y$ ) associado pela função: Se  $t = f(x)$  e  $w = f(x)$ , então  $t = w$ .
- a correspondência é total, ou seja, um valor assumido pela variável dependente estará associado para todo valor possível de ser assumido pela variável independente.

A tabela a seguir mostra dois exemplos de relações que **não** são funções:

	
<p>Nesse caso, um mesmo elemento (3) do domínio <math>X</math> aparece associado a dois elementos do contradomínio <math>Y(c, d)</math>.</p>	<p>Aqui a correspondência não é total: falta um valor associado a 1.</p>

Duas funções  $f(x)$  e  $g(x)$  são ditas **iguais** ( $f = g$ ) se e somente se para cada valor de  $x$  no domínio  $D$ ,  $f(x)$  e  $g(x)$  assumam o mesmo valor:

$$\forall x \in D: (f(x) = g(x)) \Rightarrow (g = f).$$

- **Função Injetora** ( $f: A \rightarrow B$ ) é aquela na qual a diferentes elementos do domínio correspondem diferentes

elementos no contradomínio .  $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

• **Função Sobrejetora** ( $f: A \rightarrow B$ ) é aquela na qual o contradomínio é igual à imagem, ou seja, cada elemento do contradomínio é correspondido por ao menos um do domínio.  $\text{Imagem}(f) = B$ .

• **Função Bijetora** (ou **um- a- um**) ( $f: A \rightarrow B$ ) é aquela que é tanto injetora como sobrejetora: ( $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ ) e ( $\text{Imagem}(f) = B$ )

Uma função  $f(x)$  é chamada de **contínua** em um *ponto* quando, intuitivamente, a pequenas variações no valor de  $x$  correspondem pequenas variações no valor de  $f(x)$ . Nos pontos onde a função não é contínua, diz-se que a função é **descontínua**, ou que aquele é um **ponto de descontinuidade**. Formalmente, em termos de limites [rever nos seus livros do ensino médio], uma função  $f(x)$  é chamada de contínua em um ponto  $a$  de seu domínio se, quando  $x$  tende para  $a$  quer pela esquerda quer pela direita,  $\lim f(x) = f(a)$ . Uma função  $f(x)$  é chamada de contínua em um *intervalo* contínuo se for contínua em todos seus pontos.

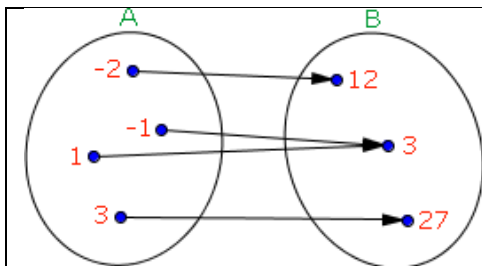
Uma função é dita **crescente**, sobre um intervalo  $[A,B]$ , se para cada valor de  $x + \varepsilon$  ( $\varepsilon$  sendo qualquer valor positivo),  $f(x) < f(x + \varepsilon)$ . ... É dita **não-decrescente**, ...  $f(x) \leq f(x + \varepsilon)$

**Composição de funções:** Sejam  $f: X \rightarrow Y$  e  $g: Z \rightarrow W$  duas funções. Se a imagem de  $f$  está contida no domínio de  $g$  podemos definir a **função composta**

$$g \circ f: X \rightarrow W$$

como sendo

$$g \circ f(x) = g(f(x)) \quad \forall x \in X$$



EXEMPLO 10 (função sobrejetora e não injetora):

Analisar o **diagrama de flechas** que está à esquerda.

Relembre que o conjunto  $A$  é o domínio da função e o conjunto  $B$  é o seu contradomínio; o conjunto imagem é o conjunto formado por todos os elementos do contradomínio que estão associados a pelo menos um elemento do domínio.

Classificamos como sobrejetora as funções que possuem o contradomínio igual ao conjunto imagem. Note que em uma função sobrejetora não existem elementos no contradomínio que não estão flechados por algum elemento do domínio.

Resposta:

Nesta função do exemplo temos:

Domínio:  $D(f) = \{-2, -1, 1, 3\}$

Contradomínio:  $CD(f) = \{12, 3, 27\}$

Conjunto Imagem:  $Im(f) = \{12, 3, 27\}$

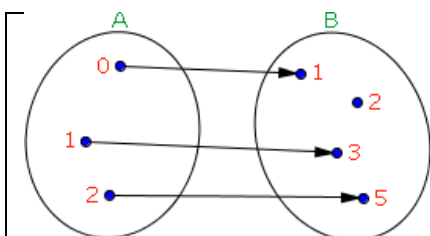
Portanto, nesta função, contradomínio é igual ao conjunto imagem.

Esta função é definida por:

$$f: A \rightarrow B, f(x) = 3x^2$$

Substituindo a variável independente  $x$ , de  $3x^2$ , por qualquer elemento de  $A$ , iremos obter o elemento de  $B$  ao qual ele está associado, isto é, obteremos  $f(x)$ .

Do que será explicado a seguir, poderemos concluir que embora esta função seja sobrejetora, ela não é uma função injetora, pois ambos  $-1$  e  $1$  têm  $3$  como imagem (eles têm a mesma imagem).



EXEMPLO 11 (função injetora e não sobrejetora):

Analisar o diagrama de flechas que está à esquerda.

Resposta:

Podemos notar que nem todos os elementos de  $B$  estão associados a algum elemento de  $A$ , isto é, nesta função o conjunto imagem difere do contradomínio, portanto esta não é uma função sobrejetora.

Além disso, podemos notar que esta função tem uma outra característica distinta da função anterior. Veja que não há nenhum elemento em  $B$  que está associado a mais de um elemento de  $A$ , ou seja, não há em  $B$  qualquer elemento com mais de uma flechada. Em outras palavras, não há mais de um elemento distinto de  $A$  com a mesma imagem em  $B$ .

Nesta função temos:

Domínio:  $D(f) = \{0, 1, 2\}$

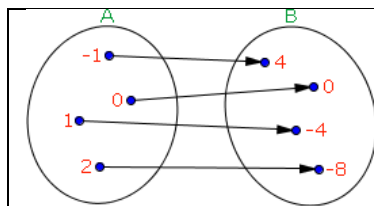
Contradomínio:  $CD(f) = \{1, 2, 3, 5\}$

Conjunto Imagem:  $\text{Im}(f) = \{1, 3, 5\}$

Definimos esta função por:

$$f: A \rightarrow B, f(x) = 2x + 1$$

Veja que não há no  $D(f)$  qualquer elemento que substituindo  $x$  em  $2x + 1$ , nos permita obter o elemento 2 do  $\text{CD}(f)$ , isto é, o elemento 2 do  $\text{CD}(f)$  não é elemento da  $\text{Im}(f)$ .



EXEMPLO 12 (função bijetora):

Analise o diagrama de flechas que está à esquerda.

Resposta:

Podemos ver que este é o diagrama de uma função sobrejetora, pois não há elementos em  $B$  que não foram flechados. Vemos, também, que esta é uma função injetora, já que todos os elementos de  $B$  recebem uma única flechada. Portanto, concluímos que a função é bijetora.

Esta função tem:

Domínio:  $D(f) = \{-1, 0, 1, 2\}$

Contradomínio:  $\text{CD}(f) = \{4, 0, -4, -8\}$

Conjunto Imagem:  $\text{Im}(f) = \{4, 0, -4, -8\}$

Esta função é definida por:

$$f: A \rightarrow B, f(x) = -4x$$

Ao substituirmos  $x$  em  $-4x$ , por cada um dos elementos de  $A$ , iremos encontrar os respectivos elementos de  $B$ , sem que sobre elementos em  $\text{CD}(f)$  e sem que haja mais de um elemento do  $D(f)$  com a mesma  $\text{Im}(f)$ .

EXEMPLO 12: Dadas as funções  $f(x) = 2x + 3$  e  $g(x) = 5x$ , determine  $g \circ f(x)$  e  $f \circ g(x)$ .

Resposta:

$$g \circ f(x) = g[f(x)] = g(2x + 3) = 5(2x + 3) = 10x + 15$$

$$f \circ g(x) = f[g(x)] = f(5x) = 2(5x) + 3 = 10x + 3. \text{ Observe que } f \circ g \neq g \circ f.$$

EXEMPLO 13: Dados três conjuntos  $A = \{-2, -1, 0, 3\}$ ,  $B = \{-3, -2, -1, 2\}$  e  $C = \{9, 4, 1, 4\}$ . Entre eles existem as seguintes funções:  $f: A \rightarrow B$  definida por  $f(x) = x - 1$  e  $g: B \rightarrow C$  definida por  $g(x) = x^2$ . Para cada elemento de  $A$  existe um elemento em  $B$  tal que  $f(x) = x - 1$  e para cada elemento de  $B$  existe um elemento de  $C$  tal que  $g(x) = x^2$ . Assim, pode-se concluir que existe uma função  $h: A \rightarrow C$  definida por  $h(x) = g(f(x))$ , isto é,  $h(x) = g(x-1) = (x-1)^2 = x^2 - 2x + 1$ .

## 1.5. Ordenação



Pela sua concisão, vamos usar, como esqueleto mestre e ordem de apresentação, partes de [http://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o\\_de\\_ordem](http://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o_de_ordem), que resume capítulo de Davey, B.A.; Priestley, H.A. *Introduction to Lattices and Order* 2nd. ed. Cambridge, Cambridge University Press, 2002. Mas omitiremos algumas partes, inseriremos muitas outras, acrescentaremos exemplos, muitas vezes refrasearemos em nossas próprias palavras. As referências principais sempre são os livros-texto da disciplina, sempre busque melhor entendimento neles.

Dado um conjunto  $A$  e uma relação binária  $R$  sobre  $A$ :  $R \subseteq A \times A$ , dizemos que  $R$  é uma **relação de ordem parcial- ampla (ou não estrita)** sobre  $A$  se satisfaz as seguintes condições:

- **Reflexividade:**  $\forall a \in A: aRa$  (ou seja, todo elemento está relacionado consigo mesmo. Exemplo, a relação *Tem\_o\_mesmo\_peso\_de*);
- **Anti-simetria:**  $\forall a, b \in A: (R(a, b) \wedge R(b, a)) \Rightarrow a = b$  (a relação só existe bidirecionalmente se for entre uma coisa e ela mesma. Exemplo, a relação *Número\_não\_maior\_que*); e
- **Transitividade:**  $\forall a, b, c \in A: aRb \wedge bRc \Rightarrow aRc$

Quando uma relação  $R$  satisfaz as condições acima,  $R(x, y)$  é escrita como  $x \leq y$ .

EXERCÍCIOS: Para 2 dos conjuntos numéricos **N**, **Z**, **Q**, **R**, verifique que a operação usual  $\leq$  satisfaz as condições acima. Idem para a operação  $\subseteq$  sobre conjuntos. Idem para a operação " $|$ " (divide) definida na

unidade VII (Teoria dos Números).

Dado um conjunto  $A$  e uma relação binária  $R$  sobre  $A$ :  $R \subseteq A \times A$ , dizemos que  $R$  é uma relação de **ordem parcial-estrita** sobre  $A$  se satisfaz transitividade e:

• **Irreflexividade**:  $\forall a \in A: \neg R(a,a)$  (ou seja, nenhum elemento está relacionado consigo mesmo. Exemplo, a relação  $\acute{e\_pai\_de}$ ). Se uma relação satisfaz transitividade e irreflexividade, pode ser demonstrado que também satisfaz:

• **Assimetria**:  $\forall a,b \in A: (R(a,b) \Rightarrow \neg R(b,a))$  (isto proíbe  $R(x,x)$ )

(Se uma relação  $R$  satisfaz transitividade e assimetria, então também satisfaz irreflexividade).

Quando uma relação  $R$  é uma relação de ordem parcial-estrita,  $R(x,y)$  é escrito como  $x < y$ .

Um conjunto que possui uma relação de ordem é chamado de **conjunto parcialmente ordenado**.

Exemplo: a relação "é antepassado de"

Sendo  $R$  uma relação sobre  $A$ , a **totalidade** (ou **linearidade**) está dada por:

- para ordens amplas:  $\forall x,y \in A, (x \leq y \vee y \leq x)$
- para ordens estritas:  $\forall x,y \in A, (x \neq y \Rightarrow x < y \vee y < x)$

• Dada um relação  $R$ , dizemos que  $x,y \in A$  (onde  $x \neq y$ ) **são incomparáveis**, se e somente se  $\neg R(x,y) \wedge \neg R(y,x)$ . Uma relação de ordem linear ou total não têm elementos incomparáveis.

• As ordens dos conjuntos numéricos, **N, Z, Q, R** são **lineares**.

• Dado um conjunto  $A$  com dois ou mais elementos, **P(A)**, o conjunto das partes de  $A$  não está linearmente ordenado por inclusão ( $\subseteq$ ).

• Uma relação de ordem estrita, quer seja parcial ou total, é denominada **densa** se entre dois elementos sempre existe um outro:  $\forall x,y \in A (x < y \Rightarrow \exists z \exists S (x < z < y))$

• **Inversa (" $>$ ") de uma relação de ordem estrita (" $<$ ")**: Se uma relação  $R$  é uma ordem estrita, então a relação inversa de  $R$ :

$$R^{-1} = \{(y,x): (x,y) \in R\}$$

também é uma relação de ordem estrita.

• **Inversa (" $\geq$ ") de uma relação de ordem ampla (" $\leq$ ")** pode ser definida similarmente.

• Dada uma relação de ordem ampla  $\leq$  sobre um conjunto  $A$ , um elemento  $a \in A$  é denominado **elemento mínimo** ou **primeiro elemento** se e somente se:

$$\forall b \in A (a \leq b).$$

• De maneira simétrica, é denominado **elemento máximo ou último elemento** se e somente se:

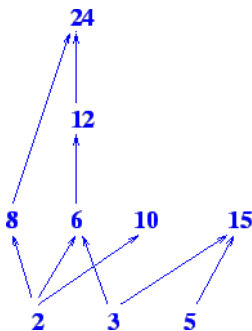
$$\forall b \in A (a \geq b).$$

• O conjunto **N** tem mínimo, mas não tem máximo. Os conjuntos **Z, Q, R** não têm nem máximo, nem mínimo. O intervalo  $[0,1] = \{x \in \mathbf{R}: 0 \leq x \leq 1\}$  tem mínimo 0 e máximo 1. Dado um conjunto  $A$  e considerando a ordem inclusão,  $\subseteq$ , o conjunto **P(A)**, das partes de  $A$ , tem mínimo  $\emptyset$  e máximo  $A$ . Se um conjunto tem mínimo, então tem um único mínimo. O mesmo vale para o máximo.

• Dada uma relação de ordem estrita  $<$  sobre um conjunto  $A$ , um elemento  $a \in A$  é denominado **minimal** (ou **ínfimo**) quando não existe outro elemento que seja menor que ele:

$$\neg \exists x \in A, x < a$$

e é denominado **maximal** (ou **supremo**) quando não existe outro elemento que seja maior que ele. No reticulado abaixo, 2, 3 e 5 são minimais, e 10, 15 e 24 são maximais.



• Um elemento  $a \in A$  é uma **cota inferior ou minorante** de um subconjunto  $B \subseteq A$  se e somente se:

$$\forall b \in B (a \leq b)$$

• Um elemento  $a \in A$  é uma **cota superior ou majorante** de um subconjunto  $B \subseteq A$  se e somente se:

$$\forall b \in B (a \geq b)$$

• Seja  $(A, \leq)$  um conjunto parcialmente ordenado.  $A$  é dito **completo** se para todo conjunto  $B \subseteq A$ ,  $B \neq \emptyset$ , se  $B$  tem majorante, então tem supremo.

• Uma relação de ordem estrita  $R$  sobre um conjunto  $A$  é denominada uma **boa ordem** se e somente se todo subconjunto não vazio de  $A$  tem primeiro elemento segundo  $R$ .

• Um conjunto com uma relação de boa ordem é denominado **bem ordenado**. Por exemplo, **N** é bem ordenado pela relação natural "<" desse conjunto, mas **Z**, **Q** e **R** não são, segundo as suas ordens naturais. *Uma boa ordem é sempre uma ordem linear.*

EXEMPLO 14: O intervalo fechado  $[0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$  possui um elemento mínimo 0 e um elemento máximo 1.

EXEMPLO 15: O intervalo semi fechado  $[0,1) = [0,1[ = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$  possui um elemento mínimo 0, todo  $x \geq 1$  é majorante do conjunto e seu supremo nos reais é o 1 que não pertence ao conjunto e, portanto, esse conjunto não tem elemento máximo.

EXEMPLO 16:  $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$ . Esse conjunto possui um supremo real  $\sqrt{2}$ , e infinitas cotas superiores racionais. No entanto, não possui supremo nos números racionais. Portanto, o conjunto dos números racionais não é completo. Por outro lado, o conjunto dos números reais é completo.

EXEMPLO 17: **P(A)**, para um conjunto qualquer A (onde  $|A| \geq 2$ ) considerando a ordem parcial ampla inclusão,  $\subseteq$ : Esse conjunto tem elemento mínimo  $\emptyset$  e elemento máximo A, segundo a ordem  $\subseteq$ . Todo  $B \subseteq \mathbf{P(A)}$  tem supremo e ínfimo em **P(A)**, segundo a ordem  $\subseteq$ .

## 1.6. Números Naturais, Inteiros, Racionais, Reais

- **Naturais**  $\mathbf{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots\}$  (cardinalidade  $\aleph_0$ ) (leia  $\aleph$  como "aleph", a primeira letra do alfabeto hebraico, cuja pronúncia é "álef")
- Naturais positivos  $\mathbf{N}^+ = \mathbf{N} - \{0\}$  (cardinalidade  $\aleph_0$ )
- **Inteiros**  $\mathbf{Z} = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots\} = \{0, -1, +1, -2, +2, -3, +3, \dots\}$  (cardinalidade  $\aleph_0$ )
- **Racionais** positivos  $\mathbf{Q}^+ = \{p/q \text{ tais que } p, q \in \mathbf{N}^+\} = \{1/1, 1/2, 2/1, 3/1, 2/2, 1/3, 1/4, 2/4, 3/2, 4/1, \dots\}$  (cardinalidade  $\aleph_0$ ) (pela diagonalização de Georg Cantor)
- Racionais negativos  $\mathbf{Q}^- = \{-x: x \in \mathbf{Q}^+\}$  (cardinalidade  $\aleph_0$ )
- Racionais:  $\mathbf{Q} = \mathbf{Z} \cup \mathbf{Q}^+ \cup \mathbf{Q}^-$  (cardinalidade  $\aleph_0$ )
- **Irracionais**  $\mathbf{I} = \{\sqrt{8}; -\sqrt{6}; 2,36521452 \dots\}$  (cardinalidade  $\aleph_1$ )
- **Reais**:  $\mathbf{R} = \mathbf{Q} \cup \mathbf{I}$  (cardinalidade:  $c$  (c. do contínuo)  $= 2^{\aleph_0} = \aleph_1$ )

### Relações entre os conjuntos de números:

$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$	( <b>N</b> está contido em <b>Z</b> , que está contido em <b>Q</b> e que está contido em <b>R</b> )
$\mathbf{I} \subset \mathbf{R}$	<b>I</b> está contido em <b>R</b>
$\mathbf{Q} \cup \mathbf{I} = \mathbf{R}$	<b>Q</b> união com <b>I</b> corresponde a <b>R</b>
$\mathbf{Q} \cap \mathbf{I} = \emptyset$	<b>Q</b> intersecção com <b>I</b> corresponde a vazio
$\mathbf{I} = \mathbf{R} - \mathbf{Q}$	<b>I</b> corresponde a <b>R</b> subtraído de <b>Q</b>
$\mathbf{N} \cap \mathbf{Z} = \mathbf{Z}^+$	inteiros positivos (inclui o 0)
$\mathbf{Z} - \mathbf{N} = \mathbf{Z}^-$	inteiros negativos (inclui o 0)
$(\mathbf{N} \cap \mathbf{Q}) \cup \mathbf{Z} = \mathbf{Z}$	
$(\mathbf{Q} \cup \mathbf{I}) \cap \mathbf{N} = \mathbf{N}$	
$\mathbf{R} \cap \mathbf{N} = \mathbf{N}$	
$\mathbf{N} \cup \mathbf{Z} = \mathbf{Z}$	

## 1.7. Conjuntos Contáveis e Não-Contáveis



As referências principais sempre são os livros-texto da disciplina, sempre busque melhor entendimento neles. Se não puder, veja em outros bons livros na Internet ou, pelo menos, em [http://pt.wikipedia.org/wiki/Conjunto\\_cont%C3%A1vel](http://pt.wikipedia.org/wiki/Conjunto_cont%C3%A1vel).

Um **conjunto contável** é um conjunto de mesma cardinalidade (número de elementos) de um subconjunto qualquer de  $\mathbf{N}$  (inclusive o próprio  $\mathbf{N}$ ). Um conjunto é dito **não-contável** quando ele não é contável. Se o conjunto for infinito (em números de termos), então, se for contável, também é chamado de **enumerável** (ou **infinito contável**), senão, de **não enumerável**.

Formalmente, um conjunto  $S$  é **contável** se existe uma *função injetora*  
 $f: S \rightarrow \mathbf{N}$

Dois conjuntos  $R, S$  são **de mesmo tamanho** se existe uma *função bijetora*  
 $f: S \leftrightarrow R$

**Teorema** (Georg Cantor): O conjunto  $\mathbf{Q}^+$  dos racionais positivos tem o mesmo tamanho (cardinalidade) do conjunto dos inteiros positivos <sup>[isto surpreendeu muitos]</sup>.

**Demonstração:** façamos uma tabela onde as colunas representam  $p$  (o numerador do racional), e as linhas representam  $q$  (o denominador). Note como todas as células em uma diagonal têm mesma soma  $p+q$  em cada célula. Agora, percorramos a tabela pelas suas diagonais em um padrão zig-zag, onde zig é a direção ↖ e zag a ↗

1/1	1/2	1/3	1/4	1/5	1/6	...
2/1	2/2	2/3	2/4	2/5	2/6	...
3/1	3/2	3/3	3/4	3/5	3/6	...
4/1	4/2	4/3	4/4	4/5	4/6	...
...	...	...	...	...	...	...

Começamos caminhando assim ↖, pela diagonal de soma  $p+q=2$ ,  
 façamos 1/1 mapear no inteiro 1

depois caminhemos assim ↗, pela diagonal de soma  $p+q=3$ ,  
 façamos 2/1 mapear no inteiro 2  
 façamos 1/2 mapear no inteiro 3

depois caminhemos assim ↖ pela diagonal de soma  $p+q=4$ ,  
 façamos 1/3 mapear no inteiro 4  
 façamos 2/2 mapear no inteiro 5  
 façamos 3/1 mapear no inteiro 6

depois caminhemos assim ↗ pela diagonal de soma  $p+q=5$

...

é assim por diante

**Teorema:** O produto cartesiano de uma quantidade finita de conjuntos contáveis é contável.

**Teorema:** Todo subconjunto de um conjunto contável é contável. Em particular, todo subconjunto infinito de um conjunto infinito contável é infinito contável.

EXEMPLO: O conjunto dos números primos é contável, mapeando o  $n$ -ésimo primo para  $n$ .

**Teorema:** A união de um sistema finito de conjuntos contáveis é contável.

**Teorema:** O conjunto de todas as sequências de tamanho finito dos números naturais é contável.

**Teorema:** O conjunto de todos os subconjuntos finitos dos números naturais é contável.

**Teorema [Básico]:** Seja  $S$  um conjunto. As seguintes declarações são equivalentes:

- 1)  $S$  é contável, ou seja, existe uma função injetora  $f: S \rightarrow \mathbf{N}$
- 2) Ou  $S$  é vazio, ou existe uma função sobrejetora  $g: \mathbf{N} \rightarrow S$
- 3) Ou  $S$  é finito ou existe uma bijeção  $h: \mathbf{N} \rightarrow S$

Muitas propriedades padrões são concluídas facilmente a partir deste teorema. Observe que  $\mathbf{N}$  no teorema pode ser substituído por qualquer conjunto infinito contável. Em particular temos o seguinte corolário.

**Corolário:** Sejam  $S$  e  $T$  conjuntos.

- 1) Se a função  $f: S \rightarrow T$  é injetora e  $T$  é contável então  $S$  é contável.
- 2) Se a função  $g: S \rightarrow T$  é sobrejetora e  $S$  é contável então  $T$  é contável.

EXEMPLO 17:  $E = \{2,4,6,\dots\}$ , o conjunto dos números pares maiores que 0, tem cardinalidade menor que a dos naturais ( $\aleph_0$ )? Prove.

Resposta:  $|E| = \aleph_0$ , porque podemos mapear  $E$  para  $\mathbf{N}$  pela função  $f(n) = 2n$ .

EXEMPLO 18: Entre dois quaisquer naturais vizinhos existem infinitos racionais (por exemplo, se os dois naturais vizinhos forem 0 e 1, temos os infinitos racionais  $1/2, 1/3, 1/4, \dots, 2/3, 2/4, 2/5, \dots, 3/4, 3/5, 3/6, \dots, 4/5, 4/6, 4/7, \dots$  (basta que o numerador seja menor que o denominador). Portanto, pode-se dizer que a cardinalidade dos racionais é maior que  $\aleph_0$ , que é a dos naturais. Certo?

Resposta: Não. Veja o teorema da diagonalização de Georg Cantor, acima.



Uma das provas mais elegantes da Matemática é a que há infinitos reais entre 0 e 1. Também deve-se a Georg Cantor. Na Internet, onde a encontrei mais fácil de ser entendida foi em

<http://www.seara.ufc.br/especiais/matematica/transfinitos/transfinitos3.htm>. Não deixe de ver.

## **Problemas sobre toda a Unidade:**

(sugeridos pelo Prof. *Rivanildo Garcia da Silva*, fico-lhe muito grato por isso)

PROBLEMA 1) Represente os conjuntos a seguir na forma de extensão.

- a)  $\{x \mid x \text{ é mês do ano formado por 9 letras}\}$
- b)  $\{x \mid x \text{ é múltiplo de 3 e de 6 maior ou igual a 12 e menor que 24}\}$
- c)  $\{x \mid x \text{ é planeta do sistema solar que começa com a letra P}\}$

PROBLEMA 2) Dados os conjuntos  $A = \{0,1,2,3\}$ ,  $B = \{1,2,3\}$  e  $C = \{2,3,4,5\}$ , determine:

- a)  $A - B$
- b)  $(A - C) \cap (B - C)$
- c)  $C - \emptyset$
- d)  $\emptyset - A$
- e)  $C_A^{(B \cap C)}$

PROBLEMA 3) Usando os símbolos  $\subset$  e  $\not\subset$ , indique a relação entre os conjuntos numéricos a seguir:

- a)  $\mathbf{N} \quad \mathbf{N}^*$
- b)  $\mathbf{Q} \quad \mathbf{R}$
- c)  $\mathbf{Z}^- \quad \mathbf{R}$
- d)  $\mathbf{N} \quad \mathbf{Z}^-$

PROBLEMA 4) Observe os números:  $-4; 0; 0,888\dots; \sqrt{2}; \frac{1}{2}; 4,86$ ; Dentre esses números determine quais são:

- a) Números naturais

- b) Números inteiros
- c) Números racionais
- d) Números irracionais
- e) Números reais

PROBLEMA 5) Identifique os números abaixo como racionais ou irracionais:

- a)  $\sqrt{4}$
- b)  $-1$
- c)  $2\sqrt{3}$
- d)  $1/2$
- e)  $\sqrt{4} + \sqrt{2}$
- f)  $\sqrt{(9 \cdot 4)}$
- g)  $(\sqrt{2})/2$

PROBLEMA 6) Determine se a relação R sobre o conjunto A dado é de equivalência.

- a)  $A = \{a; b; c; d\}$  e  $R = \{(a; a); (b; a); (b; b); (c; c); (d; d); (d; c)\}$
- b)  $A = \{1; 2; 3; 4\}$  e  $R = \{(1; 1); (1; 2); (2; 1); (2; 2); (3; 1); (3; 3); (1; 3); (4; 1); (4; 4)\}$

PROBLEMA 7) Temos que R é uma relação de equivalência, e como todo inteiro podemos expressar na forma  $x = 5q + r$  onde  $0 \leq r < 5$  existem cinco classes  $\bar{0}, \bar{1}, \bar{2}, \bar{3}$  e  $\bar{4}$ . Determine quais são estas classes:

PROBLEMA 8) Verifique se as funções são injetoras, sobrejetoras ou bijetoras:

- c)  $f: \mathbf{R} \rightarrow \mathbf{R}^+$  definida por  $f(x) = x^2$
- d)  $f: \mathbf{R} \rightarrow \mathbf{R}$  definida por  $f(x) = x + 2$
- e)  $f: \{0; 1; 2; 3; 4\} \rightarrow \mathbf{N}$  definida por  $f(x) = 2x$

PROBLEMA 9) Analise as afirmações abaixo classificando-as em (V) verdadeiras ou (F) falsas:

- a) ( ) Se uma função é bijetora, então ela também é sobrejetora.
- b) ( ) Toda função injetora é bijetora.
- c) ( ) Uma função afim do tipo  $f(x) = ax + b$ , com  $a \neq 0$ , com domínio e contradomínio nos reais é bijetora.
- d) ( ) Qualquer função quadrática é bijetora.
- e) ( ) Se qualquer reta paralela ao eixo das abscissas intercepta o gráfico de uma função em um único ponto, então a função é injetora.
- f) ( ) Se o contradomínio de uma função é igual ao conjunto imagem, então a função é sobrejetora.
- g) ( ) Se uma função é sobrejetora e injetora ao mesmo tempo, então a função é bijetora.
- h) ( ) Se uma função é bijetora, então ela é injetora.

PROBLEMA 10) Sabendo que  $f(g(x)) = 3x - 7$  e  $f(x) = x/3 - 2$ , então qual opção abaixo é verdadeira?

- a)  $g(x) = 9x - 15$
- b)  $g(x) = 9x + 15$
- c)  $g(x) = 15x - 9$
- d)  $g(x) = 15x + 9$
- e)  $g(x) = 9x - 5$

PROBLEMA 11) O domínio da função real  $f(g(x))$ , sabendo-se que  $f(x) = x^{1/2}$  e  $g(x) = (x^2 + x)(x + 2)^{-1}$ , é:

- a)  $D = \{x \in \mathbf{R} / x^{1/2} \neq -2\}$
- b)  $D = \{x \in \mathbf{R} / x \geq 0 \text{ e } x \neq -2\}$
- c)  $D = \{x \in \mathbf{R} / -2 < x \leq -1 \text{ ou } x \geq 0\}$
- d)  $D = \{x \in \mathbf{R} / -2 \leq x \leq -1 \text{ ou } x \geq 0\}$
- e)  $D = \{x \in \mathbf{R} / -2 < x < -1 \text{ ou } x \geq 0\}$

PROBLEMA 12) Considere as funções  $f(x) = 2x + 1$  e  $g(x) = x^2 - 1$ . Então as raízes da equação  $f(g(x)) = 0$  são:

- a) inteiras
- b) negativas
- c) racionais
- d) inversas
- e) opostas

PROBLEMA 13) Sejam  $f(x) = x^2 + 1$  e  $g(x) = x - 1$  duas funções reais.

Definimos a função composta de f e g como sendo  $g \circ f(x) = g(f(x))$ . Então  $g \circ f(y - 1)$  é igual a:

- a)  $y^2 - 2y + 1$
- b)  $(y - 1)^2 + 1$
- c)  $y^2 + 2y - 2$
- d)  $y^2 - 2y + 3$
- e)  $y^2 - 1$

PROBLEMA 14) Identifique se as funções abaixo são contínuas nos intervalos mencionados e justifique sua resposta.

- a)  $f(x) = 9x - 15$  em  $(0, 1)$
- b)  $g(x) = \sqrt{x - 5}$  em  $[0, 1]$
- c)  $\frac{x-5}{3}$  em  $(-3, 3)$



## **Recapitulando a unidade**

Parabéns! Você concluiu a unidade I e, se foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter relembado (ou aprendido) muitas coisas da parte básica da "Teoria dos Conjuntos" que lhe serão indispensáveis ou muito úteis em todo o resto do curso e sua vida profissional: axiomas e definições sobre conjuntos e relações entre conjuntos; operações com conjuntos; relações; funções; ordenação; conjuntos dos números naturais, e dos inteiros, e dos racionais, e dos reais; conjuntos contáveis e incontáveis. Para você treinar ainda melhor, recomendamos a Lista de Exercícios sobre Teoria dos Conjuntos, Prof. Loureiro, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE5.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE5.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE5\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE5_Solucao.pdf). E sobre Funções, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE6.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE6.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE6\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE6_Solucao.pdf). E sobre Relações, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE8.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE8.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE8\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE8_Solucao.pdf).

Na próxima unidade, a II, você será introduzido à Lógica Matemática, a investigação formal da validade de argumentações dedutivas, que são conjuntos de enunciados dos quais um é a conclusão e os demais premissas. É um assunto fascinante e profundo, muito importante para sua profissão. Você vai gostar, mesmo que só dispomos de tempo de estudo e espaço no livro para uma introdução.

## UNIDADE II

# 2. Introdução à LÓGICA MATEMÁTICA

**Lógica** é o estudo dos mecanismos de raciocínio (os que são válidos, e os que são falaciosos). **Lógica Matemática** é o estudo das inferências válidas dentro de uma linguagem *formal* (em oposição a linguagem informal). Uma *linguagem formal* é um conjunto de *símbolos* e um conjunto de *regras* para combiná-los.

**Nosso objetivo, nesta unidade,** é que, ao final dela, você domine as mais básicas noções e propriedades da parte mais fácil e básica da Lógica Matemática, que é a *Lógica Proposicional*, podendo verificar se suas fórmulas são sintaticamente bem formadas, sabendo corretamente derivar fórmulas a partir de outras, decidir se fórmulas são semanticamente verdadeiras ou falsas, se são satisfatíveis ou não, se são tautologias ou não, se inferências são válidas ou não, etc. Só assim você será capaz de, ainda nesta atual disciplina, vencer duas futuras unidades (III e IV), sobre métodos de prova de teoremas; e, no futuro, será capaz de acompanhar a disciplina *Agentes Inteligentes* e, talvez, outras disciplinas complementares optativas.

*Lembre: Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, **cada semana dedicando 4 a 8 horas para estudar este livro**, entender e reter os exemplos, resolver sozinho pelo menos 1/3 dos exercícios propostos, resumir em sua mente os principais pontos desta unidade.*

### Conteúdo desta unidade:

- 2.1. *Motivação. Lógica. Porque só Veremos a Lógica Proposicional*
- 2.2. *A Linguagem  $\mathcal{L}$  da Lógica Proposicional*
- 2.3. *Regras de Inferência. Sistemas Formais. Sistema Natural de Inferência*
- 2.4. *Sanidade, Completude, Consistência. Os Problemas da Satisfatibilidade e da Tautologia. Modelo e Teoria*



Se você quiser ver o assunto mais explicada e profundamente, não precisará de mais que os livros textos da ementa da disciplina. Outro bom livro é *Introdução à Lógica para a Ciência da Computação* (Abe, Scalzitti, Silva Filho).

Mas, para escrever esta unidade, além deles também usamos (mais como esqueleto mestre e plano geral e ordem de apresentação) partes do artigo *A First Look at Propositional Logic*, por Andreas Klappenecker, [http://faculty.cs.tamu.edu/klappi/cpsc289-f08/propositional\\_logic.pdf](http://faculty.cs.tamu.edu/klappi/cpsc289-f08/propositional_logic.pdf). Alguns exemplos e problemas devem-se aos livros-texto, outros à Professora Joseluce de Farias Cunha, em <http://buscatextual.cnpq.br/buscatextual/visualizacv.do?metodo=apresentar&id=K4776902Y4>; outros à Prof. Virgínia Maria Rodrigues, em <http://www.pucrs.br/famat/demat/facin/estrualg.htm>; outros, à Prof. Maria Helena Santos Marques [http://www.estig.ipbeja.pt/~mhsm/mat\\_dis\\_informacoes.htm](http://www.estig.ipbeja.pt/~mhsm/mat_dis_informacoes.htm); outros, ao aluno <http://www.danielclemente.com/logica/dn.en.html>; e outras fontes que serão indicadas.

## 2.1. Motivação. Lógica. Porque só Veremos a Lógica Proposicional

- **Lógica** é o estudo dos mecanismos de raciocínio (os que são válidos, e os que são falaciosos).
- **Lógica Matemática** é o estudo das inferências válidas dentro de uma linguagem *formal* (em oposição a linguagem informal), onde uma *linguagem formal* é um conjunto de *símbolos* e um conjunto de *regras* para combiná-los. A Lógica Matemática pode ser dividida em lógicas clássicas e não clássicas.
- **Lógicas Matemáticas Clássicas** são aquelas que compartilham das seguintes características básicas:

- *Lei do terceiro excluído* (cada proposição é verdadeira ou é falsa, não havendo nenhuma outra possibilidade entre ou além dessas duas) e *eliminação da dupla negação* (uma negação de uma negação equivale a uma afirmação);
- *Lei da não contradição* (declarações contraditórias não podem ambas ser verdadeiras no mesmo sentido e ao mesmo tempo), e o *princípio da explosão* (se aceitássemos uma contradição como uma verdade, tudo poderia ser deduzido);
- *Monotonicidade de vinculação* (uma proposição que teve um valor Verdade ou Falso a ela atribuído sempre o continuará a ter, e podemos livremente adicionar outras proposições como suposições suas companheiras, desde que não a contrariem) e *idempotência de vinculação* (de muitas maneiras deduzir um mesmo valor Verdade ou Falso para uma declaração não tem nenhum valor a mais que deduzi-lo uma só vez);
- *Comutatividade da conjunção* (a proposição "A e B" é o mesmo que a proposição "B e A");
- *Dualidade de De Morgan*: cada conectivo lógico é dual de outro (detalhes mais adiante).

Há muitas razões para você estudar Lógica Matemática (clássica), pois ela é a indispensável base para todas as provas de teoremas da Matemática, para você provar que um programa é correto, para você conceber e projetar circuitos lógicos, e muitas e importantes outras coisas. O estudo da Lógica Matemática é tão importante e fascinante que poderia ser uma disciplina em si. Seja como for, no curso de Licenciatura em Computação ela já é cerca de um quarto de uma das disciplinas complementares optativas do curso, a disciplina *Agentes Inteligentes*. Pela nossa exiguidade de tempo de estudo e de espaço nesta disciplina e livro, só poderemos estudar a primeira e mais fácil parte da Lógica Matemática, isto é, a Lógica Proposicional, que não tem variáveis. Em Agentes Inteligentes você procederá para a Lógica de 1ª Ordem. Dominar a Lógica Proposicional agora será muito necessário para você fazer o resto desta disciplina, e do curso, e depois, para certos aspectos de sua vida profissional.

- Uma **proposição** (ou **sentença**) é uma declaração que é verdadeira ou é falsa. Dois exemplos: João é honesto; o sol é quadrado.
- **Lógica Proposicional** (ou **sentencial**) estuda como proposições verdadeiras podem ser combinadas por meio de conectivos para produzir outras afirmações verdadeiras. Um exemplo: Se supusermos que ambas as proposições 'o cão é branco' e 'o cão é manso' são verdadeiras, então podemos combiná-las na afirmação 'o cão é branco e o cão é manso' e podemos inferir que ela é verdadeira. No entanto, se constatarmos que a segunda afirmativa é falsa, então podemos concluir que a afirmativa combinada também é falsa. Lógica Proposicional nos permite *formalizar* tais declarações e raciocínios, com a vantagem colateral de que ficarão mais concisos [e frequentemente removerão a ambiguidade da linguagem natural e as fraquezas do raciocínio natural]: Podemos chamar de A a primeira proposição ('o cão é branco') e de B a segunda ('o cão é manso'), então a declaração combinada "A e B" se expressa na Lógica Proposicional na forma  $A \wedge B$ , onde  $\wedge$  é um conectivo que formaliza a palavra 'e'.

## 2.2. A Linguagem £ da Lógica Proposicional

A Lógica Proposicional tem uma linguagem artificial que chamaremos de **£** ("£" é uma letra do alfabeto do latim antigo, usada como símbolo da unidade monetária romana, a libra. Os exigentes pronunciam "£" como "libra", os não exigentes como nossa letra l "éle"). Como toda linguagem, £ tem um *sintaxe* e uma *semântica*. A *sintaxe* de uma linguagem preocupa-se com sua *forma*: o vocabulário inicial e as regras de formação de "expressões" bem- formadas a partir dele. A *semântica* está preocupada com o *significado* destas expressões bem- formadas.

### 2.2.1. A Sintaxe de $\mathcal{L}$

- O **vocabulário** (inicial) de  $\mathcal{L}$  é constituído dos seguintes símbolos:

<b>letras proposicionais</b> (ou <b>símbolos de proposições</b> ) (em número infinito mas contável):	$a, a_0, a_1, \dots, b, b_0, b_1, \dots, z, z_0, z_1, \dots$
<b>conectivos lógicos:</b>	$\neg$ // ler “ <b>não</b> ”), $\wedge$ // ler “ <b>e</b> ”), $\oplus$ // ler “ <b>ou- excludente</b> ”), $\vee$ // ler “ <b>ou</b> ”), $\rightarrow$ // ler “ <b>implica</b> ”, ou “ <b>se</b> ”, ou “ <b>se- então</b> ”, ou “ <b>implicação material</b> ”, ou “ <b>condicional</b> ”), $\leftrightarrow$ // ler “ <b>se- e- somente- se</b> ”, ou “ <b>equivale- a,</b> ” ou “ <b>implica- nos- dois- sentidos</b> ”, ou “ <b>equivalência material</b> ”, ou “ <b>bicondicional</b> ”) <p>Há quem acrescente outros conectivos: <b>nor</b> (<math>\bar{\vee}</math>) é a negação do <math>\vee</math>; <b>nand</b> (<math>\bar{\wedge}</math>) é a negação do <math>\wedge</math>; <b>a<math>\leftarrow</math>b</b> (“<b>a é implicado por b</b>”) é definido como equivalente a <b>b<math>\rightarrow</math>a</b>; etc. Mas podemos viver sem eles, por isso vamos deixá-los de fora. Também poderíamos viver sem o <math>\oplus</math>, o <math>\rightarrow</math> e o <math>\leftrightarrow</math>, mas os conservamos pela sua conveniência.</p>
<b>sinais de pontuação:</b>	( // ler “ <b>abre- parênteses</b> ” ) // ler “ <b>fecha-parênteses</b> ”

- Uma **fórmula** de  $\mathcal{L}$  é toda sequência finita contendo símbolos somente do seu vocabulário.

<b>EXEMPLO 1: São fórmulas:</b> $p_1$ $\wedge p_{20} \leftrightarrow \dots$ $(p_1 \wedge p_2 \vee \neg p_{67})$	<b>EXEMPLO 2: não são fórmulas:</b> $\#_1$ // porque não previmos $\#_1$ no vocabulário $\sim p_2$ // porque $\sim$ não pertence ao vocabulário de $\mathcal{L}$ $q_1 \& q_2$ // porque $\&$ não pertence ao vocabulário de $\mathcal{L}$
--	--

- Uma **fórmula bem formada (fbf)** de  $\mathcal{L}$  é toda fórmula que satisfaz as seguintes condições:

$V, F$  são fbf's

Toda letra proposicional é uma fórmula que também é uma fbf, isto é,  $p_1, p_2, p_3, p_4, \dots$  são fbf's.

Se  $\alpha$  for uma fbf, então  $\neg \alpha$  será uma fbf.

//  $\alpha$  é uma metavariable, isto é, não pertence à linguagem  $\mathcal{L}$ , é apenas um nome genérico, a ser instanciado para ser qualquer nome realmente pertencente a  $\mathcal{L}$ .

Se  $\alpha$  e  $\beta$  forem fbf's, então  $\alpha \wedge \beta$  será uma fbf.

Se  $\alpha$  e  $\beta$  forem fbf's, então  $\alpha \oplus \beta$  será uma fbf.

Se  $\alpha$  e  $\beta$  forem fbf's, então  $\alpha \vee \beta$  será uma fbf.

Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \rightarrow \beta)$  será uma fbf.

Se  $\alpha$  e  $\beta$  forem fbf's, então  $\alpha \leftrightarrow \beta$  será uma fbf.

Se  $\alpha$  for uma fbf, então  $(\alpha)$  será uma fbf.

Nada mais é fbf.

Ambiguidades (quando as regras acima lhe deixarem em dúvida sobre que operação fazer primeiro, porque mais de uma delas pode ser aplicada) são resolvidas através da **ordem de precedência para os operadores** (que, de maior para menor, é  $\neg \wedge \oplus \vee \rightarrow \leftrightarrow$ ) ou através de parênteses. Por exemplo,

$$\neg P \vee Q \wedge R \Rightarrow S$$

é equivalente a  $((\neg P) \vee (Q \wedge R)) \Rightarrow S$

// primeiro fizemos todos os  $\neg$  de 1º nível

da fbf, depois todos os  $\wedge$ , depois todos os  $\vee$ , finalmente todos os  $\Rightarrow$

EXEMPLO 3: São fbf's:

$p_{123}$ ,  $(\neg p_1)$ ,  $(p_1 \vee p_2)$ ,  $(p_2 \vee p_1)$ ,  $(p_5 \rightarrow p_6)$ ,  $((p_1 \vee p_2) \leftrightarrow (p_3 \rightarrow p_4))$

EXEMPLO 4: São fórmulas não bem- formadas:

$p_1(8$  // falta um fecha parênteses, e 8 não é uma letra proposicional  
 $\neg p_1$  // o problema é o espaço em branco entre  $\neg$  e  $p_1$   
 $p_1 \wedge p_3$  // o problema são os espaços em branco ao redor de  $\wedge$   
 $((\neg p_1) \vee p_1) \rightarrow p_3$  // os abre-parênteses e fecha-parênteses não casam  
 $((\neg p_1) \vee) \rightarrow p_3$  // falta o 2º argumento do  $\vee$

Somente quando você chegar à disciplina Teoria da Computação estudará o formalismo chamado de Forma de Backus- Naur (em inglês, BNF, abreviação de Backus Naur Form), usado para especificar a parte livre-de- contexto das linguagens de programação. Mas como ele é muito intuitivo, veja em BNF a mesma definição de fbf que foi escrita pouco acima:

```
<fbf> ::=  $\neg$ <fbf>
        | <fbf>  $\wedge$  <fbf>
        | <fbf>  $\oplus$  <fbf>
        | <fbf>  $\vee$  <fbf>
        | <fbf>  $\rightarrow$  <fbf>
        | <fbf>  $\leftrightarrow$  <fbf>
        | (<fbf>)
        | <SímboloDeProposição> | V | F
```

<SímboloDeProposição> é qualquer outro símbolo terminal: qualquer letra minúscula, possivelmente com subscrito que seja um inteiro sem sinal. Isto é, um elemento do conjunto  $S = \{a, a_0, a_1, \dots, b, b_0, b_1, \dots, z, z_0, z_1, \dots\}$ .

// A precedência de operadores  $\neg \wedge \oplus \vee \rightarrow \leftrightarrow$  será usada na escolha das regras BNF que puderem ser aplicadas a um mesmo estágio da avaliação da árvore sintática (ou de derivação ou de parsing). A associatividade, para cada conectivo binário, é escolhida ser da esquerda para a direita. Na disciplina Teoria da Computação (e na complementar optativa Introdução aos Compiladores) você verá os conceitos de árvore de derivação e entenderá melhor isto, bem como a detecção automatizada se uma fórmula é bem formada ou não.

É preferível uma BNF que seja inambígua sem recorrer a definições extra gramática da precedência e associatividade (esquerda para direita) de operadores:

```
<FBF> ::= <ExprSe> | <FBF>  $\leftrightarrow$  <ExprImplica>
<ExprImplica> ::= <ExprOu> | <ExprImplica>  $\rightarrow$  <ExprOu>
<ExprOu> ::= <ExprXor> | <ExprOu>  $\vee$  <ExprXor>
<ExprXor> ::= <ExprE> | <ExprXor>  $\oplus$  <ExprE>
<ExprE> ::= <FormAtomica> | <ExprE>  $\wedge$  <FormAtomica>
<FormAtomica> ::= V | F | < SímboloDeProposição > |  $\neg$ <FormAtomica> | (<FBF>)
< SímboloDeProposição > ::= qualquer outro símbolo terminal: qualquer letra minúscula,
possivelmente com subscrito que seja um inteiro sem sinal. Isto é, um elemento do conjunto  $S = \{a, a_0, a_1, \dots, b, b_0, b_1, \dots, z, z_0, z_1, \dots\}$ 
```

EXEMPLO 5 (PUCRS, Virgínia Maria Rodrigues, em <http://www.pucrs.br/famat/demat/facin/estrualg.htm>):

Sejam as proposições: p: Gosto de viajar e q: Visitei o Chile. Escreva as sentenças verbais que estão representadas pelas proposições abaixo:

(a)  $p \leftrightarrow q$  (b)  $\neg q \rightarrow \neg p$  (c)  $(p \wedge \neg q) \rightarrow \neg p$  (d)  $q \wedge \neg p$   
(e)  $\neg(p \wedge q)$  (f)  $q \rightarrow p$  (g)  $\neg p \vee \neg q$  (h)  $(p \vee \neg q) \wedge (\neg p \rightarrow q)$

RESPOSTA:

- (a) Gosto de viajar se e somente visitei o Chile.  
(b) Se não visitei o Chile, então não gosto de viajar.  
(c) Se gosto de viajar e não visitei o Chile, então não gosto de viajar.  
(d) Visitei o Chile e não gosto de viajar.  
(e) Não é verdade que: gosto de viajar e visitei o Chile.  
(f) Se visitei o Chile, então gosto de viajar.  
(g) Não gosto de viajar ou não visitei o Chile.

(h) Se gosto de viajar ou não visitei o Chile; e, se não gosto de viajar, então visitei o Chile.

EXEMPLO 6 (PUCRS, Prof. Virgínia Maria Rodrigues): Descreva as sentenças abaixo em termos de proposições simples e operadores lógicos. Por exemplo, se a sentença for "Se  $1 > 2$  então qualquer coisa é possível", faça o símbolo  $p$  valer por " $1 > 2$ " e o símbolo  $q$  valer por "qualquer coisa é possível", então a frase (a resposta) será:  $p \rightarrow q$ .

(a) Se elefantes podem subir em árvores, então 3 é um número irracional.

(b) É proibido fumar cigarro ou charuto.

(c) Não é verdade que  $\Pi > 0$  se e somente se  $\Pi > 1$ . // Pela ordem de prioridades dos conectivos, isso deve ser pensado como "(Não é verdade que  $\Pi > 0$ ) se e somente se  $\Pi > 1$ ", não como "Não é verdade que ( $\Pi > 0$  se e somente se  $\Pi > 1$ )".

(d) Se as laranjas são amarelas, então os morangos são vermelhos.

(e) É falso que se Montreal é a capital do Canadá, então a próxima copa será realizada no Brasil.

(f) Se é falso que Montreal é a capital do Canadá, então a próxima copa (2010) será realizada no Brasil.

RESPOSTA:

(a)  $p$ : elefantes podem subir em árvores

$q$ : 3 é um número irracional

frase:  $p \rightarrow q$

(b)  $p$ : fumar cigarro

$q$ : fumar charuto

frase:  $\neg(p \vee q)$

(c)  $p$ :  $\Pi > 0$

$q$ :  $\Pi > 1$

frase:  $\neg p \leftrightarrow q$

(d)  $p$ : as laranjas são amarelas

$q$ : os morangos são vermelhos

frase:  $p \rightarrow q$

(e)  $p$ : Montreal é a capital do Canadá

$q$ : a próxima copa será realizada no Brasil frase:  $\neg(p \rightarrow q)$

(f)  $p$ : Montreal é a capital do Canadá

$q$ : a próxima copa será realizada no Brasil frase:  $\neg p \rightarrow q$

## 2.2.2. A Semântica de $\mathcal{L}$

• A semântica da Lógica Proposicional depende de uma **interpretação** (ou **valoração**)  $I$ , que é uma função que atribui a cada letra proposicional um dos dois valores de verdade: o Verdadeiro (V) ou o Falso (F).

• Os **conectivos** (seus nomes e símbolos) básicos da Lógica Proposicional são dados na 1ª linha da seguinte tabela: **não** ( $\neg$ ), **e** ( $\wedge$ ), **xor** ( $\oplus$ ), **ou** ( $\vee$ ), **implica** ( $\rightarrow$ ), **ssse** ( $\leftrightarrow$ ). Depois explicaremos seus significados. Por enquanto, procure memorizar seus símbolos e nomes.

		Conectivo:					
		não $\neg$	e $\wedge$	xor $\oplus$	ou $\vee$	implica $\rightarrow$	ssse $\leftrightarrow$
a	b	$\neg b$	$a \wedge b$	$a \oplus b$	$a \vee b$	$a \rightarrow b$	$a \leftrightarrow b$
F	F	V	F	F	F	V	V
F	V	F	F	V	V	V	F
V	F	V	F	V	V	F	F
V	V	F	V	F	V	V	V

• Letras proposicionais são chamadas de **fórmulas atômicas** (atômicas no sentido de indecomponíveis em partes menores). As fbf's constituídas pela combinação de fórmulas atômicas com elementos de  $\{\neg, \wedge, \oplus, \vee, \rightarrow, \leftrightarrow, (, )\}$  são chamadas de **fórmulas moleculares** (molecular no sentido de decomponível em partes menores). Por exemplo,  $(\neg p_1 \vee (p_2 \wedge (p_3 \rightarrow p_4))) \leftrightarrow p_5$  é uma fbf e fórmula molecular.

O valor semântico (isto é, o valor de verdade) de uma fórmula molecular depende do valor semântico (valor de verdade) das fórmulas atômicas e do significado semântico dos conectivos lógicos que as combinam, que está bem definido na tabela acima, mas você tem que tomar alguns 5 minutos para entender e memorizar como *cada* conectivo funciona. Faça isto AGORA. Pronto? Não tente enganar e roubar a si mesmo, pulando esta etapa, senão você se prejudicará muitíssimo, vai ter dificuldades em toda esta unidade e durante toda

sua vida. Novamente, tome 5 minutos para entender e memorizar como *cada* conectivo funciona, isto é, o valor V ou F que ele atribui a duas proposições  $x, y$  que interconecte, quando os de  $x$  e  $y$  são F F, F V, V F, e V V. Agora, tome mais 5 minutos e rascunhe em papel uma curto resumo de como você entendeu que cada conectivo funciona. Por exemplo, comece com algo assim " $x \oplus y$  é V ssse  $x$  e  $y$  tiverem valores verdade opostos". Vamos, rascunhe seu entendimento de todos os conectivos. 5 minutos. Pronto? Agora, novamente confira suas definições contra a tabela acima. Tem certeza de que entendeu e descreveu tudo corretamente? Finalmente, confira suas definições contra as nossas definições, abaixo, do significado semântico de cada conectivo lógico.

Nossa definição (em prosa, mas equivalente à tabela) do significado semântico de cada conectivo lógico:

- **"Não"**: Se  $\alpha$  for uma fbf, então  $(\neg\alpha)$  será V somente quando  $\alpha$  for falso, e  $(\neg\alpha)$  será F somente quando  $\alpha$  for V. Ou seja, a negação "troca" o valor de verdade.
- **"E"**: Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \wedge \beta)$  será V somente quando ambos  $\alpha$  e  $\beta$  forem V, e  $(\alpha \wedge \beta)$  será F somente quando ou  $\alpha$  ou  $\beta$  (ou ambos) for(em) F.
- **"Ou- excludente"**: Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \oplus \beta)$  será V quando  $\alpha$  e  $\beta$  tiverem valores verdade diferentes, e será F quando tiverem um mesmo valor verdade.
- **"Ou"**: Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \vee \beta)$  será V somente quando  $\alpha$  ou  $\beta$  (ou ambos) for(em) V, e  $(\alpha \vee \beta)$  será F somente quando ambos  $\alpha$  e  $\beta$  forem F.
- **"Implica"**: Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \rightarrow \beta)$  será V somente quando  $\alpha$  for F ou quando  $\beta$  for V, e  $(\alpha \rightarrow \beta)$  será F somente quando  $\alpha$  for V e  $\beta$  for F.
- **"Se e somente se"**: Se  $\alpha$  e  $\beta$  forem fbf's, então  $(\alpha \leftrightarrow \beta)$  será V somente quando  $\alpha$  e  $\beta$  tiverem o mesmo valor de verdade, e  $(\alpha \leftrightarrow \beta)$  será F, em caso contrário.

EXEMPLO 7 (PUCRS, Prof. Virgínia Maria Rodrigues): Determine o valor lógico das proposições enunciadas no exercício anterior (número 6). Justifique (por exemplo: *Se  $1 > 2$  então qualquer coisa é possível.*

Verdadeira, pois é falso que  $1 > 2$ ):

RESPOSTA:

- (a) Verdadeira, pois  $p$  é falsa uma vez que elefantes não podem subir em árvores.  
 (b) Assumindo-se que esta proibição esteja sendo feita em algum lugar, teremos uma proposição verdadeira, pois será proibido fumar cigarro ( $p$  será verdadeira) e será proibido fumar charuto ( $q$  será verdadeira).  
 (c) Falsa, pois  $\neg p$  é falsa e  $q$  é verdadeira.  
 (d) Verdadeira, pois  $p$  é falsa.  
 (e) Falsa, pois a proposição  $p \rightarrow q$  é verdadeira visto que  $p$  é falsa.  
 (f) Falsa, pois Montreal não é a capital do Canadá e a próxima copa (2010) não será realizada no Brasil, ou seja,  $\neg p$  é verdadeira e  $q$  é falsa.

EXEMPLO 8 (PUCRS, Prof. Virgínia Maria Rodrigues): Considerando  $p$  e  $q$  proposições verdadeiras, e  $r$  e  $s$  proposições falsas, determine o valor lógico das proposições abaixo:

- (a)  $((\neg r \wedge \neg s) \vee (p \rightarrow q)) \leftrightarrow (r \vee \neg q)$   
 (b)  $((p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)) \rightarrow (r \vee s)$

RESPOSTA (Achamos que já dá para você entender, mas, se quiser, veja a definição de  $\leftrightarrow$  um pouco abaixo.

Se preferir, faça a tabela verdade, mas dará mais trabalho):

- (a)  $((\neg F \wedge \neg F) \vee (V \rightarrow V)) \leftrightarrow (F \vee \neg V) \Leftrightarrow ((V \wedge V) \vee (V \rightarrow V)) \leftrightarrow (F \vee F) \Leftrightarrow (V \vee V) \leftrightarrow (F) \Leftrightarrow F$   
 (b)  $((V \wedge V) \vee (V \wedge \neg V) \vee (\neg V \wedge V) \vee (\neg V \wedge \neg V)) \rightarrow (F \vee F) \Leftrightarrow ((V) \vee (V \wedge F) \vee (F \wedge V) \vee (\neg(V \wedge F))) \rightarrow (F) \Leftrightarrow (V \vee (F) \vee (F) \vee (\neg(F))) \rightarrow F \Leftrightarrow (V \vee F \vee F \vee (\neg F)) \rightarrow F \Leftrightarrow (V \vee F \vee F \vee V) \rightarrow F \Leftrightarrow \dots$   
 $\Leftrightarrow V \rightarrow F \Leftrightarrow F$

**Propriedades:** Todas as propriedades seguintes facilmente se demonstram, em  $\mathcal{L}$ , recorrendo à tabela de verdade, acima.

• **Propriedades da conjunção ( $\wedge$ ) e da disjunção ( $\vee$ ):**

Propriedades	Conjunção ( $\wedge$ )	Disjunção ( $\vee$ )
Comutativa	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
Associativa	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$	$(p \vee q) \vee r = p \vee (q \vee r)$

Existência de elemento neutro	$V \wedge p = p \wedge V = p$	$F \vee p = p \vee F = p$
Existência de elemento absorvente	$F \wedge p = p \wedge F = F$	$V \vee p = p \vee V = V$
Idempotência	$p \wedge p = p$	$p \vee p = p$

### • Propriedades de combinação da conjunção e da disjunção

A conjunção é distributiva em relação à disjunção:

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

$$(q \vee r) \wedge p = (q \wedge p) \vee (r \wedge p)$$

A disjunção ( $\vee$ ) é distributiva em relação à conjunção ( $\wedge$ ):

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$

$$(q \wedge r) \vee p = (q \vee p) \wedge (r \vee p)$$

### • Propriedades da negação

Dupla negação

$$\neg \neg p = p$$

Leis de De Morgan

$$\neg(p \wedge q) = \neg p \vee \neg q$$

$$\neg(p \vee q) = \neg p \wedge \neg q$$

### • Propriedades da implicação (ou se, ou implicação material, ou condicional)

Relação da implicação com a disjunção

$$p \rightarrow q = \neg p \vee q$$

Esta mesma propriedade permite exprimir uma disjunção numa implicação

$$p \vee q = \neg p \rightarrow q$$

Negação da implicação

$$\neg(p \rightarrow q) = p \wedge \neg q$$

Lei da conversão

$$p \rightarrow q = \neg q \rightarrow \neg p$$

Transitividade

$$(p \rightarrow q \wedge q \rightarrow r) \rightarrow (p \rightarrow r)$$

### • Propriedades do se- e- somente- se (ou equivalência material, ou bicondicional)

A equivalência como conjunção de implicações

$$p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p)$$

Negação da equivalência

$$\neg(p \leftrightarrow q) = (p \wedge \neg q) \vee (q \wedge \neg p) = p \vee q$$

## 2.3. Regras de Inferência sobre £. Sistemas Formais. Sistema Natural de Inferência

• Seja  $f_1$  uma fbf. Se existe pelo menos uma atribuição de valores V, F a seus símbolos de proposição de tal forma que  $f_1$  resulte no valor V  $\{*\}$ , então  $f_1$  é dita ser **satisfatível**. Se todas as valorações resultam em  $f_1$  valer F  $\{*\}$ ,  $f_1$  é dita ser **insatisfatível** (ou **não satisfatível, ou contraditória**). Se todas  $\{*\}$  as valorações resultam em  $f_1$  valer V,  $f_1$  é dita ser uma **tautologia**. Se existe pelo menos alguma valoração que resulte em  $f_1$  valer V  $\{*\}$ , e existe pelo menos outra valoração que resulte em  $f_1$  valer F  $\{*\}$  então  $f_1$  é dita ser **contingente**. A fbf  $f_1$  é tautologia ssse  $f_1$  não é contraditória.  $\{*\}$  isto pode ser visto em uma tabela verdade, embora seja pesado construí-la.

EXEMPLO 9: Faça duas tabela verdade e verifique que  $p \vee \neg p$  é uma tautologia e  $p \wedge \neg p$  é uma contradição:

RESPOSTA: Basta notar que a coluna  $p \vee \neg p$  só tem V e a coluna  $p \wedge \neg p$  só tem F:

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
V	F	V	F
F	V	V	F



EXEMPLO 10: Verifique que $((a \rightarrow b) \leftrightarrow (\neg a \vee b))$ é uma tautologia.	a	b	$(a \rightarrow b)$	$(\neg a \vee b)$	$((a \rightarrow b) \leftrightarrow (\neg a \vee b))$
RESPOSTA: Há 2 símbolos proposicionais, portanto $2^2 = 4$ casos. Na tabela verdade, a coluna da fbf só tem V.	F	F	V	V	V
	F	V	V	V	V
	V	F	F	F	V
	V	V	V	V	V

EXEMPLO 11:  $((a \oplus b) \rightarrow \neg(a \vee b))$  é satisfatível?

RESPOSTA: Sim. Se escolhermos uma valoração (ou interpretação)  $v$  tal que  $a = F$  e  $b = F$ , então  $a \oplus b = F$ , daí, como  $F$  implica qualquer coisa,  $((a \oplus b) \rightarrow \neg(a \vee b)) = V$ .

EXEMPLO 12: A proposição  $(a \wedge \neg a)$  é insatisfatível?

RESPOSTA: Sim. Se escolhermos uma valoração  $v$  tal que  $a = V$ , então  $\neg a = F$ , então  $(a \wedge \neg a) = F$ . A única outra interpretação possível é  $a = F$ , o que também implica  $(a \wedge \neg a) = F$ . Portanto, a proposição  $(a \wedge \neg a)$  é insatisfatível.

- Dadas duas fbf's (em oposição a proposições)  $f_1, f_2$ , então  $f_1 \Rightarrow f_2$  (ler "a fbf  $f_1$  **logicamente implica** a fbf  $f_2$ ") se e somente se  $f_1 \Rightarrow f_2$  é uma tautologia;
- Dadas duas fbf's (em oposição a proposições)  $f_1, f_2$ , então  $f_1 \Leftrightarrow f_2$  (ler "a fbf  $f_1$  **logicamente equivale** a fbf  $f_2$ ") se e somente se  $f_1 \Leftrightarrow f_2$  é uma tautologia.

EXEMPLO 13:  $p \wedge (p \rightarrow q)$  logicamente implica  $p \wedge q$ ? Isto é, podemos escrever  $p \wedge (p \rightarrow q) \Rightarrow p \wedge q$ ?

RESPOSTA: Sim, pois  $p \wedge (p \rightarrow q) \rightarrow (p \wedge q)$  é uma tautologia:

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge q)$	$p \wedge (p \rightarrow q) \rightarrow (p \wedge q)$
F	F	V	F	F	V
F	V	V	F	F	V
V	F	F	F	F	V
V	V	V	V	V	V

EXEMPLO 14:  $p \wedge (p \rightarrow q)$  logicamente equivale a  $p \wedge q$ ? Isto é, podemos escrever  $p \wedge (p \rightarrow q) \Leftrightarrow p \wedge q$ ?

RESPOSTA: Sim, pois  $p \wedge (p \rightarrow q) \leftrightarrow (p \wedge q)$  é uma tautologia:

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge q)$	$p \wedge (p \rightarrow q) \leftrightarrow (p \wedge q)$
F	F	V	F	F	V
F	V	V	F	F	V
V	F	F	F	F	V
V	V	V	V	V	V



Note: Sejam  $f_1$  e  $f_2$  fbf's. Então  $f_1 \Rightarrow f_2$ , bem como  $f_1 \Leftrightarrow f_2$ , não são fbf's (pois os símbolos  $\Rightarrow$  e  $\Leftrightarrow$  sequer pertencem ao conjunto dos conectivos de  $\mathcal{L}$ ). De fato,  $f_1 \Rightarrow f_2$ , bem como  $f_1 \Leftrightarrow f_2$ , podem ser consideradas como proposições (tais como "João é alto"), mas isso não é muito útil. Mais útil é, bastante é pensar de  $\Rightarrow$  como "a fbf ... implica logicamente à fbf ..." e de  $\Leftrightarrow$  como "a fbf ... é logicamente equivalente à fbf ...".

Sejam  $f_1, f_2, \dots, f_n$  fbf's envolvendo  $m$  símbolos proposicionais. Para mostrar que uma certa combinação dessas fbf's (através de conectivos lógicos) logicamente implica uma outra fbf,  $g$ , era preciso fazermos uma tabela verdade, o que somente era manejável se o número de símbolos proposicionais,  $m$ , fosse na ordem de 2 ou 3, talvez 4. Isto motivou a busca pelo desenvolvimento de aparatos que permitissem o raciocínio ser feito a nível puramente sintático, sem necessidade de nenhuma interpretação (atribuição de V,F aos símbolos proposicionais) ter que ser considerada. Estes aparatos foram chamados de *sistema de dedução (formal)*, de *teoria de prova*, de *sistema de inferência*, ou de *cálculo lógico*. Tais

sistemas podem ser classificados em sistemas de dedução e sistemas de refutação. Aqui somente falaremos (e muito pouco) sobre os primeiros.

Um **sistema de dedução** (ou **sistema de regras de inferência**, ou **sistema de inferências**) nos permite, através apenas de operações *sintáticas*, tirar conclusões a partir de um conjunto de fbf's. Através de manipulações meramente sintáticas, a partir das fbf's originais vamos gerando outras que lhe são consequências lógicas, até que cheguemos à fbf desejada, todo o processo sendo mecânico e podendo ser automatizado. Um sistema de dedução compreende um conjunto finito de **regras de inferência** (que são tautologias) e um conjunto de fbf's chamado de **axiomas lógicos**. (Acima da Lógica Proposicional, como você verá em disciplinas tais como Teoria da Computação e como Lógica, este último conjunto é frequentemente infinito, mas isto é contornado através do uso de *templates* (que são *esquemas axiomáticos* que fornecem uma fbf que serve de modelo ou padrão para infinitas fbf's.)).

• Há vários sistemas de dedução possíveis para a Lógica Proposicional, mas o mais usado é este que se segue, conhecido como **Sistema Natural de Regras de Inferência** (deve nome e popularidade ao fato de refletir o raciocínio naturalmente usado nas demonstrações informais em Matemática ou em qualquer outro argumento lógico informal):

<i>Axiomas:</i>	$p \vee \neg p, p \rightarrow p$	
<i>conjunção:</i>	$p, q \Rightarrow p \wedge q$ $p \wedge q \Rightarrow p, q$	Intro $\wedge$ Elim $\wedge$
<i>disjunção:</i>	$p \Rightarrow p \vee q$ ou $q \Rightarrow p \vee q$ $p \vee q, \neg p \Rightarrow q$ ou $p \vee q, \neg q \Rightarrow p$ $p \vee q, p \rightarrow r, q \rightarrow r \Rightarrow r$	Intro $\vee$ Elim $\vee$ com 2 argumentos Elim $\vee$ com 3 argumentos
<i>implicação:</i>	$q \Rightarrow p \rightarrow q$ $p \rightarrow q, p \Rightarrow q$	Intro $\rightarrow$ Elim $\rightarrow$ ( <i>modus ponens</i> )
<i>equivalência:</i>	$p \rightarrow q, q \rightarrow p \Rightarrow p \leftrightarrow q$ $p \leftrightarrow q \Rightarrow p \rightarrow q, q \rightarrow p$	Intro $\leftrightarrow$ Elim $\leftrightarrow$

Outras regras e teoremas, úteis, derivadas do sistema acima (tente prová-los, será um bom exercício):

<i>introdução de negação:</i>	$p \Rightarrow \neg \neg p$ $p \rightarrow q, \neg q \Rightarrow \neg p$	Intro $\neg$ com 1 argumento Intro $\neg$ com 3 argumentos
<i>eliminação de negação:</i>	$\neg \neg p \Rightarrow p$	Elim $\neg$
<i>negação de disjunção:</i>	$\neg(p \vee q) \Rightarrow \neg p \wedge \neg q$	Neg $\vee$
<i>negação de conjunção:</i>	$\neg(p \wedge q) \Rightarrow \neg p \vee \neg q$	Neg $\wedge$
<i>negação de implicação:</i>	$\neg(p \rightarrow q) \Rightarrow p \wedge \neg q$	Neg $\rightarrow$
<i>transitividade de implicação:</i>	$p \rightarrow q, q \rightarrow r \Rightarrow p \rightarrow r$	Trnstv $\rightarrow$
<i>transposição:</i>	$p \rightarrow q \Rightarrow \neg q \rightarrow \neg p$	Trnspsc $\rightarrow$
<i>modus tollens/contrapositivo</i>	$p \rightarrow q, \neg q \Rightarrow \neg p$	ContraP

• Um outro [o segundo] sistema de regras de inferência pode ser:

Regras de Inferência	Tautologia	Nome
$\underline{p}$ $\therefore p \vee q$	$p \rightarrow (p \vee q)$	Adição ou Introdução (como disjunção)
$\underline{p \wedge q}$ $\therefore p$	$(p \wedge q) \rightarrow p$	Simplificação ou Eliminação (em disjunção)
$\underline{p}$ $\underline{q}$ $\therefore p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunção
$\underline{p}$ $\underline{p \rightarrow q}$ $\therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\underline{\neg q}$ $\underline{p \rightarrow q}$ $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$\underline{p \rightarrow q}$ $\underline{q \rightarrow r}$ $\therefore p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Silogismo hipotético
$\underline{p \vee q}$ $\underline{\neg p}$ $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Silogismo disjuntivo

$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolução
--	--	-----------

### • Teorema da substituição

Sejam  $f$ ,  $g$  e  $h$  fórmulas proposicionais tais que  $f \Leftrightarrow h$ . Então

1.  $\neg f \Leftrightarrow \neg h$
2.  $f \vee g \Leftrightarrow h \vee g$
3.  $f \wedge g \Leftrightarrow h \wedge g$
4.  $f \rightarrow g \Leftrightarrow h \rightarrow g$
5. Sendo ainda  $g \Leftrightarrow h'$ , então  $f \rightarrow g \Leftrightarrow h \rightarrow h'$

### • Um Sistema Formal, em Matemática, consiste de:

- Um conjunto finito de **símbolos** (ou seja, o **alfabeto**), que é usado para a construção de **fórmulas** (i.e. strings finitas de símbolos);
- Uma **gramática**, que especifica como **fórmulas bem formadas** (fbf's) são construídas a partir dos símbolos do alfabeto. Um procedimento de decisão determina se uma fórmula é bem formada ou não;
- Um conjunto de **axiomas** (fbf's iniciais assumidas válidas e usadas para todos os problemas),
- Um conjunto de **regras de inferência** (como as 9 regras acima).

(os próximos 6 exemplos foram tirados de <http://www.danielclemente.com/logica/dn.en.html> )

<p>EXEMPLO 15: deduza, pelo sistema de dedução natural, que de <math>p</math> e de <math>p \rightarrow q</math> podemos logicamente concluir <math>p \wedge q</math>. Isto é:</p> <p><math>p, p \rightarrow q \Rightarrow p \wedge q</math></p>	<p>(vamos numerar as linhas da dedução):</p> <table><tr><td>1</td><td><math>p</math></td><td>// premissa</td></tr><tr><td>2</td><td><math>p \rightarrow q</math></td><td>// premissa</td></tr><tr><td>3</td><td><math>q</math></td><td>// Elim<math>\rightarrow</math> 2,1</td></tr><tr><td>4</td><td><math>p \wedge q</math></td><td>// Intr<math>\wedge</math> 1,3</td></tr></table>	1	$p$	// premissa	2	$p \rightarrow q$	// premissa	3	$q$	// Elim $\rightarrow$ 2,1	4	$p \wedge q$	// Intr $\wedge$ 1,3
1	$p$	// premissa											
2	$p \rightarrow q$	// premissa											
3	$q$	// Elim $\rightarrow$ 2,1											
4	$p \wedge q$	// Intr $\wedge$ 1,3											

EXEMPLO 16: deduza	Dedução:	
$p \wedge q \rightarrow r, q \rightarrow p, q \Rightarrow r$	1	$p \wedge q \rightarrow r$ // premissa
	2	$q \rightarrow p$ // premissa
	3	$q$ // premissa
	4	$p$ // Elim $\rightarrow$ 2,3
	5	$p \wedge q$ // Intro $\wedge$ 4,3
	6	$r$ // Elim $\rightarrow$ 1,5

EXEMPLO 17 (começando a fazer suposições): deduza	1	$p \rightarrow q$	// premissa
	2	$q \rightarrow r$	// premissa
	3	$p$	// hipótese, para provar a implicação na conclusão final
$p \rightarrow q, q \rightarrow r \Rightarrow p \rightarrow q \wedge r$	4	$q$	// Elim $\rightarrow$ 1,3
	5	$r$	// Elim $\rightarrow$ 2,4
	6	$q \wedge r$	// Intro $\wedge$ 4,5
	7	$p \rightarrow q \wedge r$	// Intro $\rightarrow$ 3,6 (hipótese absorvida)
	Note que a hipótese foi absorvida, pois não estamos afirmando que		

	$p$ é V, mas somente que, se o for, então $q \wedge r$ o são.
--	---

EXEMPLO 18 (usando reiteração, dizer novamente, copiar): deduza  $p \Rightarrow q \rightarrow r$	1	$p$	// premissa
	2	$q$	// hipótese, para provar a implicação na conclusão final
	3	$p$	// reiteração, repetição 1
	4	$q \rightarrow r$	// Intro $\rightarrow$ 2,3 (hipótese absorvida)

EXEMPLO 19 (redução ao absurdo): deduza  $p \rightarrow q, \neg q \Rightarrow \neg p$	1	$p \rightarrow q$	// premissa
	2	$\neg q$	// premissa
	3	$p$	// hipótese, a disprovar por redução ao absurdo
	4	$q$	// Elim $\rightarrow$ 1,3
	5	$\neg q$	// Reiter 2
	6	$\neg p$	//Intro $\neg$ 3,4,5

EXEMPLO 20 (com sub-sub-demonstração): deduza  $p \rightarrow (q \rightarrow r) \Rightarrow q \rightarrow (p \rightarrow r)$	1	$p \rightarrow (q \rightarrow r)$	// premissa
	2	$q$	// hipótese 1
	3	$p$	// hipótese 2
	4	$q \rightarrow r$	// Elim $\rightarrow$ 1,3
	5	$r$	// Elim $\rightarrow$ 4,2
	6	$p \rightarrow r$	// Intro $\rightarrow$ 3,5 (hipótese 2 absorvida)
	7	$q \rightarrow (p \rightarrow r)$	// intro $\rightarrow$ 2,6 (hipótese 1 absorvida)

- Um sistema formal é chamado de **recursivo** (no sentido de que é eficaz, funciona), se o conjunto de axiomas e o de regras de inferência são conjuntos decidíveis (ou, em outros contextos, semidecidíveis). Um conjunto é **decidível** se existe um algoritmo que termina após uma quantidade finita de tempo e decide corretamente se um elemento pertence ou não ao conjunto.
- Um **sistema lógico** (ou, simplesmente, uma lógica) é um sistema formal juntamente com uma semântica (geralmente sob a forma de interpretação modelo-teoria) que atribui valores de verdade (V,F) às sentenças da linguagem formal que não contenham variáveis livres. A lógica é **sadia** (sound), se todas as fbf's que podem ser derivadas são verdadeiras na interpretação. É **completa** se todas as sentenças verdadeiras podem ser derivadas. É **consistente** se, sempre que uma fbf  $\alpha$  é um teorema,  $\sim \alpha$  não é um teorema.

## **2.4. Sanidade, Completude, Consistência. Os Problemas da Satisfatibilidade e da Tautologia (são Decidíveis, mas NP-Completos). Modelo e Teoria**

(pela exiguidade de tempo e de espaço, nesta seção não apresentaremos demonstrações, nem exemplos. Nos exercícios de avaliação, se colocarmos questões sobre a seção, no máximo eles cobrarão o entendimento simples e direto das definições e conceitos.)

- Com os sistemas de inferência acima vistos, ou com outros igualmente adequados, a Lógica Proposicional é **sadia** (só deriva verdades), **completa** (pode derivar todas as fbf's verdadeiras) e **consistente** (não deriva contradições).
- O problema da **satisfatibilidade** é **decidível** para fbf da Lógica Proposicional. Isto é, podemos achar

um algoritmo (um procedimento que sempre, para todas as entradas possíveis, conclui sua execução em tempo finito, e sempre dá a resposta correta) que pode levar trilhões de anos, mas decide se uma fbf é satisfatível, isto é, se há uma interpretação (atribuição de V,F a seus símbolos) tal que a faça, à inteira fbf, ter o valor V.

Mas satisfatibilidade, em Lógica Proposicional, é um problema **NP-completo**. Você só entenderá isto completamente na disciplina Teoria da Computação, mas, em termos práticos, quando se descobre que um problema é NP-completo nosso sangue gela, perdemos toda a esperança de que jamais se possa vir a ter um algoritmo (exato) aceitavelmente eficiente para ele (ainda mais se não for possível truques e técnicas de armazenar dados intermediários em estruturas de dados auxiliares.) Um exemplo: suponha que uma fbf tenha 10000 símbolos (note que problemas com arrays de milhares de elementos são muito usuais e são até considerados modestos, e a expressão deles em Lógica Proposicional precisaria de milhares de símbolos proposicionais). Como cada símbolo pode ser V ou pode ser F, então, para se achar uma interpretação que faça a fbf ter valor V, ou para se dizer que nenhuma tal interpretação existe, temos que explorar  $2^{10000}$  possíveis combinações de valores verdade dos símbolos!!! Impraticável mesmo se cada átomo do universo virasse um supercomputador super-rápido, todos eles trabalhando em paralelo durante muitos trilhões de anos.

- Usando argumentos semelhantes, podemos dizer que, em Lógica Proposicional, o problema da **tautologia é decidível**. Isto é, podemos achar um algoritmo que pode levar trilhões de anos, mas decide se uma fbf é uma tautologia, isto é, se toda interpretação (atribuição de V,F a seus símbolos) resulta em ela ter o valor V. Mas é um problema **NP-completo**, nosso coração gela, etc. ...
- Um **modelo** de uma fbf  $f$  é uma interpretação (atribuição de V,F a seus símbolos proposicionais) que a faça resultar ter valor V. Por exemplo, a interpretação  $a = F, b = F$  é um modelo para  $((a \oplus b) \rightarrow \neg(a \vee b))$ .
- Uma **teoria** é um **sistema formal** (com seus **alfabeto** e **gramática** definindo suas fbf's, seus genéricos axiomas e genéricas regras de inferência), juntamente com axiomas específicos do domínio desejado de problemas a que se aplicará, e com todas as fbf's, que serão chamadas de **teoremas** da teoria e que podem, usando regras de inferência, ser mostradas ser consequências lógicas dos axiomas genéricos e específicos, ou de outros teoremas anteriormente derivados). Por exemplo, a Teoria das Álgebras Booleanas.

## **Problemas sobre toda a Unidade:**

Além dos livros-texto, há muitos outros bons livros e notas de aula sobre Lógica Matemática, muitos deles disponíveis gratuitamente na internet, inclusive nos links que colocamos ao longo desta unidade. Muitos deles têm centenas de exemplos *resolvidos* sobre Lógica Proposicional, portanto sugerimos que escolha os livros e notas de aula mais introdutórios e de formalismo menos pesado, os mais fáceis de ler, e neles escolha os exemplos resolvidos para você fazer sem olhar a solução, só depois comparar a sua com a dele. Escolha somente os assuntos que aqui cobrimos, há muita coisa que consideramos difícil demais e não tão necessária, salte tais assuntos. Recomendamos particularmente as listas de exercícios acompanhadas de gabaritos, da Professora Joseluze de Farias Cunha, em <http://www.dsc.ufcg.edu.br/~logica/>. Também recomendamos a Lista de Exercícios do Prof. Loureiro sobre Lógica Proposicional, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE1.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE1.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE1\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE1_Solucao.pdf), e, futuramente, sobre Cálculo Proposicional [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE2.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE2.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE2\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE2_Solucao.pdf).

## **Recapitulando a Unidade**

Que bom, você já concluiu a unidade II! Se foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter aprendido muitas coisas da parte básica da Lógica Proposicional (a primeira e mais fácil parte da Lógica Matemática, a qual você continuará a ver em Teoria da Computação e em Agentes Inteligentes). Coisas que lhe serão indispensáveis ou muito úteis em todo o resto do curso e sua vida profissional: Você aprendeu mecanismos de raciocínio válidos, esperamos que isso o ajude a diferenciá-los dos falaciosos; aprendeu a sintaxe da linguagem  $\mathcal{L}$  (língua) da Lógica Proposicional, seus conectivos, as regras

para construir fórmulas bem formadas (fbf's); aprendeu a representar as sentenças menores e mais simples da linguagem natural (com apenas um verbo, explícito ou implícito) como símbolos proposicionais, depois a expressar como fbf's as frases que as juntam, depois aprendeu a usar as regras da semântica de  $\mathcal{L}$  para verificar se argumentos da linguagem natural são válidos ou falaciosos; aprendeu o sistema natural de regras de inferências (particularmente o *modus ponens*), a base para todo raciocínio exato das provas de teoremas, concepção de programas, análise e prova da correteza dos mesmos, argumentação jurídica e em geral, etc.. E aprendeu importantes conceitos que lhe serão úteis a vida inteira: satisfatível e não satisfatível (ou contraditório); tautologia; implicação lógica (além da material) e equivalência lógica (*idem*); a sanidade, completude e consistência da Lógica Proposicional com o sistema de inferência natural; a decidibilidade mas NP-Completo do problema da satisfatibilidade e do problema da tautologia de uma fbf.

Na próxima unidade, a III, você estudará recorrência (definir funções e programar computadores através de recursão, achar as equações de recorrência da complexidade de um programa, etc.) e como fazer provas por indução, que certamente é o tipo de provas mais frequentemente usado na Ciência da Computação, a ponto de poder se dizer que programar e provar por indução são gêmeos, quem aprende bem um aprende bem o outro, e quem não aprende bem um não aprende bem o outro. Será um ótimo e importante assunto e você já tem certa familiaridade com ele mesmo se não se deu conta, pois muitas provas (e.g., soma dos termos de uma progressão aritmética) e programas (e.g., Fibonacci, Hanói, etc.) do ensino médio e da disciplina Introdução à Programação já usaram o que vamos estudar mais profundamente. Até lá.

## **Apêndice à Unidade II: Falácias Lógicas**

Uma **falácia** é um argumento que *não* segue as regras de inferência de nenhum *são* sistema formal de Lógica, podendo levar a conclusões falsas (tal argumento, mesmo que leve a uma conclusão verdadeira, é **falacioso** e precisa ser trocado por um logicamente correto).

Com maus propósitos, alguns aprendem em livros e cursos como usar falácias (ver <http://www.csun.edu/~dgdw61315/fallacies.html>) em discursos e debates; outros aprendem estudando os discursos e vídeos de passados mestres do enganar; outros apenas desenvolvem um mau "talento inato". Muitos argumentos usados na retórica dos maus líderes políticos e religiosos, maus advogados, etc. são poderosos para persuasão de multidões de ouvintes, parecendo-lhes muito corretos e convincentes, apesar de conterem falácias. Por isso, todos (ainda mais nós, cuja profissão nos leva a diariamente lidar com provas, com Lógica, com Matemática, com algoritmos) deveriam estudar para reconhecer e evitar falácias. O livro <http://www.logicallyfallacious.com/> expõe e dá exemplos de 300 diferentes tipos de falácias e elas são de variadas classes (incluindo as informais, as que apelam às emoções, apelam a pressões dos nossos pares e da galeria, etc.). Mas, agora, só teremos tempo de ver uma pequena amostra das falácias, com mais ênfase nas que resultam de mau uso da Lógica Formal do que nos malévolos truques da retórica. Agradeço os exemplos aos meus alunos de Linguagem Formais, 2013. Sugiro que, quando você puder, leia mais sobre o assunto, será uma leitura muito interessante (e não será difícil).

**Acidente** (ou "*Dicto Simpliciter Ad Dictum Secundum Quid*", ou "Simplificação de um dito", ou "Generalização Apressada"): assume que uma regra sempre vale, quando, na realidade ela somente vale quase sempre. Depois, toma um caso que é uma exceção da regra, e aplica-a.

EXEMPLO:

1. Aves <sup>[usualmente]</sup> voam
2. Chiquita, a galinha, é uma ave
3. Logo, Chiquita voa

**Afirmação do Consequente:** consiste em se tomar uma condição suficiente e concluir que ela é necessária. Em Lógica, esta falácia corresponde a, do fato  $A \rightarrow B$ , e do fato de B ser verdade, inferirmos (erroneamente) que A é verdade.

EXEMPLO:

- 1) Se estudarmos mais que qualquer pessoa, passaremos em qualquer concurso // note que esta condição é suficiente, não necessária
- 2) Ora, passamos neste concurso
- 3) Logo, estudamos mais que qualquer pessoa // note o erro de estar raciocinando como se (1) fosse necessária, o que não é

**Anfibologia ou Ambiguidade:** consiste em uma (ou mais) das premissas ser ambígua, e a tomarmos no

sentido inadequado.

- 1) O rádio disse "goleou o time local a seleção nacional, em jogo treino" // Isto pode significar que o time local goleou a seleção (improvável), ou que a seleção goleou o time local (mais provável)
- 2) O rádio não mente
- 3) Portanto, vou espalhar que o time local deu uma surra na seleção

**Apelo à Vaidade:** apela à vaidade de quem está ouvindo, a fim de ludibriá-lo e conseguir apoio em uma discussão

- 1) Todas as pessoas cultas e inteligentes acreditam que X é verdade
- 2) Você é a pessoa mais culta e inteligente em todo mundo
- 3) Logo, você acredita que X é verdade, não é?

**Apelo ao Preconceito:** consiste em desnudar maus valores morais do seu adversário ou da classe dele, fazendo despertar preconceito contra ele, somente com isso tentando provar que o que ele disse é sempre falso. É um típico argumento *ad hominem*.

EXEMPLO:

- 1) Juca afirma que o sol é redondo
- 2) A família de Juca é toda ela de desprezíveis mentirosões, por exemplo Juca- Pai e Juca- Avô
- 3) Logo, o sol não é redondo mas, sim, quadrado

Argumentum **Ad Antiquitatem:** consiste em justificar uma conclusão apenas apelando à tradição, ou seja, "se é antigo está completamente correto."

EXEMPLO: Nesta Instituição nunca foi permitido que mulheres ascendessem à posição de chefia; sempre foi assim, e não é por termos mulheres competentes e dispostas a trabalhar que isso precisa mudar

Argumentum **Ad Hominem:** ("Contra o <sup>[caráter do]</sup> Homem <sup>[opositor]" ): consiste em procurar negar uma proposição com uma crítica ao seu autor e não ao seu conteúdo. É uma forte e muito usada arma retórica, mas sem base lógica.</sup>

EXEMPLO:

- 1) Hitler defendia que a sociedade perde se estimular a preguiça e o vadiar
- 2) Hitler foi um dos mais infames homens de todos os tempos
- 3) Logo, (1) é falsa: a sociedade não perde se estimular a preguiça e o vadiar // a conclusão é uma verdade, mesmo o argumento sendo uma falácia e tendo que ser corrigido

EXEMPLO (chamado de "Você Também") (tem muita força retórica, nenhuma da lógica):

- 1) Você disse que não se deve gastar mais do que se ganha
- 2) No entanto, mais de uma vez você ficou tremendamente endividado
- 3) Logo, o que você disse não merece nenhum crédito

EXEMPLO (chamado de "culpa por associação") (tem muita força retórica, nenhuma da lógica):

- 1) Você disse que a terra é redonda
- 2) Isso é exatamente o que Hitler defendia
- 3) Logo, você está em má companhia e o que você disse não merece nenhum crédito. A terra é quadrada

EXEMPLO (chamado de "Você Ganha Ao Defender Isso") (tem muita força retórica, nenhuma da lógica):

- 1) Você diz que atravessar o rio nadando é perigoso
- 2) Você tem um grande barco e cobra para fazer a travessia
- 3) Logo, a afirmativa (1) é movida por sua ganância, e é falsa.

EXEMPLO: Quando Osvaldo apresentou de maneira clara e sucinta as possíveis mudanças no condomínio, Leonardo questionou os presentes se eles deveriam mesmo acreditar no que diz um homem que bebe, profere palavras de baixo calão, e que torce obsessivamente pelo Vasco.

Argumentum **Ad Populum** ("Apelo Ao Povo" ou "À Maioria" ou "A Voz Do Povo É A Voz Da Verdade"): consiste em tomar uma proposição como verdadeira ou falsa simplesmente porque a grande maioria (ou as mais importantes pessoas) acredita que seja assim.

EXEMPLO:

- 1) A maioria dos cientistas mais sérios acredita na Teoria da Evolução, a matéria tendo a inteligência e poder de, em bilhões de anos, evoluir a si mesma desde o Big Bang, inteligentes átomos de hidrogênio, até o ser humano
- 2) Logo, a Teoria da Evolução tem que ser verdadeira

Argumentum **Ad Verecundiam** ("Apelo À Autoridade", "O Mestre Disse"): adota a decisão final de alguma autoridade tomada como infalível, sem sequer analisar as razões que porventura tenha apresentado .

EXEMPLO:

- 1) Linus Pauling, o único homem a ganhar dois prêmios Nobel (Química; e Paz) disse que tomar 20.000 mg de vitamina C/dia retardaria por 20 anos a eclosão de qualquer câncer que já estivesse incubado dentro

duma pessoa

2) Logo, vitamina C é a solução para praticamente erradicar o câncer da humanidade // ele não fez nenhuma experiência sobre isso, não tinha nenhuma autoridade em Medicina, diagnóstico e tratamento de neoplasias malignas, e nenhuma experiência posterior confirmou tal exagero de vitamina C como a cura de muitas das doenças. Mas convenceu milhões de ingênuos, até dizem que ganhou milhões de dólares de laboratórios ...

**Bola de Neve** é um raciocínio em muitas etapas, que parte de uma verdade e vai deduzindo verdades em cadeia, mas insere uma falsidade na cadeia de raciocínio, depois a usa para deduzir uma conclusão que pode ser falsa.

EXEMPLO:

- 1) estamos quase a permitir que todos portem cortadores de unha,
- 2) disso, certamente permitiremos que todos portem tesourinhas, // discutível, mas continuemos
- 3) disso, é certo que permitiremos que todos portem espadas em todos os locais // esta inferência é falsa, (2) não necessariamente implica (3)
- 4) todos que andam com espada, pra lá e pra cá, terminam matando outra pessoa // esta proposição também é falsa, mas não precisaremos dela
- 5) se cada pessoa matar uma outra, então metade da população matará a outra metade
- 6) isso seria horrível e tem que ser evitado
- 7) Portanto, temos que proibir todos de portarem cortadores de unha // conclusão falsa

**Causa Complexa:** consiste em supervalorizar apenas uma (talvez nem mesmo a mais importante) das várias causas possíveis.

EXEMPLO:

- 1) a pista não estava perfeitamente varrida nem lavada
- 2) estas duas coisas podem contribuir para atropelamentos
- 3) logo, este atropelamento não teria ocorrido se não fosse a imperfeita limpeza da pista // isto pode estar ignorando que o motorista estava bêbado e em alta velocidade, e que o pedestre estava descuidado e sem seus óculos e aparelho de surdez, e que o carro não tinha freio, etc.

**Degolar o Espantalho:** seu adversário defende a afirmação X, você a torce para X', depois a destrói a golpes de espada, por fim canta vitória com se tivesse destruído X.

EXEMPLO: Juca disse que dias de sol [também] são bons. Inimigo diz que Juca defende que somente dias de sol são bons; depois observa que, se nunca chovesse, todos morreriam de fome; todos concordam com ele; ele comemora dizendo que venceu Juca e provou que dias de sol sempre são um mal.

EXEMPLO: Fátima alertar para Lourdes comer menos para manter a saúde; Lourdes levanta a voz "vejam todos, Fátima está dizendo que sempre devo jogar parte da comida da mesa no lixo"; todos acreditam em Lourdes e ficam contra Fátima.

**Erro de Categorização- Composição:** consiste em tomar para o todo uma propriedade de suas partes. Mas note: Primeiro, o fato de alguns elementos de um conjunto terem (ou não terem) uma propriedade não implica que todos a tenham (ou não a tenham). Segundo, mesmo que todos a tenham (ou não a tenham), o todo pode ter uma estrutura que faz com que não a tenha (ou a tenha). Terceiro, o todo pode estar numa dimensão diferente da propriedade que alguns (ou mesmo todos) os seus membros têm (ou não têm).

EXEMPLO:

- 1) O Clube de Matemática deste colégio é constituída de membros
- 2) Todos esses membros são torcedores do Vasco
- 3) Logo, o Clube de Matemática é torcedor do Vasco

EXEMPLO:

- 1) Cérebros são constituídos de células
- 2) Nenhuma célula é pensante
- 3) Logo, cérebros não pensam // isto ignora que a estrutura pode dar ao todo características que nenhuma das partes tem no menor dos graus

**Falácia da Divisão** ("tomar a parte pelo todo"): é o oposto da falácia da categorização- composição. Supõe que cada parte de um todo tem cada propriedade dele.

EXEMPLO:

- 1) o cérebro humano é constituído de células (neurônios)
- 2) o cérebro humano é pensante, capaz de raciocínio do mais alto nível
- 3) Logo, cada célula do cérebro humano é pensante, capaz de pensar ao mesmo nível do cérebro // isto ignora que a estrutura pode dar ao todo características que nenhuma das partes tem no menor dos graus

EXEMPLO: "João estuda num colégio de ricos, logo João é rico"



**Falácia Genética:** consiste em tomar algo como verdadeiro ou falso, bom ou mau, certo ou errado, baseando-se unicamente em sua origem.

EXEMPLO:

1) Dizem que, no princípio, aliança de casamento simbolizava o grilhão colocado no tornozelo da mulher para prendê-la e fazê-la escrava // isso é duvidoso e, se é que teve este significado num local nos primeiros séculos de uso, não é necessário que o teve em todos os outros locais e sempre

2) Você pediu à sua noiva para usar aliança depois do casamento

3) Logo, você é um machista que quer fazer sua esposa de escrava. // mesmo se a aliança tivesse tido tal significado em todos os locais, 4.000 anos atrás (e eu duvido disso), não quer dizer que você lhe dê o mesmo significado, hoje.

**Falsa Causa tipo Antecedência,** ou "*Post Hoc, Ergo Propter Hoc*" = "Depois Disso, Portanto Por Causa Disso": consiste em atribuir a causa de um fenômeno a outra fenômeno, pela simples razão de o preceder temporalmente.

EXEMPLO:

1) eu comecei a ler sua carta

2) depois disso, o cão latiu no quintal

3) logo, a fato de eu ler sua carta causa o cão latir no quintal

EXEMPLO:

1) eu lhe aluguei minha casa

2) depois disso, as paredes dela começaram a rachar

3) logo, sua presença foi a causa das rachaduras na parede

EXEMPLO:

1) mais jovens começaram a poder entrar na universidade

2) depois disso, o uso de drogas aumentou na sociedade

3) logo, de alguma forma, a universidade está causando o aumento no consumo de drogas

(as vezes a conclusão vem na ordem reversa: logo, evitar que os jovens entrem na universidade fará com que o consumo de drogas não aumente)

EXEMPLO (conhecido como a **Síndrome do Galo**):.

1) todas as vezes que o galo cantou pela a 6ª vez na noite, pouco depois o sol raiou.

2) logo, é o 6º canto do galo que faz o sol raiar.

**Falsa Causa tipo Simultaneidade,** ou "*Cum Hoc Ergo Propter Hoc*", ou "Com Isso, Portanto Por Causa Disso": consiste em tomar duas coisas que ocorrem juntamente e considerar uma como causa da outra.

EXEMPLO: Na década de 80, toda a Medicina caiu na falácia abaixo

1) no universo das mulheres de uma cara rede de assistência médica, fazer reposição hormonal depois da menopausa apareceu juntamente com a diminuição de número de problemas coronarianos nelas

2) logo, fazer reposição hormonal depois da menopausa faz com que as mulheres tenham menos problemas coronarianos.

Depois, melhores estudos estatísticos descobriram que as mulheres que faziam reposição hormonal eram mais ricas, cuidavam melhor da saúde, tinham tempo para diariamente correr e caminhar e fazer academia, controlavam o peso, comiam mais saudavelmente, e isso, sim, era que diminuía a prevalência das doenças coronarianas.

**Falsa Dicotomia:** consiste em colocar apenas duas alternativas como as duas únicas soluções (quando, de fato, há outras).

EXEMPLO:

1) Antônio só gosta da cor azul ou só gosta da cor verde // isto é um ou-excludente, uma premissa errada que só lhe dá 1 entre 2 opções, e ele pode gostar de muitas outras cores

2) ele hoje está de verde

3) logo, ele não gosta da cor azul, nem de nenhuma outra cor senão a verde

**Falsa Premissa:** mesmo usando corretamente as regras de inferência, parte de uma premissa falsa (mesmo que chegue a uma conclusão verdadeira).

EXEMPLO:

1) todos cães são vegetarianos. // premissa falsa

2) Dálmatas são cães. // premissa verdadeira

3) logo, dálmatas são vegetarianos. // raciocínio correto, mas a partir de premissa falsa, pode levar a falsas conclusões

EXEMPLO:

1) todos os peixes vivem na água. // premissa verdadeira

2) a baleia é um peixe. // premissa falsa

3) logo, a baleia vive na água. // conclusão verdadeira, dedução falaciosa

EXEMPLO:

- 1) nenhum mamífero é um animal aquático // isto é falso
- 2) o golfinho é um animal aquático
- 3) logo, o golfinho não é um mamífero

**Inversão do Ônus da Prova:** consiste em afirmar algo sem provar, desafiando seu oponente provar que é falso, senão terá que aceitar como verdadeiro.

EXEMPLO:

- 1) nesta ditadura, quem não provar que não é inocente é culpado
- 2) você não provou que não foi você o assassino
- 3) logo, é você o assassino e ficará preso até que possa provar sua inocência

EXEMPLO:

- 1) foi facilmente provado que  $P \subseteq NP$
- 2) em mais de 50 anos de esforços, ninguém achar que um problema em NP não está em P, ninguém conseguiu provar que  $P \subset NP$
- 3) logo, está provado que  $P = NP$

**Negação do Antecedente:** Toma uma implicação se-então ( $\rightarrow$ ) que é verdadeira mas não é uma equivalência se-e-somente-se ( $\leftrightarrow$ ) (portanto, seu antecedente não é necessário para sua conclusão), e toma a negação do seu antecedente, para inferir a negação de sua conclusão.

EXEMPLO:

- 1) se é de ouro, então é caro. //A condição é verdadeira, mas não é necessária.
- 2) não é de ouro.
- 3) então não é caro. //Não se pode afirmar isso somente levando em consideração a premissa (1).

EXEMPLO:

- 1) se em ti tivesse caído um raio no aniversário de 20 anos ontem comemorado, terias morrido jovem
- 2) tal raio não caiu
- 3) logo, é certo que não morrerás jovem



## UNIDADE III

# 3. EQUAÇÕES DE RECORRÊNCIA e PROVAS POR INDUÇÃO MATEMÁTICA

Deus nos deu duas formas básicas de raciocínio: o indutivo e o dedutivo. Às vezes são bem usados, muitas vezes não.

- O **raciocínio indutivo** parte de experiências e observações de fatos individuais e tenta chegar a conclusões, a regras que expliquem os fatos e generalizem as observações (Por exemplo: "estou atravessando esta pequena cidade de madrugada, só vi 3 pessoas nas ruas, e todas elas estavam bêbadas. Daí, posso induzir que todos os habitantes dela são bêbados." Onde está o erro deste raciocínio?).
- O **raciocínio dedutivo**, baseando-se na lógica, parte de axiomas e de teoremas já demonstrados e, usando regras de inferência da lógica, chega a conclusões (Por exemplo: "sem exceção, todos os homens de tal família são e serão desonestos, todos concordam, não é?; esse menino acabou de nascer nessa família; logo, será desonesto" Onde está a falácia deste raciocínio?).

Feitos de forma intuitiva e informal (portanto com riscos de imprecisão e ambiguidade) ambos tais tipos de raciocínio podem levar a erros, tanto na vida informal como na Matemática e demais ciências exatas.

**Nosso objetivo nesta unidade** é que, ao final, você, usando os rigores da Matemática e da Lógica, saiba perfeitamente como estudar problemas e os modelar usando o que chamaremos de equações de recorrência, depois usar um *são e preciso* raciocínio indutivo para produzir provas de indução usando tamanhos formalismo e rigor que lhes garantam absolutas precisão e correte. Na unidade IV faremos o mesmo quanto o raciocínio dedutivo.

*Lembre: Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, **cada semana dedicando 4 a 8 horas para estudar este livro.***

### Conteúdo desta unidade:

- 3.1. Equações de Recorrência. Determinação Delas. Fórmulas Fechadas (Conjecturas)
- 3.2. Provas pelo Princípio da Indução Matemática Simples (ou Fraca)
- 3.3. Provas pelo Princípio de Indução Matemática Completa (ou Forte)



---

Se você quiser ver o assunto mais explicado e profundamente, não precisará de mais que os livros textos da ementa da disciplina. Mas, se ademais ou ao invés deles, quiser algo gratuito ou da internet, talvez possa começar por *Indução Matemática*, Abramo Hefez, <http://server22.obmep.org.br:8080/media/servicos/recursos/296654.o>; ou *Indução e Indução Matemática*, palestra de José Morgado <http://nautilus.fis.uc.pt/bspm/revistas/17/023-034.150.pdf>. Agradeço ao aluno *Túlio Albuquerque Pascoal* por ter ajudado a revisar esta unidade.

---

### 3.1. Equações de Recorrência. Determinação Delas. Fórmulas Fechadas (Conjecturas)

• Uma **Relação de Recorrência** ou **Equação de Recorrência** é aquela que, em parte de sua definição, diz como resolver diretamente a menor e mais simples possível instância do problema, e nisso não faz referência a nenhuma outra instância do problema; e, no restante da sua definição, diz como resolver instâncias maiores e mais complexas do problema, nisso usando, fazendo referência a uma ou mais de suas instâncias menores. Em outras palavras, uma recorrência é uma expressão que dá o valor de uma função em termos dos valores "anteriores" da mesma função. Uma função recursiva  $f(n)$  é definida em termos de valores para  $f(m)$ , onde  $m < n$ .

#### EXEMPLO 1:

a) No domínio dos naturais, você define fatorial de  $n$  como 1, se  $n$  for 0; e define como  $n$  vezes fatorial de  $n-1$ , se  $n$  for maior que 0:

$$\begin{aligned} n! &= 1 && \text{caso } n = 0 \\ n! &= n(n-1)! && \text{caso } n > 0 \end{aligned}$$

b) Você define a relação binária "É\_Ancestral\_De" assim:

$$\begin{aligned} x \text{ É\_Ancestral\_De } z &\text{ SE } x \text{ É\_Pai\_Ou\_Mãe\_De } y \text{ E } y \text{ É\_Ancestral\_De } z. \\ \text{OU} \\ x \text{ É\_Ancestral\_De } y &\text{ SE } x \text{ É\_Pai\_Ou\_Mãe\_De } y. \end{aligned}$$

c) No domínio dos naturais não nulos  $\{1, 2, 3, \dots\}$ , você define a soma dos  $n$  primeiros deles como sendo 1 se  $n$  for 1, e como sendo  $n$  mais a soma dos  $n-1$  primeiros naturais, se  $n$  for maior que 1:

$$\begin{aligned} S(n) &= 1 && \text{caso } n=1 \\ S(n) &= n + S(n-1) && \text{caso } n>1 \end{aligned}$$

d) (Prof. Becceneri, INPE): Um processo cria memória dinamicamente. Inicialmente, aloca 64 MB (chamemos isto de  $M_0$ ). A cada iteração exige mais 15% de memória. Então, as equações de recorrência para este problema são (complete):

$$\begin{aligned} M_i &= 64 && \text{para } i = 0 \\ M_i &= 1,15M_{i-1} && \text{para } i > 0 \end{aligned}$$

e)  $n$  está no domínio dos naturais não nulos, e você sabe que uma certa função  $f$  de  $n$  vale 1 para  $n=1$ , e, nos demais casos, vale o valor anterior ( $f(n-1)$ ) mais  $3n$  mais 2. Escreva as equações de recorrência:

$$\begin{aligned} f(n) &= 1 && \text{caso } n=1 \\ f(n) &= f(n-1) + 3n + 2 && \text{caso } n>1 \end{aligned}$$

• Uma recorrência pode ser vista como um **algoritmo recursivo** que calcula uma função a partir de um "valor inicial". Talvez haja um fundo de verdade em quem diz que *"saber programar é saber achar algoritmos recursivos, e vice-versa, e ambas essas coisas equivalem à proficiência em achar definições recursivas para funções."* Acharmos que, se isso não for totalmente verdade, tem um certo fundo de verdade, e isso é bom. Nesta unidade, primeiramente invistamos em achar definições recursivas, pois isto vai lhe ajudar muito a programar, no futuro. E, em segundo lugar, invistamos também em achar fórmulas fechadas para recursões e prová-las rigorosamente, por indução, pois isto vai ajudá-lo a descobrir como é fácil errarmos em pensar que uma recursão ou loop estão totalmente corretos, e vai nos ensinar a ser mais cuidadosos, e a identificar e corrigir esses erros, e a saber provar a correção de programas (mesmo os iterativos).

• **Resolver** um sistema de equações recorrentes é encontrar uma **fórmula fechada** que lhe seja solução. Uma **fórmula fechada**, ou **solução explícita**, dá o valor da função recursiva diretamente em termos do seu argumento, sem referência a nenhum valor da função para uma instância menor do problema. Tipicamente, uma fórmula fechada é uma combinação de polinômios, de quocientes de polinômios, de logaritmos, de exponenciais, etc. Só não pode ter recorrência dentro dela, isto é, não pode se referir a instâncias menores do problema, mesmo que disfarçadas dentro de somatórios ( $\Sigma$ ) e produtórios ( $\Pi$ ) e loops de programas.

EXEMPLO 2: Ache a fórmula fechada para os problemas c, d, e, do exemplo acima.

RESPOSTA:

c) Temos uma progressão aritmética de  $n$  termos, primeiro termo (chamado de  $S(1)$ ) 1, e razão 1, e a fórmula da soma dos termos de uma P.A. nos dá

$$S(n) = n(1+n)/2, \quad \text{para } n \geq 1$$

d) Temos uma progressão geométrica de  $n+1$  termos, primeiro termo (chamado  $M_0$ ) 64, e quociente 1,15, e a fórmula da soma dos termos de uma P.G. nos dá

$$64(1,15^{n+1} - 1)/(1,15 - 1) = 64(1,15^{n+1} - 1)/0,15 = 426,667(1,15^{n+1} - 1) \quad \text{para } n \geq 0$$

e) A resposta é  $(3n^2)/2 + 7n/2 - 4$ . Bem, é bastante fácil você verificar que a resposta está correta para qualquer  $n$  relativamente pequeno (1,2,3,4,5,6,...); dentro de poucas páginas você aprenderá a provar por indução que a fórmula é válida para todo natural não nulo; mas o mais difícil é como chegar ao começo de tudo, isto é, como "adivinhar" que a resposta, a fórmula fechada, é essa. Isso você só começará a ver, de

leve, no exemplo 7, e, em casos mais difíceis (como o problema 2, muito difícil), talvez no mestrado, em cursos sobre Análise de Complexidade de Algoritmos (método de adivinhação inteligente, substituição, árvores de recorrência, etc.)

EXEMPLO 3: Considere o algoritmo recursivo abaixo, para o conhecido problema da Torre de Hanói (não se preocupe nada com a linguagem, com detalhes, só se preocupe com a ideia principal, geral e superficial do algoritmo. E nem se preocupe em entender bem o algoritmo e seu funcionamento real, a baixo nível. Basta que você se concentre em contar cada movimento de um só disco

[http://upload.wikimedia.org/wikipedia/commons/thumb/6/60/Tower\\_of\\_Hanoi\\_4.gif/300px-Tower\\_of\\_Hanoi\\_4.gif](http://upload.wikimedia.org/wikipedia/commons/thumb/6/60/Tower_of_Hanoi_4.gif/300px-Tower_of_Hanoi_4.gif)):

**procedure Hanói(De, Para, Aux, n):**

**se  $n > 1$  então Hanói(De,Aux,Para,n-1)**

**mova disco de De para Para**

**Hanói(Aux,Para,De,n-1)**

**senão mova disco do topo de De para Para**

Quais as equações de recorrência para o tempo de execução? (Repetimos: assuma que basta contar os movimentos dos discos)

RESPOSTA:

Pelo exame do algoritmo (pense bem, examinando-o), concluímos que as equações de recorrência são:

$$\begin{aligned} T(n) &= T(n-1) + 1 + T(n-1) = 2T(n-1) + 1 && \text{caso } n > 1 \\ T(n) &= 1 && \text{caso } n = 1 \end{aligned}$$

EXEMPLO 4: Um procedimento recursivo consome 1 unidade de tempo se o tamanho (n) do problema é 1. Caso contrário, o procedimento divide o problema de tamanho n em 3 partes de tamanhos os mais iguais possíveis a  $n/3$ , resolve-os recursivamente, depois junta as soluções parciais formando a solução mais geral, e gasta um tempo  $n \times \log_3 n$  para fazer a divisão mais a junção. Quais as equações de recorrência para o tempo de execução deste algoritmo?

RESPOSTA:

$$\begin{aligned} T(n) &= 1 && \text{para } n = 1 \\ T(n) &= 3 \times T(n/3) + n \times \log_3 n && \text{para } n > 1 \end{aligned}$$

EXEMPLO 5: Eis o algoritmo para pesquisa binária por um valor Chave em um arranjo ordenado A[] cujo menor índice é IMin e maior índice é IMax. Se a pesquisa encontrar Chave, retorna a posição onde a encontrou:

```
int PesqBinaria(int A[], int Chave, int IMin, int IMax)
{
    // teste se o arranjo está vazio
    if (IMax < IMin):
        // o arranjo está vazio, portanto retorne algo que signifique que Chave não foi encontrada
        return Chave_NÃO_ENCONTRADA;
    else
    {
        // calcule o ponto central, para dividir a faixa do arranjo em duas metades
        int IMeio = (IMin + IMax) divisãointeira 2;

        // comparação que tem 3 possibilidades
        if (A[IMeio] > Chave)
            // Chave está na metade mais baixa da faixa de A
            return PesqBinaria(A, Chave, IMin, IMeio-1);
        else if (A[IMeio] < Chave)
            // Chave está na metade mais alta da faixa de A
            return PesqBinaria(A, Chave, IMeio+1, IMax);
        else
            // Chave foi encontrada
            return IMeio;
    }
}
```

Quais as equações de recorrência para o tempo de execução deste algoritmo? Assuma que só o que importa é o tempo de comparação.

RESPOSTA:

$$\begin{aligned} T(1) &= 1 \\ T(n) &= T(\text{teto}(n/2)) + 1 && \text{para } n > 1 \end{aligned}$$

EXEMPLO 6: Procure a definição recursiva do algoritmo de ordenação MergeSort, e escreva as equações de recorrência para seu tempo de execução, considerando que só importa o tempo das comparações.

RESPOSTA:

$$\begin{aligned} T(n) &= 2 \times T(n/2) + n && \text{para } n > 1 \\ T(1) &= 1 \end{aligned}$$

## 3.2. Provas pelo Princípio da Indução Matemática Simples (ou Fraca)

Analogia com escada:



Dada uma escada de infinitos degraus, para que se alcance um qualquer degrau  $n$  (que não está abaixo de um dado degrau  $n_0$ ), basta que:

- 1) o degrau  $n_0$  seja alcançado;
- 2) qualquer que seja  $k$  não abaixo de  $n_0$ , se o degrau  $k-1$  for alcançado, isto implica que o degrau  $k$  também o será.

Analogia com dominós caindo em fila



Dados infinitos dominós em fila, para eles caírem em sequência e derrubarem uma qualquer peça  $n$  (que não está antes que uma dada peça  $n_0$ ) basta que:

- 1) o dominó  $n_0$  seja derrubado;
- 2) qualquer que seja  $k$  não abaixo de  $n_0$ , se o dominó  $k-1$  cair derrubará o dominó  $k$ .

### **Princípio de Indução Matemática** (Simples, Fraca) (P.I.M. versão I):

Seja  $P$  uma proposição <sup>[isto é, a afirmação de uma propriedade]</sup> definida nos inteiros não negativos. Se pudermos provar que:

(i) para um dado inteiro não negativo  $n_0$ , a proposição a ele associada <sup>[i.e., a proposição  $P(n_0)$ ]</sup> é verdadeira; e

(ii) para qualquer inteiro  $m > n_0$ , a suposição de que a preposição associada ao inteiro  $m-1$  <sup>[i.e., a proposição  $P(m-1)$ ]</sup> é verdadeira implicará que a preposição associada ao inteiro  $m$  <sup>[i.e.,  $P(m)$ ]</sup> também é verdadeira,

então concluímos que é verdadeira a proposição aplicada a *todo* inteiro  $n \geq n_0$  <sup>[i.e.,  $P(n)$ ]</sup>.

[(i) é chamada de "*passo base* ou  $P(n_0)$ "; a suposição em (ii) é chamada de "*hipótese indutiva* ou  $P(n-1)$ "; e a implicação em (ii) é chamada "*passo indutivo* ou  $P(n)$ ". Usualmente (mas não necessariamente),  $n_0$  é 1 ou 0]

### **Princípio de Indução Matemática** (Simples, Fraca) (P.I.M. versão II)

[equivalente à I, acima. Você sempre pode usar a versão que preferir, portanto só precisa aprender e usar uma delas]:

Seja  $P$  uma proposição definida nos inteiros não negativos. Se pudermos provar que:

(i) para um dado inteiro não negativo  $n_0$ ,  $P(n_0)$  é verdadeira; e

(ii) para qualquer inteiro  $m \geq n_0$ , a suposição de que  $P(m)$  é verdadeira implicará que  $P(m+1)$  também é verdadeira,  
então concluímos que  $P(n)$  é verdadeira para *todo*  $n \geq n_0$ .

EXEMPLO 7: Você está procurando descobrir uma fórmula para a soma dos primeiros  $n$  números ímpares. Para talvez lhe ajudar a descobrir algum tipo de regularidade ou algo semelhante, você rascunhou a tabela tendo, onde, em cada coluna, a 1ª linha dá o valor de  $n$ , a 2ª linha dá o  $n^{\text{ésimo}}$  ímpar, e a 3ª linha dá a dita soma,

$n$	0	1	2	3	4	...	$n$
$n^{\text{ésimo}}$ ímpar	não existe	1	3	5	7	...	$2n-1$
$S(n)$ , a soma $1+3+5+7+\dots+(2n-1)$	0	$1 = 1$	$1+3 = 4$ $= n^2$	$1+3+5 = 9$ $= n^2$	$1+3+5+7 = 16$ $= n^2$	...	$n^2$ (CONJECTURA!)

Analisando a tabela, você percebe que, para  $n$  igual a 0,1,2,3,4, a soma sempre é igual a  $n^2$ . Será isso uma coincidência? Valerá isto para qualquer inteiro não negativo  $n$ ? Você forma, em sua mente, a conjectura de que é verdadeira a proposição  $P(n)$  definida como "para qualquer inteiro não negativo  $n$ , a soma  $S(n)$  dos primeiros  $n$  números ímpares [i.e.,  $1 + 3 + 5 + \dots + (2n-1)$ ] é igual a  $n^2$ ". Provemos esta conjectura, usando o P.I.M. versão I.

[i] Para  $n_0 = 0$ , a proposição  $P(n_0)$  é verdadeira porque ela leva a  $S(n_0) = S(0) = n_0^2 = 0^2 = 0$ , que concorda com a definição de que a soma dos primeiros 0 elementos de qualquer sequência é 0;

[ii] para qualquer inteiro  $m > n_0$ , façamos a hipótese de que  $P(m-1)$  é verdade, i.e.,  $S(m-1) = 1+3+5+\dots+(2(m-1)-1) = (m-1)^2$ . Então

$$\begin{aligned} S(m) &= [1+3+5+\dots+(2(m-1)-1)] + (2m-1) = S(m-1) + (2m-1) && // \text{ Por definição de } S(m-1) \\ &= (m-1)^2 + (2m-1) && // \text{ pela hipótese indutiva, aplicada a } S(m-1) \\ &= m^2 - 2m + 1 + 2m - 1 && // \text{ algebrismo simples: } (a-b)^2 = a^2 - 2ab + b^2 \\ &= m^2, \text{ portanto a } P(m) \text{ é verdadeira} \end{aligned}$$

Portanto, uma vez que provamos as etapas (i) e (ii), então, pelo Princípio de Indução Matemática [versão I], a proposição está provada. C.Q.D. (Como se Queria Demonstrar).

EXEMPLO 8: Sr. "Intuitivo" (nada preciso nem científico) fez muitas contas e verificou que, para  $n = 0,1,2,3, \dots, 40$ , sempre resultou que  $f(n) = n^2 - n + 41$  é um número primo (isto é, que só é divisível por 1 e por si mesmo). Daí, numa "indução caipira", ele diz que "provou" que isto sempre é verdadeiro. Pode você ajudá-lo por realmente provar sua conjectura? Ou por achar um contraexemplo que a refute?

Bem, a proposição dele é "para qualquer inteiro não negativo  $n$ ,  $f(n) = n^2 - n + 41$  é um número primo." Tentemos provar esta conjectura.

[i] Para  $n_0 = 0$ , a proposição  $P(n_0)$  é verdadeira porque  $f(0) = 0^2 - 0 + 41 = 41$ , que realmente é primo (porque testamos e vimos que não é divisível por nenhum inteiro entre 2 e  $41-1=40$ );

[ii] para qualquer inteiro  $m > n_0$ , façamos a hipótese de que  $f(m-1) = (m-1)^2 - (m-1) + 41 = m^2 - 2m + 1 - m + 1 + 41 = m^2 - 3m + 43$  é primo. Então  $f(m) = m^2 - m + 41 = f(m-1) + 2m + 2$  deveria sempre ser primo para a prova prosseguir, mas isso não é verdade para  $m = 41$ , que resulta em  $f(m-1) = f(40) = 40^2 - 40 + 41 = 1601$  que é primo (verifique), mas resulta em  $f(m) = f(41) = f(41-1) + 2 \times 41 + 2 = 1601 + 82 + 2 = 1685$  que é divisível por 5.

Portanto, não pudemos usar o P.I.M.-I para provar a conjectura, e descobrimos que  $n=41$  é um contraexemplo que a refuta.

EXEMPLO 9 ("bolas de golfe"): Começamos com 4 recipientes que contêm quantidades conhecidas de bolas de golfe. Um "movimento legal" é definido como removendo 1 bola de cada um de três quaisquer dos recipientes e colocando essas 3 bolas no recipiente restante. Por exemplo, se os 4 recipientes contêm 10, 12, 14, 16 bolas, então o resultado de um dos 4 "movimentos legais" possíveis seria 13, 11, 13, 15. A questão é: dada uma distribuição inicial, é possível, através de uma sequência de "movimentos legais", chegar a uma distribuição que tenha o mesmo número de bolas em cada recipiente? Assim, no exemplo, poderíamos nós chegar a 13, 13, 13, 13? Sua tarefa é usar o P.I.M.-II para determinar uma condição, ou conjunto de condições, sobre a distribuição inicial, que permitirá o jogo ser ganho.

RESPOSTA:

- Sejam  $(n_1, n_2, n_3, n_4)$  os números naturais de bolas nos quatro recipientes.

- Depois de muito pensar e fazer experimentos usando lápis e papel, formulamos a conjectura: A condição necessária e suficiente para o jogo terminar (com sucesso, claro!) é que, no início, o valor absoluto da



diferença entre os números de bolas entre dois recipientes quaisquer seja múltiplo de 4 (note que isto implica que a soma dos números de bolas nos quatro recipientes seja múltiplo de 4).

- A prova é por indução sobre o número ( $n$ ) de jogadas necessárias para se chegar à solução.

- *Passo base* ( $n = 0$ ): Uma solução é da forma  $(x, x, x, x)$  (onde  $x$  é qualquer natural), evidentemente satisfazendo a condição da conjectura.

- *Hipótese Indutiva* ( $n = m$ ): Suponhamos que a condição da tese vale para  $n = m$ , onde  $m$  é um natural qualquer, isto é: estamos com um estado  $(n_1, n_2, n_3, n_4)$  que dista  $m$  jogadas da solução, e  $|(n_1 - n_2)|$ ,  $|(n_1 - n_3)|$ ,  $|(n_1 - n_4)|$ ,  $|(n_2 - n_3)|$ ,  $|(n_2 - n_4)|$ , e  $|(n_3 - n_4)|$  são múltiplos de 4.

Só nos resta provar que as condições da conjectura também valem para  $m + 1$ .

- *Passo indutivo* ( $n = m + 1$ ): Ora, há 4 estados que podem ter sido os anteriores do atual. O primeiro, que corresponde a termos movido as 3 bolas para o 4º recipiente, é  $(n_1 - 1, n_2 - 1, n_3 - 1, n_4 + 3)$ , e você pode checar que este estado ainda satisfaz as 6 equações na hipótese indutiva, isto é, satisfaz a condição da conjectura. Semelhantemente para os outros 3 estados possíveis de ter sido anteriores ao atual (obviamente, devem ser descartados os estados que tenham um dos recipientes com número negativo de bolas). C.Q.D.

EXEMPLO 10 ("Soma dos termos de uma P.A."): Dada a progressão aritmética

$$a_1, a_2, \dots, a_n,$$

onde  $a_i = a_1 + (i-1)r$  para um certo  $a_1$ , um certo  $r$ , e para todo inteiro  $i$  no intervalo  $[1, n]$ ,

prova por **Indução Matemática Simples** (ou Fraca) a conjectura:

"a soma  $(a_1 + a_2 + \dots + a_n)$  dos  $n$  primeiros termos da P.A., simbolizada por  $S(n)$ , é dada por  $S(n) = (n/2)(a_1 + a_n)$ " (C)

RESPOSTA:

*Etapa Base* ( $n = 1$ ):

A definição de soma de uma sequência de 1 só elemento resulta que  $S(n) = a_1$ , e a fórmula (C) também resulta que  $S(n) = (1/2)(a_1 + a_1) = a_1$ , portanto (C) é válida.

*Hipótese Indutiva* ( $n = m - 1$ ):

Suponhamos que (C) é válida para  $m - 1$ , onde  $m$  é um qualquer inteiro  $m > 1$ :

$$S(m-1) = ((m-1)/2)(a_1 + a_{m-1}) \quad (H)$$

ou, equivalentemente,

$$\begin{aligned} S(m-1) &= (1/2)(m-1)(a_1 + (a_1 + (m-2)r)) \\ &= (1/2)(m-1)(2a_1 + (m-2)r) \end{aligned} \quad (H')$$

Só nos falta provar que (C) também é válida para  $m$ .

*Etapa Indutiva* ( $n = m$ ):

$$S(m) = S(m-1) + a_m$$

$$= (1/2)(m-1)(2a_1 + (m-2)r) + a_m \quad (\text{usando } H')$$

$$= (1/2)(m-1)(2a_1 + (m-2)r) + (a_1 + (m-1)r) \quad (\text{usando a definição de } a_m)$$

$$= (1/2)(m-1)(2a_1 + (m-1)r) + a_1 + (m-1)r \quad (\text{"Truque" que uma vez esqueci de usar em um aula de improviso})$$

$$= (1/2)(m-1)(2a_1 + (m-1)r) - (1/2)(m-1)r + a_1 + (m-1)r \quad (\text{colocando } (m-1)r \text{ em evidência})$$

$$= (1/2)(m-1)(2a_1 + (m-1)r) + (1/2)(m-1)r + a_1 \quad (\text{colocando } (m-1)r \text{ em evidência})$$

$$= ((1/2)(m-1) + 1/2)(2a_1 + (m-1)r) \quad (\text{colocando } (2a_1 + (m-1)r) \text{ em evidência})$$

$$= (1/2)(m)(2a_1 + (m-1)r)$$

$$= (1/2)(m)(a_1 + (a_1 + (m-1)r)) \quad (\text{usando o "truque" } 2a_1 = a_1 + a_1)$$

$$= (1/2)(m)(a_1 + a_m)$$

Portanto, (C) também é válida para  $m$ , C.Q.D.

PROBLEMA 1 [COM SOLUÇÃO]:

Considere as equações de recorrência [correspondentes à complexidade temporal de um algoritmo recursivo chamado de MaxMin, que determina quais são o maior e o menor elemento de um conjunto com  $n \geq 2$  elementos].

$$T(n) = 1 \quad \text{para } n = 2;$$

$$T(n) = 2T(n/2) + 2 \quad \text{caso } n > 2$$

Use o Princípio de Indução Matemática (pode ser a versão II) para provar a conjectura, que é esta: "para todo  $n > 2$ ,  $T(n) = 3n/2 - 2$ ".

Dica: Mude a variável por uma que torne as coisas mais simples, com todas as divisões inteiras. Isto é, considere, por simplicidade, que  $n = 2^i$ , para algum  $i$  nos naturais positivos ( $i \geq 1$ , portanto  $n \geq 2$ ); depois, ao invés de fazer indução sobre  $n$ , faça-a sobre  $i$ .

--- \*\* Cubra abaixo e resolva sozinho\* \*\* ---

RESPOSTA:

Por facilidade (evitando divisões não inteiras), mudemos a variável para  $i$ , onde  $n = 2^i$ . As equações de recorrência ficam sendo

$$\begin{aligned} T(2^i) &= 1 && \text{para } i=1; \\ T(2^i) &= 2T(2^{i-1}) + 2 && \text{caso } i>1 \end{aligned}$$

e a conjectura que queremos provar fica sendo “para todo  $i>1$ ,  $T(2^i) = (3 \times 2^{i-1}) - 2$ ”.

Um modo de provar:

*Passo base:* ( $i=1$ ): pela definição recursiva, já temos que  $T(2^1) = 1$ . A conjectura é verdadeira porque também resulta em  $(3 \times 2^{1-1}) - 2 = 3 - 2 = 1$ .

*Passo indutivo:* Seja um qualquer inteiro  $i>1$ . Assumamos que a conjectura vale para  $i-1$ , isto é,  $T(2^{i-1}) = (3 \times 2^{i-2}) - 2$ . Agora, só precisamos provar que a conjectura é verdadeira para  $i$ . Tomemos a equação de recorrência  $T(2^i) = 2T(2^{i-1}) + 2$ . Apliquemos aqui a hipótese indutiva, resultando em  $T(2^i) = 2((3 \times 2^{i-2}) - 2) + 2 = 3 \times 2^{i-1} - 4 + 2 = 3 \times 2^{i-1} - 2$ . A conjectura vale para  $i$ . C.Q.D.

Outro modo de provar:

- *Passo base* ( $i = 1$ ) (portanto,  $n = 2$ )

A conjectura é válida, pois ela resulta em  $3 \times 2/2 - 2 = 1$ , o que concorda com a 1ª equação de recorrência.

- *Hipótese Indutiva* ( $i=k$ ): suponhamos que a conjectura vale para um certo  $i=k$ , isto é  $T(2^k) = 3 \times (2^k)/2 - 2$ .

Agora, só temos que provar que a conjectura vale para  $i=k+1$ .

- *Passo indutivo* ( $i = k+1$ ) (isto é,  $S$  tem  $2n = 2^{k+1}$  elementos):

$$\begin{aligned} T(2n) &= 2T(n) + 2 && // \text{pela 2ª equação de recorrência} \\ &= 2 \times (3 \times (2^k)/2 - 2) + 2 && // \text{pela hipótese indutiva} \\ &= (3 \times (2^{k+1})/2) - 4 + 2 \\ &= 3 \times (2^{k+1})/2 - 2 \end{aligned}$$

C.Q.D.

[Note como ambas as provas equivalem a termos provado (voltando à variável  $n$ ):  $T(n) = 3n/2 - 2$ ]

PROBLEMA 2 [COM SOLUÇÃO, mas muito difícil].

Seja a seguinte recorrência:

$$T(n) = \text{se } n = 1 \text{ então } 1 \text{ senão } 3T(n \text{ divisão inteira } 2) + n$$

Funções descontínuas tais como a função piso (implícita na divisão inteira) são difíceis de analisar, portanto comecemos nos restringindo a  $n$  ser uma exata potência de 2 [expoente é um natural]:

$$T(2^k) = \text{se } k = 0 \text{ então } 1 \text{ senão } 3T(2^{k-1}) + 2^k$$

Pode você formar uma conjectura para uma solução (uma fórmula fechada, direta, sem recursão nem somatório nem produtório, mas, sim, “simples e direta”)? Pode prová-la por indução?

--- \* \* \* Cubra abaixo e resolva sozinho \* \* \* ---

RESPOSTA:

Primeiro, tabulemos:

$n$	1	2	4	8	16	32	...
$T(n)$	1	5	19	65	211	665	...

Segundo, após muitas tentativas, achamos regularidade ao guardarmos uma grande quantidade de “história”:

$n$	$2^0$	$2^1$	$2^2$	$2^3$	$2^4$	$2^5$	...
$T(n)$	1	$3 \times 1 + 2$	$3^2 \times 1 + 3 \times 2 + 2^2$	$3^3 \times 1 + 3^2 \times 2 + 3^1 \times 2^2 + 2^3$	$3^4 \times 1 + 3^3 \times 2 + 3^2 \times 2^2 + 3 \times 2^3 + 2^4$	$3^5 \times 1 + 3^4 \times 2 + 3^3 \times 2^2 + 3^2 \times 2^3 + 3 \times 2^4 + 2^5$	...

Terceiro, concebemos a conjectura generalizante:

$T(2^k) = \sum_{i=0}^k (3^{k-i} \times 2^i)$ , que *parece* (mas teremos que provar a conjectura) a soma dos  $(k+1)$  primeiros termos de uma p. geométrica de primeiro termo 1 e quociente  $2/3$ . Portanto, pela conhecida fórmula para essa soma,

$$T(2^k) = 3^k(1-(2/3)^{k+1})/(1-2/3) = 3^{k+1} - 2^{k+1}$$

Quarto, provamos a conjectura

$$T(2^k) = 3^{k+1} - 2^{k+1} \quad (\#)$$

por indução matemática:

*Passo base ( $k=0$ ):* O valor da fórmula  $(\#)$  coincide com a realidade (expressa na tabela) quando  $k=0$ .

*Hipótese Indutiva ( $k=m$ ):* Suponhamos que  $(\#)$  é válida para um inteiro qualquer,  $m$ , tal que  $m \geq 1$ :  $T(2^m) = 3^{m+1} - 2^{m+1}$

*Passo indutivo ( $k=m+1$ ):* Quando  $k = m+1$ , a recorrência resulta em

$$T(2^{m+1}) = 3T(2^m) + 2^{m+1}$$

Usando a hipótese indutiva, temos

$$T(2^{m+1}) = 3 \times (3^{m+1} - 2^{m+1}) + 2^{m+1} = 3^{m+2} - 2^{m+2}$$

Portanto, a conjectura também é válida para  $k=m+1$ .

..*Conclusão:*  $(\#)$  está provada, por indução matemática.

### PROBLEMA 3 [COM SOLUÇÃO]:

Prove que a soma dos  $n$  primeiros naturais, isto é  $1+2+3+ \dots + n$ , é dada pela fórmula  $\sum_{k=1}^n k = \frac{n(n+1)}{2}$

--- \*\* \* Cubra abaixo e resolva sozinho\* \* \* ---

RESPOSTA:

*Passo base ( $n=1$ ):*

O lado esquerdo da fórmula a provar resulta em 1. O lado direito também resulta em  $1 \times 2/2 = 1$ . Portanto, a fórmula vale para  $n=1$ .

*Hipótese Indutiva ( $n=m$ ):* suponhamos que a fórmula a provar vale para  $n$  igual a um certo natural  $m$ , qualquer. Isto é:

$$\sum_{k=1}^m k = \frac{m(m+1)}{2}$$

*Passo indutivo ( $n=m+1$ ):*

$$\begin{aligned} \sum_{k=1}^{m+1} k &= \sum_{k=1}^m k + (m+1) && // \text{ porque ...} \\ &= m(m+1)/2 + (m+1) && // \text{ pela hipótese indutiva} \\ &= (m+1)(m/2 + 1) && // \text{ colocamos } (m+1) \text{ em evidência} \\ &= (m+1)((m+2)/2) && // \text{ reduzimos } m/2 + 1 \text{ ao mesmo denominador} \\ &= (m+1)((m+1)+1)/2 && // \text{ ora, para qualquer } x, \text{ temos } x+2 = x+1+1 \end{aligned}$$

Portanto, a fórmula a provar vale para  $n = m+1$ .

Portanto, pelo princípio de indução matemática, a fórmula está provada para todo  $k \geq 1$ .

### PROBLEMA 4 [COM SOLUÇÃO]:

Pelo exame do algoritmo da Torre de Hanói (Exemplo 3), concluímos que as equações de recorrência são:

$$T(n) = T(n-1) + 1 + T(n-1) = 2T(n-1) + 1 \quad \text{caso } n > 1 \quad (1)$$

$$T(n) = 1 \quad \text{caso } n = 1 \quad (2)$$

Prove é que a solução para as equações acima é

$$T(n) = 2^n - 1 \quad (3)$$

--- \*\* \* Cubra abaixo e resolva sozinho\* \* \* ---

RESPOSTA: Prova por indução matemática:

*Passo base ( $n=1$ ):*

Para  $n=1$ , a equação (2) produz 1, e a tese (3) produz o mesmo valor:  $2^1 - 1 = 2 - 1 = 1$ .

*Hipótese Indutiva ( $n = m$ , onde  $m$  é um qualquer natural):*

Assumamos que, para  $m$  um qualquer natural, a tese vale, isto é:

$$T(m) = 2^m - 1 \quad (4)$$

*Passo indutivo ( $n=m+1$ ):*

$$\begin{aligned} T(m+1) &= T(m+1-1) + 1 + T(m+1-1) && // \text{ pelo exame do algoritmo, ou de (1)} \\ &= 2T(m) + 1 \\ &= 2 \times (2^m - 1) + 1 && (\text{por (4)}) \\ &= 2^{m+1} - 2 + 1 \\ &= 2^{m+1} - 1 \end{aligned}$$

Portanto, (3) também vale para  $m+1$ .

Conclusão: o teorema está provado, pelo Princípio da Indução Matemática

PROBLEMA 5 [COM SOLUÇÃO]:

Pode você vislumbrar a fórmula fechada para a soma dos cubos dos  $n$  primeiros naturais  $(1,2,3,\dots)$ ? Isto é, para  $S(n) = 1^3 + 2^3 + 3^3 + \dots + n^3$ ? E pode prová-la?

--- \*\* Cubra abaixo e resolva sozinho\* \*\* ---

Depois de alguns experimentos, formulamos a conjectura de que a soma dos cubos dos  $n$  primeiros naturais é

$$S(n) = n^2(n+1)^2 / 4 \quad (1)$$

*Passo base ( $n=1$ ):* (1) é válida porque seu lado esquerdo é 1 (por constatação direta) e seu lado direito também é 1, pois  $1^2(1+1)^2 / 4 = 1 \times 4 / 4 = 1$ .

*Hipótese Indutiva ( $n = k$ ):* suponhamos que (1) é válida para  $n = k$ . Isto é,

$$S(k) = k^2(k+1)^2 / 4 \quad (2)$$

*Passo indutivo ( $n = k+1$ ):*

$$\begin{aligned} S(k+1) &= \dots = S(k) + (k+1)^3 && (\text{aplicação da definição de } S, \text{ e ajuntamento de parcelas de soma}). \\ \therefore S(k+1) &= [k^2(k+1)^2 / 4] + (k+1)^3 && (\text{pela hipótese indutiva, (2)}) \\ \therefore S(k+1) &= [k^2(k+1)^2 + 4(k+1)^3] / 4 && (\text{reduzimos tudo ao mesmo denominador}) \\ \therefore S(k+1) &= (k+1)^2 [k^2 + 4(k+1)] / 4 && (\text{pusemos o fator } (k+1)^2 \text{ em evidência}) \\ \therefore S(k+1) &= (k+1)^2 (k^2 + 4k + 4) / 4 \\ \therefore S(k+1) &= (k+1)^2 (k+2)^2 / 4 = (k+1)^2 [(k+1) + 1]^2 / 4 \\ \therefore &\text{a suposição que (1) é válida para } n = k \text{ implica que também é válida para } n = k+1 \end{aligned}$$

Portanto, pelo Princípio de Indução Matemática, (1) está provada.

PROBLEMA 6:

Tente usar o P.I.M. Simples (ou Fraca), acima visto, para provar que, para todo  $n \geq 2$ ,  $n$  é um número primo ou é um produto de números primos.

--- \*\* Cubra abaixo e resolva sozinho\* \*\* ---

RESPOSTA: O P.I.M. Simples não basta para a prova porque, na hipótese indutiva, você supôs que a propriedade vale para  $k-1$ . Depois, na etapa indutiva, no subcaso em que  $n$  não é primo mas sim um produto de primos, você chamou este produto de  $k = a.b$ , depois você chegou a provar que  $a, b$  têm que estar no intervalo fechado  $[2, k-1]$ , mas não pode usar a hipótese indutiva porque ela só se refere a  $k-1$ , e  $a, b$  podem ser menores que isto.

Este problema foi proposto somente com o objetivo de mostrar que, às vezes, você precisa de um princípio de indução mais completo e forte, baseado em supor que muito mais coisas são verdadeiras abaixo de  $n$ . Espere, e verá este problema resolvido no Exemplo 11, abaixo.

### 3.3. Provas pelo Princípio de Indução Matemática Completa (ou Forte)

**Princípio de Indução Matemática Completa** (ou Forte) (P.I.M.C. versão I):

Seja  $P$  uma proposição definida nos inteiros não negativos. Se pudermos provar que,

- (i) para  $k$  dados inteiros não negativo  $n_0, n_0+1, \dots, n_0+k-1$ , então as  $k$  proposições  $P(n_0), P(n_0+1), \dots, P(n_0+k-1)$  são verdadeiras; e
  - (ii) para qualquer inteiro  $n \geq n_0+k$ , a suposição de que as preposições  $P(n-1), P(n-2), \dots, P(n-k)$  são verdadeiras implicará que a preposição  $P(n)$  também é verdadeira,
- então concluímos que a proposição  $P(n)$  é verdade para *todo* inteiro  $n \geq n_0$ .

#### EXEMPLO 11:

Seja  $\{a_n\}$  é a sequência definida recursivamente por  $a_1 = 1, a_2 = 4, a_3 = 9$ , e  $a_{n+1} = 3a_n - 3a_{n-1} + a_{n-2}$  para todo  $n \geq 3$ . Usando o Princípio de Indução Matemática Completa, prove que  $a_n = n^2$ .

RESPOSTA:

- (i) Temos  $n_0 = 1$  e  $k = 3$ .

Para  $n = n_0 = 1$ , aplicando a fórmula  $P(n) = n^2$ , temos  $P(1) = 1^2 = 1$ , que coincide com  $a_1 = 1$ ;

para  $n = n_0 + 1 = 2$ , aplicando a fórmula  $P(n) = n^2$ , temos  $P(2) = 2^2 = 4$ , que coincide com  $a_2 = 4$ ;

para  $n = n_0 + k - 1 = 3$ , aplicando a fórmula  $P(n) = n^2$ , temos  $P(3) = 3^2 = 9$ , que coincide com  $a_3 = 9$ ;

(ii) para qualquer inteiro  $n \geq n_0 + k = 4$ , a suposição de que as preposições  $P(n-1), P(n-2), \dots, P(n-k)$  são verdadeiras implicará que a preposição  $P(n)$  também é verdadeira, porque  $P(n) = 3a_{n-1} - 3a_{n-2} + a_{n-3} = 3(n-1)^2 - 3(n-2)^2 + (n-3)^2 = 3n^2 - 6n + 3 - 3n^2 + 12n - 12 + n^2 - 6n + 9 = n^2$

Então, pelo P.I.M.C. I, concluímos que a proposição  $P(n)$  é verdade para todo inteiro  $n \geq 1$ .

#### **Princípio de Indução Matemática Completa** (ou Forte) (P.I.M.C. **versão II**):

Seja  $P$  uma proposição definida nos inteiros não negativos. Se pudermos provar que,

- (i) para um dado inteiro não negativo  $n_0$ , a proposições  $P(n_0)$  é verdadeira; e
  - (ii) para qualquer inteiro  $n > n_0$ , a suposição de que todas as preposições aplicadas aos números entre  $n_0$  e  $n-1$  [isto é, todas  $P(n_0), P(n_0+1), P(n_0+2), \dots, P(n-1)$ ] são verdadeiras implicará que a preposição  $P(n)$  também é verdadeira,
- então concluímos que a proposição  $P(n)$  é verdade para *todo* inteiro  $n \geq n_0$ .

#### EXEMPLO 12:

Prove que é verdadeira a proposição  $P(n)$ : "para todo  $n \geq 2$ ,  $n$  é um número primo ou  $n$  é um produto de números primos"

RESPOSTA:

(*passo base*) ( $n=2$ ):  $P(2)$  é verdadeira, porque 2 é primo.

(*hipótese indutiva*): Assumamos que, para todo  $2 \leq r \leq k-1$ ,  $P(r)$  é verdadeira.

(*passo indutivo*) ( $n=k$ ): Analisemos  $P(k)$ :

Caso 1,  $k$  é primo: então  $P(k)$  será verdadeira;

Caso 2,  $k$  não é primo: Como  $k$  não é primo, então pode ser escrito como o produto  $k=a.b$ , onde  $2 \leq a \leq k-1$  e  $2 \leq b \leq k-1$ . Portanto, a hipótese indutiva se aplica tanto a  $a$  como a  $b$ , de modo que tanto  $a$  como  $b$  são (cada um) primo ou produto de primos. Portanto,  $k=1.b$  será um produto de [pelo menos dois] primos. Logo,  $P(k)$  é verdadeira.

Os casos 1 e 2 esgotam todas as possibilidades, portanto  $P(k)$  é verdadeira.

(conclusão): Portanto, pelo princípio da Indução Matemática Completa,  $P(n)$  é verdadeira. C.Q.D.

#### EXEMPLO 13:

Seja  $P(n)$  a afirmativa " $n$  pode ser escrito como a soma de distintas potências de 2"

RESPOSTA:

$P(1)$  é verdade, uma vez que  $1 = 2^0$ .

Assuma que  $P(j)$  é verdadeira para todo inteiro positivo  $j$ , onde  $1 \leq j \leq k$ , isto é, podemos escrever  $j = 2^{p_1} + 2^{p_2} + 2^{p_3} + \dots + 2^{p_t}$ , onde as potências  $p_1 < p_2 < p_3 < \dots < p_t$ . Agora considere  $k+1$ . Temos dois casos:

Caso 1:  $k+1$  é par. Então  $k+1 = 2j$  para algum  $1 \leq j \leq k$  e assim, pela hipótese indutiva,  $k+1 = 2(2^{p_1} + 2^{p_2} + 2^{p_3} + \dots + 2^{p_t})$ , onde todas as potências ainda são distintas; e

Caso 2:  $k+1$  é ímpar. Então  $k$  é par e, pela hipótese indutiva, podemos escrever  $k = 2^{p_1} + 2^{p_2} + 2^{p_3} + \dots + 2^{p_t}$ , onde  $1 \leq p_1 < p_2 < p_3 < \dots < p_t$ . (todas as potências têm valor  $\geq 1$ , uma vez que  $k$  é par). Mas então  $1+k = 2^0 + 2^{p_1} + 2^{p_2} + 2^{p_3} + \dots + 2^{p_t}$ , e todas as potências são diferentes.

Portanto, temos

- (i)  $P(1)$

- (ii)  $P(1) \wedge P(2) \wedge P(3) \rightarrow P(k+1)$ .

Assim, pelo P.I.M. Completa,  $P(n)$  é verdadeira para todo inteiro positivo  $n$ .

#### EXEMPLO 14:

Prove que a propriedade  $P(n)$  definida como "qualquer inteiro positivo  $n$  maior ou igual a 8 pode ser representado como a soma de números 3 e números 5."

RESPOSTA:

*Passo Base ( $n=8$ ):* Ora,  $8 = 3+5$ , portanto  $P(8)$  é verdadeira.

*Hipótese indutiva ( $n=k$ ):* Suponhamos que para qualquer  $r$  tal que  $8 \leq r \leq k$ ,  $P(r)$  é verdadeira, isto é,  $r$  é a soma de números 3 e números 5..

*Passo indutivo ( $n=k+1$ ):*

Caso  $n=9$ :  $P(n)$  vale porque  $9 = 3+3+3$

Caso  $n=10$ :  $P(n)$  vale porque  $10 = 5+5$

Caso  $n \geq 11$ : Seja  $n=k+3$  com  $k \geq 8$ . Pela hipótese indutiva,  $P(k)$  vale, isto é  $k$  é uma soma de números 3 e de números 5. Portanto, somando-se 3 a esta soma, teremos que  $P(n)$  também vale.

Estes são todos os casos possíveis e, neles,  $P(n)$  sempre valeu.

Portanto, pelo P.I.M.C., está provado o que queríamos provar.

## **Problemas sobre toda a Unidade:**

PROBLEMA 7: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 2n$ . Use indução para provar a fórmula fechada  $T(n) = 1n^2 + 1n + 1$ .

PROBLEMA 8: Para  $n = 0$  temos  $T(n) = -1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 2n$ . Use indução para provar a fórmula fechada  $T(n) = n^2 + n - 1$ .

PROBLEMA 9: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 2n - 2$ . Use indução para provar a fórmula fechada  $T(n) = n^2 - n + 1$ .

PROBLEMA 10: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) - 2n + 2$ . Use indução para provar a fórmula fechada  $T(n) = -n^2 + n + 1$ .

PROBLEMA 11: Para  $n = 0$  temos  $T(n) = -1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 2n - 2$ . Use indução para provar a fórmula fechada  $T(n) = n^2 - n - 1$ .

PROBLEMA 12: Para  $n = 0$  temos  $T(n) = -1$  e para  $n > 0$  temos  $T(n) = T(n-1) - 2n + 2$ . Use indução para provar a fórmula fechada  $T(n) = -n^2 + n - 1$ .

PROBLEMA 13: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 3n^2 - 1n + 1$ . Use indução para provar a fórmula fechada  $T(n) = n^3 + n^2 + n + 1$ .

PROBLEMA 14: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 6n^2 - 4n + 2$ . Use indução para provar a fórmula fechada  $T(n) = 2n^3 + n^2 + n + 1$ .

PROBLEMA 15: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 3n^2 + 1n + 0$ . Use indução para provar a fórmula fechada  $T(n) = n^3 + 2n^2 + n + 1$ .

PROBLEMA 16: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 3n^2 - 1n + 2$ . Use indução para provar a fórmula fechada  $T(n) = n^3 + n^2 + 2n + 1$ .

PROBLEMA 17: Para  $n = 0$  temos  $T(n) = 2$  e para  $n > 0$  temos  $T(n) = T(n-1) + 3n^2 - 1n + 1$ . Use indução para provar a fórmula fechada  $T(n) = n^3 + n^2 + n + 2$ .

PROBLEMA 18: Para  $n = 0$  temos  $T(n) = 1$  e para  $n > 0$  temos  $T(n) = T(n-1) + 9n^2 - 7n + 3$ . Use indução para provar a fórmula fechada  $T(n) = 3n^3 + n^2 + n + 1$ .

Se você quiser uma boa e diferente explicação, veja a videoaula :

<http://www.youtube.com/watch?v=2Z6ztPCddAg&list=PL9A14AAD8392362DA&index=3>. Para você treinar ainda melhor, recomendamos a Lista de Exercícios sobre Sequências e Indução Matemática, Prof. Loureiro, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE4.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE4.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE4\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE4_Solucao.pdf).

## **Recapitulando a unidade**

Ótimo, você já concluiu a unidade III, já chegou quase à metade da disciplina. Parabéns, não desista nunca, persevere, esforce-se cada vez mais para vencer com honestidade, garra e competência, seja um vencedor! Se você foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter aprendido a modelar os problemas de Matemática e de programação através de equações recorrentes, depois aprendido a formar uma conjectura para uma fórmula fechada que as resolva, depois aprendido a provar essa conjectura por Indução Matemática (quer Simples ou Completa), com toda precisão e rigor. Essas coisas são muito interessantes e importantes. Importantes porque há um fundo de verdade no dito "*até que você bem aprenda a encontrar equações recorrentes para resolver seus problemas, você não terá aprendido a bem programar. E até que você bem aprenda a provar por Indução Matemática as fórmulas fechadas que conjecturar para suas equações recorrentes, você não terá aprendido a discernir se seus programas são ou não corretos, e a provar isto.*"

Aqui, nós dois concentramo-nos em estudar o raciocínio *indutivo*. Na próxima unidade, a IV, vamos juntamente nos concentrar no raciocínio *dedutivo*, que se baseia na lógica para, partindo de axiomas e de teoremas já demonstrados, e usando regras de inferência da lógica, chega a conclusões lógicas. Estudaremos e treinaremos com vários métodos para provas dedutivas. Será divertido agora, será importante e útil depois.

## UNIDADE IV

# 4. PROVAS DEDUTIVAS

Já dissemos que Deus nos deu duas formas básicas de raciocínio: o indutivo e o dedutivo. Na unidade anterior (III) estudamos o indutivo, agora estudaremos o dedutivo. Uma dedução baseia-se na Lógica Matemática, em axiomas, e em um (ou mais) dos teoremas já demonstrados; e, usando um são e completo de regras de inferência da Lógica, chega a conclusões (Por exemplo: "todos os homens tem peso não negativo; Juca é um homem; logo, Juca tem peso não negativo."). Se raciocinarmos de forma informal (portanto com riscos de imprecisão e ambiguidade) e sem cuidados, isto pode levar a erros, tanto na vida informal como, particularmente, nas provas da Matemática e das demais ciências exatas.

**Nosso objetivo nesta unidade** é que você passe a dominar os principais métodos de prova dedutiva formal, de tal modo que, ao final da unidade, você, usando os rigores da Matemática e da Lógica, a cada necessidade saiba provar tudo que precisar provar dedutivamente, sabendo escolher e usar um método que melhor se aplique ao caso (ou saiba criticar, aceitando ou recusando provas já apresentadas).

*Sempre vamos repetir: Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, **cada semana dedicando 4 a 8 horas para estudar este livro.***

### Conteúdo desta unidade:

- 4.1. INTRODUÇÃO. Definição de Prova (ou Demonstração) Matemática:
- 4.2. DESEMPANHANDO AS DEFINIÇÕES (Começando a Prova)
- 4.3. PROVANDO/ DISPROVANDO AFIRMAÇÕES UNIVERSAIS "SE-ENTÃO" ("Se  $P$ , então  $Q$ ")
  - 4.3.1. Provas Diretas; Divisão em Casos; Exaustão; Generalização de um Elemento Específico, mas Escolhido Arbitrariamente
  - 4.3.2. Provas Indiretas; Contra-Exemplo; Contradição e Redução ao Absurdo; Contrapositivo
- 4.4. PROVAS "SE- E- SOMENTE- SE"
- 4.5. PROVANDO PROPOSIÇÕES EXISTENCIAIS
  - 4.5.1. Achando Exemplo ("Adivinhando" o Elemento)
  - 4.5.2. Prova Construtiva de Existência
  - 4.5.3. Prova Não- Construtiva de Existência
- 4.6. QUE SIGNIFICA "BEM DEFINIDO"?
- 4.7. O PRINCÍPIO DAS CASAS DE POMBOS
- 4.8. ERROS COMUNS NAS [pseudo] "PROVAS"



Se você quiser ver o assunto mais explicada e profundamente, não precisará de mais que os livros textos da ementa da disciplina. Se quiser ainda mais, veja, em português: [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_3MetodosDeProva.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_3MetodosDeProva.pdf) (Antonio Alfredo Ferreira Loureiro); <http://www.ic.unicamp.br/~anamaria/cursos/MC348/2010-2/livro-apost-03.pdf> e <http://www.sbm.org.br/docs/coloquios/SU-2.08.pdf> (mais completo, é um livro com 106 páginas). Em inglês, são considerados clássicos e devem poder ser encontrados nas bibliotecas dos cursos de Matemática: Cupillari, Antonella. *The Nuts and Bolts of Proofs*; Franklin, James; Daoud, Albert. *Proof in Mathematics: An Introduction*; Pólya, George. *Mathematics and Plausible Reasoning: Patterns of Plausible Inference*; Solow, Daniel. *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes* (muitos dos seus exercícios estão resolvidos, na internet); Velleman, Daniel. *How to Prove It: A Structured Approach*. Para treinamento, recomendamos ver algumas das dezenas das mais elegantes provas da História, em <http://www.cut-the-knot.org/proofs/>, começando pelas dezenas classificadas como simples. Leia, estude, e aprenda; depois de dois dias tente fazer as provas sozinho, depois compare com as provas dos grandes mestres. Ao escrever esta unidade, além dos livros textos e dos acima citados, também nos baseamos, parcialmente, em *How To Write Proofs*, <http://zimmer.csufresno.edu/~larryc/proofs/proofs.html> (Larry W. Cusick), curto mas instrutivo.



## 4.1. INTRODUÇÃO (Definição de Prova (ou Demonstração) Matemática)

As provas são o coração da Matemática. Você deve ser capaz de bem ler, entender, checar-avaliar, e escrever provas matemáticas.

• Dados um conjunto  $A$  de sentenças tidas como verdades (axiomáticas ou já provadas) e dada uma nova assertiva,  $S$ , então uma **prova (ou demonstração) matemática** de  $S$  é um argumento (possível de ser inspecionado sequencialmente, e isso em tempo finito, portanto um argumento de comprimento finito) que você apresenta de que  $S$  é consequência lógica de  $A$ , sendo o argumento por você apresentado tão preciso e rigoroso que qualquer outro matemático, depois de escrutiná-lo com rigor, possa ficar completamente convencido da sua correteza. Isto é, **a estrutura básica de uma prova é uma sequência de declarações, cada um sendo:**

**A) uma verdade axiomática** ou **uma verdade já provada (um teorema)**, ou algo assumido como **hipótese**; OU

**B) uma consequência** (clara e precisamente justificada por regras de inferência da Lógica e da Matemática) de declarações já estabelecidas como verdade.

• As provas podem ser **informais** (sem formalismo específico, mas com toda precisão matemática e lógica, o que geralmente nos basta) ou **formais** (com um formalismo específico e um sistema *formal* de raciocínio através de manipulação de *símbolos*, mostrando-se todas as minúcias da aplicação desse sistema na prova, o que pode ficar pesado).

• [Raramente, pode-se incluir notas de rodapé de esclarecimento nos pontos mais difíceis da prova; ainda mais raramente, pode-se inserir algum exemplo; mas ambas essas coisas devem ser usadas com muita frugalidade e com muito cuidado para não confundir mais que clarificar. Não fazem parte da prova, que, sem essas ajudas, deve poder ser entendida com precisão por alguém mais experiente.]

### Regras gerais para escrever uma prova

Escreva a palavra **"TEOREMA:"** e o preciso enunciado da assertiva a ser provada.

Marque o início da prova com a palavra **"PROVA:"**.

Escreva a prova de tal forma que ela seja auto-contida.

Isto inclui identificar cada variável usada na prova juntamente com o seu tipo. Exemplos: "Seja  $x$  um número real maior que 2"; "Suponha que  $m$  e  $n$  são inteiros." Isto é similar a declarar cada variável e seu tipo, numa linguagem de programação.

**Escreva a provas em linguagem natural (mas precisa), usando sentenças completas, anotando ao lado a mais curta possível justificativa clara de cada passo não trivial que foi tomado.** Como estamos apenas sendo precisos, mas informais, repetimos: você não precisa anotar nada nos passos mais triviais, e, nos demais, não precisa escrever coisas longas e superdetalhadas, como fez na unidade II, seção 3, nas provas formais usando o sistema de dedução natural. Por exemplo, você deve pensar em sua cabeça, mas não precisa escrever assim "isto decorre das linhas 10 e 20, usando a regra de inferência natural chamada de *modus ponens*, instanciando-se a variável<sub>1</sub> com a variável<sub>101</sub>, e ... e a variável<sub>10</sub> com a variável<sub>110</sub>, depois usando a lei de De Morgan aplicada sobre a sub-expressão fulana". Você deve ter feito isso em sua cabeça, com todo rigor, para não cometer enganos fatais, mas, na apresentação da prova precisa mas informal, basta anotar algo bem mais curto, tal como "consequência das linhas 10 e 20", ou "por transformações algébricas", ou "contradiz a hipótese". Isto é suficiente.

EXEMPLO 1: (Por enquanto, basta você entender perfeitamente e checar com rigor se cada declaração na sequência da prova abaixo é do tipo (A) ou (B), acima. Daqui a uma semana, tente fazer esta prova, sozinho, mais 2 provas do mesmo tipo)

**TEOREMA:** A raiz quadrada de 2 é um número irracional { Um número real é chamado racional se ele pode ser expressa como a razão de dois inteiros,  $p/q$ , e de irracional caso contrário }

**PROVA:** Vamos representar a raiz quadrada de 2 por  $s$ . Então, por definição,  $s$  satisfaz a equação  $s^2 = 2$

Suponhamos que  $s$  é um número racional. Então, poderemos escrever

$$s = p/q,$$

onde  $p$  e  $q$  são um par de números inteiros. De fato, dividindo-se pelo maior múltiplo comum se for necessário, podemos até mesmo assumir  $p$  e  $q$  são primos entre si {não possuem nenhum múltiplo em comum, exceto 1}.

Se agora substituirmos isto na primeira equação então, após usarmos um pouco de algebrismo, obtemos a equação

$$p^2 = 2q^2$$

Mas agora, pelo teorema fundamental da aritmética { "todo inteiro positivo tem uma representação única como um produto de números primos" }, 2 tem que aparecer na fatoração em primos do número  $p^2$  (uma vez que aparece no mesmo número,  $2q^2$ ).

Desde que 2 é um número primo, 2 também tem que aparecer na fatoração em primos do número p {entendeu? exemplo: o inteiro  $36 = 2 \times 18$  e  $\sqrt{36} = 2 \times 3$ }.

Mas, então,  $2^2$  apareceria na fatoração em primos de  $p^2$ , e, portanto, em  $2q^2$ .

Ao dividir tudo por 2, vemos que 2 está na fatoração em primos de  $q^2$ .

Como antes (com  $p^2$ ), podemos agora concluir que 2 é um fator primo de q.

Mas agora temos que p e q compartilham um fator primo, ou seja 2.

Isso viola o nosso pressuposto acima (veja se você pode encontrá-lo) de que p e q são primos entre si (não têm em comum outro múltiplo além de 1). Portanto, a hipótese inicial "Suponhamos que s é um número racional", levando a uma contradição, o teorema está provado.

## 4.2. DESEMARANHANDO AS DEFINIÇÕES (Começando a Prova)

Uma das perguntas mais frequentes de quem está dando os primeiros passos na arte de descobrir (e escrever) boas provas matemáticas é: "Como faço para começar?" A resposta geralmente é simples: "Comece *desemaranhando* as definições", isto é "**comece escrutinando o enunciado com lupa e entendendo com precisão todas as definições envolvidas.**"

Primeiro, examine com lupa e entenda perfeitamente bem o que você está sendo solicitado a provar. Será que isso envolve um termo que foi definido (na aula, ou no livro texto, ou no enunciado do problema)? Escreva a definição, escreva mesmo. Estude-a, entenda-a, e descubra e escreva em rascunho, com breves justificativas, dois exemplos que a satisfazem e dois que não a satisfazem. E sobre os pressupostos implicitamente requeridos pelo problema? Será que eles envolvem definições? Se assim for, leia-as em local confiável e escreva-as em suas próprias palavras e cheque, alhures, se as entendeu bem. Ademais, às vezes, há teoremas que são relevantes para o seu problema. Se assim for, leia-os em local confiável e escreva-os em suas próprias palavras e cheque, onde haja autoridade e competência, se os entendeu bem. Não tenha medo de anotar tudo o que sabe sobre o que você está tentando provar.

EXEMPLO 2 (máximo divisor comum) (baseado em L. Cusick): Prove o teorema abaixo

TEOREMA (RASCUNHO INICIAL): "A operação binária mdc é associativa".

DESEMARANHANDO AS DEFINIÇÕES:

Que é mdc? mdc é a abreviação de *máximo divisor comum*, assim definido:

"O máximo divisor de dois inteiros não negativos, a e b (não sendo ambos iguais a 0) é o número  $d = \text{mdc}(a,b)$  que satisfaz duas propriedades: (1) d divide a e divide b, e (2) se d' é um outro qualquer número inteiro não negativo que divide a e divide b, temos que  $d \geq d'$ . Podemos pensar do mdc como uma operação binária."

Que significa dizer que a operação binária mdc é associativa? Significa que, para quaisquer três inteiros não negativos (no máximo um deles podendo ser 0) a, b, c,  $\text{mdc}(\text{mdc}(a,b),c) = \text{mdc}(a,\text{mdc}(b,c))$ .

Formalmente, é isto que você quer provar:

TEOREMA:  $\forall a,b,c \in \mathbb{Z}^+$  (no máximo um desses números sendo 0),  $\text{mdc}(\text{mdc}(a,b),c) = \text{mdc}(a,\text{mdc}(b,c))$ . //Note:  $\mathbb{Z}^+$  inclui 0

Agora está mais claro, não é? Mas ainda falta a prova propriamente dita.

PROVA (RASCUNHO INICIAL): Você se pergunta: "O que temos *mesmo* que provar? Os mdc's do lado esquerdo e do lado direito da equação parecem tão 'iguais' ... Que estratégia usar? Por onde começar?"

Bem, chame de d um dos lados da equação. Escolhamos o lado esquerdo. Seja  $d = \text{mdc}(\text{mdc}(a,b),c)$ . O que isso significa? Significa (1) d divide  $\text{mdc}(a,b)$  e c, e (2) se d' é um qualquer outro número inteiro não negativo que divide  $\text{mdc}(a,b)$  e c, temos que  $d \geq d'$ .

Temos que provar que  $d = \text{mdc}(a,\text{mdc}(b,c))$ , que é o lado direito da equação. O que isso significa? Temos de provar duas coisas: (1) d divide a e  $\text{mdc}(b,c)$ ; e (2) se d' é um outro inteiro não negativo que divide a e  $\text{mdc}(b,c)$ , temos que  $d \geq d'$ . Basta que provemos (1), depois (2):

(1) Uma vez que d divide  $\text{mdc}(a,b)$ , d tem que dividir a e dividir b. Sabemos que d divide c, então d tem que dividir  $\text{mdc}(b,c)$ . Assim, a primeira parte está provada (foi fácil).

(2) Agora, suponha que outro número, d', divide a e divide  $\text{mdc}(b,c)$ . Então, d' divide b e divide c, por isso d' deve dividir  $\text{mdc}(a,b)$ , também. Mas, então, por nossa suposição,  $d \geq d'$ . E isso é tudo que você precisava provar.

Agora, passe a limpo a prova, apresente-a mais concisa mas igualmente precisa e fácil de entender, como seu professor e os formados do seu curso apreciam:

PROVA: Seja  $d = \text{mdc}(\text{mdc}(a,b),c)$ . Então d divide a, b e c, e, portanto, divide a e  $\text{mdc}(b,c)$ . Se outro número, d', divide a e  $\text{mdc}(b,c)$ , então d' tem que dividir  $\text{mdc}(a,b)$  e c, mas, por definição de mdc,  $d \geq d'$ . Assim,  $d = \text{mdc}(a,\text{mdc}(b,c))$ .

EXERCÍCIO 1, para você resolver por si mesmo (mínimo múltiplo comum) (baseado em L. Cusick):  
 O mínimo múltiplo comum de dois inteiros positivos  $a$  e  $b$ ,  $\text{mmc}(a,b)$ , é o inteiro positivo  $m$  que satisfaz as duas condições: (1)  $a$  divide  $m$ , e  $b$  divide  $m$ ; e (2) se  $m'$  é um outro número inteiro positivo tal que  $a$  divide  $m'$ , e  $b$  divide  $m'$ , então  $m < m'$ . Prove que a operação binária mínimo múltiplo comum é associativa, ou seja, para quaisquer três números inteiros positivos  $a$ ,  $b$ ,  $c$ , temos que  $\text{mmc}(\text{mmc}(a,b),c) = \text{mmc}(a,\text{mmc}(b,c))$ .

### 4.3. PROVANDO/ DISPROVANDO AFIRMAÇÕES UNIVERSAIS "SE-ENTÃO" ("Se $P$ , então $Q$ ")

A maioria das afirmações já provadas (ou a serem provadas) em Matemática são universais, da forma:

Afirmação:  $\forall x \in D$ : se  $P(x)$  então  $Q(x)$

Tais afirmações universais "se-então" são provadas por três métodos:

- Método da *prova direta*;
- Método da *generalização de um elemento específico, mas escolhido arbitrariamente*; e
- Método da *exaustão* (no caso do domínio  $D$  ser finito ou existir um número finito de seus elementos,  $x$ , que satisfazem  $P(x)$ ).

#### 4.3.1. Provas Diretas

Muitas vezes podemos **provar uma afirmação matemática diretamente a partir das precisas definições dos termos da sentença (basta isso)**.

EXEMPLO 3 (baseado em AAF Loureiro): Defina par e defina ímpar. Depois, prove diretamente

- (a) 0 é par.
- (b) -301 é ímpar.
- (c) Se  $a$  e  $b$  são inteiros,  $6a^2b$  é par. Por que?
- (d) Se  $a$  e  $b$  são inteiros, então  $10a + 8b + 1$  é ímpar. Por que?
- (e) Qualquer que seja um número inteiro, ou ele é par ou ele é ímpar.

RESPOSTAS:

$n$  é par significa que existe um inteiro  $m$  tal que  $n=2m$

$n$  é ímpar significa que existe um inteiro  $m$  tal que  $n=2m+1$

- (a) 0 é par?  
Sim, 0 é par porque  $0 = 2 \times 0$ .
- (b) -301 é ímpar?  
Sim, -301 é ímpar porque  $-301 = 2(-151) + 1 = -302 + 1$
- (c) Se  $a$  e  $b$  são inteiros,  $6a^2b$  é par? Por que?  
Sim, porque  $6a^2b = 2(3a^2b)$
- (d) Se  $a$  e  $b$  são inteiros, então  $10a + 8b + 1$  é ímpar. Por que?  
Sim.  $10a + 8b + 1 = 2(5a + 4b) + 1$ .
- (e) Todo número inteiro é par ou é ímpar.

Um modo de provar é notar que as definições equivalem a dizer que par é divisível por 2 e que ímpar não o é. Como as definições são cada uma o complemento da outra, segue-se que o "ou" entre elas tem que ser verdade.

Outra prova, embora envolvendo análise de casos (melhor explicada em 3.3.1.2.):

Por definição, você pode mover-se através dos números inteiros seja adicionando 1 para chegar ao próximo ou subtraindo 1 para chegar ao anterior.

Suponha que existe um inteiro  $n$  que não é par nem é ímpar. Já que sabemos que existem pares e ímpares inteiros, podemos repetidamente subtrair 1 de  $n$  até chegar ao primeiro  $j$  inteiro tal que  $j$  é par ou ímpar e  $j+1$  nem é par nem é ímpar.

Caso 1: Suponha-se que  $j$  é par, expressável na forma  $j = 2k$ . Então, pela adição de 1, temos  $j+1 = 2k + 1$ , o que é ímpar. Esta é uma contradição, pois assumimos que os inteiros de  $j+1$  até  $n$  não são ímpar nem par.

Caso 2: Suponha-se que  $j$  é ímpar, expressável na forma  $j = 2k+1$ . Então, pela adição de 1, temos  $j+1 = 2k + 2 = 2(k+1)$  o que é par. Esta é uma contradição, pois assumimos que os inteiros de  $j+1$  até  $n$  não são par nem ímpar.

Portanto, todos os casos possíveis tendo levado a uma contradição, a suposição “Suponha que existe um inteiro  $n$  que não é par nem é ímpar” é supor algo impossível, portanto o teorema está provado.

#### EXEMPLO 4:

Defina primo e número composto: Depois, prove diretamente o ...

TEOREMA: Para qualquer natural  $n \geq 2$ , segue-se que ou  $n$  é um número primo ou  $n$  é um número composto (este “ou ... ou” é um ou-excludente “ $\oplus$ ”) (Dizer que um natural  $n$  é *primo* significa que  $n > 1$  e  $n$  só tem divisão inteira por 1 e por si mesmo. Um natural  $n$  é *composto* se não for primo [isto é, se tem divisão inteira por algum inteiro diferente de 1 e diferente de si mesmo].

#### PROVA:

A afirmação é verdadeira porque as definições de primo e de composto são a negação uma da outra.

#### **4.3.1.1. Generalização de um Elemento Específico, mas Escolhido Arbitrariamente**

Para mostrar que  $\forall x \in D: P(x) \rightarrow Q(x)$  suponha que  $x$  é um elemento específico (mas escolhido arbitrariamente) no domínio  $D$  e mostre que  $x$  satisfaz a propriedade  $P(x) \rightarrow Q(x)$

#### EXEMPLO 5: Prove o

TEOREMA: a soma de dois quaisquer números racionais é um número racional.

#### PROVA:

Suponha que  $r, s$  sejam dois números racionais específicos, mas escolhidos arbitrariamente.

Deve-se mostrar quer  $r+s$  é racional.

Pela definição de racional, seja  $r = a/b$  e seja  $s = c/d$ , para inteiros  $a, b, c, d$ , onde  $b \neq 0$  e  $d \neq 0$ .

Por substituição e álgebra temos que:

$$r + s = (a/b) + (c/d) = (ad + bc) / (bd)$$

Se  $p = ad + bc$  e  $q = bd$ , então  $p, q$  são inteiros porque o conjunto dos números inteiros é “fechado” para as operações de soma e multiplicação, sendo que  $q \neq 0$ .

Logo,

$$r + s = p/q, \text{ onde } p, q \text{ são inteiros, com } q \neq 0.$$

ou seja, a soma de  $r + s$  é um número racional.

Q.E.D. (“*Quod Erat Demonstrandum*”), ou seja, C.Q.D. (“*Como Queríamos Demonstrar*”)

#### EXEMPLO 6 (transitividade da divisibilidade):

A notação  $d|n$  deve ser lida como “ $d$  divide  $n$ ”. Simbolicamente,

se  $n, d$  são inteiros e se  $d \neq 0$ , então

$$d|n \Leftrightarrow \exists \text{ um inteiro } k \text{ tal que } n = dk$$

Agora, prove

TEOREMA: Para todos inteiros  $a, b, c$ , se  $a$  divide  $b$ , e  $b$  divide  $c$ , então  $a$  divide  $c$ .

#### PROVA:

Suponha que  $a, b, c$  são inteiros [específicos mas escolhidos arbitrariamente] tais que  $a$  divide  $b$ , e  $b$  divide  $c$ .

Deve-se mostrar que  $a$  divide  $c$ .

Pela definição de divisibilidade,  $b = ar$ ,  $c = bs$  para inteiros  $r, s$ .

Por substituição e álgebra temos que:

$$c = bs = (ar)s = a(rs)$$

Seja  $k = rs$ , onde  $k$  é um número inteiro.

Logo,

$$c = ak,$$

ou seja,  $a$  divide  $c$  pela definição de divisibilidade. C.Q.D.

#### EXEMPLO 7 (Divisibilidade e números primos):

TEOREMA: Todo inteiro  $n > 1$  é divisível por um número primo.

#### PROVA:

Suponha que  $n$  é um inteiro [específico, mas escolhido arbitrariamente] maior que 1.

Deve-se mostrar que existe um número primo que divide  $n$ .

Se  $n$  é primo então  $n$  é divisível por um número primo, ou seja, ele próprio, e a prova chega ao fim. Se  $n$  não é primo então  $n$  é composto, e pela definição de número composto

$$n = r_0 s_0, \text{ onde } r_0 \text{ e } s_0 \text{ são inteiros, e}$$

$$1 < r_0 < n \text{ e } 1 < s_0 < n.$$

Pela definição de divisibilidade,  $r_0|n$ . Se  $r_0$  é primo, então  $r_0$  é um número primo que divide  $n$  e a prova chega ao fim. Se  $r_0$  não é primo então  $r_0$  é composto, e, pela definição de número composto,

$$r_0 = r_1 s_1, \text{ onde } r_1, s_1 \text{ são inteiros, e } 1 < r_1 < r_0 \text{ e } 1 < s_1 < r_0.$$

Pela definição de divisibilidade,  $r_1|r_0$ . Mas nós já sabemos que  $r_0|n$  e, pela transitividade da divisibilidade,

$r_1 | n$ . Se  $r_1$  é primo, então  $r_1$  é um número primo que divide  $n$  e a prova chega ao fim. Se  $r_1$  não é primo então podemos continuar o processo acima fatorando  $r_1$  como  $r_1 = r_2 s_2$

Pode-se continuar este processo, obtendo fatores sucessivos de  $n$  até se obter um fator primo. Este processo tem um número finito de passos já que cada novo fator é menor que o anterior (que é menor que  $n$ ) e maior que 1, e existem menos que  $n$  inteiros entre 1 e  $n$ . Desta forma, obtém-se a sequência:

$$r_0, r_1, r_2, \dots, r_k,$$

onde  $k \geq 0$ ,  $1 < r_k < r_{k-1} < \dots < r_1 < r_0 < n$ , e  $r_i | n$  para cada  $i = 0; 1; 2; \dots; k$ . A condição para término é que  $r_k$  seja primo, ou seja,  $r^k$  é um número primo que divide  $n$ . C.Q.D.

EXEMPLO 8:

TEOREMA: O número  $100\dots 01$  (que começa e termina com o algarismo "1", e tem  $3n-1$  zeros entre eles, onde  $n$  é um inteiro maior que 0) é composto (i.é, não primo)

PROVA:

$$100\dots 01 = 10^{3n} + 1, \text{ onde o inteiro } n > 0$$

$$= (10^n)^3 + 1 = (10^n + 1)(10^{2n} - 10^n + 1) \quad // \text{ Confira! Multiplique! E note que cada um dos dois fatores é maior que 1}$$

que é um número composto. C.Q.D.

EXEMPLO 9: TEOREMA: Se duas funções um- a- um podem ser compostas, então a sua composição também é um- a- um (Ver definições na unidade I. A função  $f: X \rightarrow Y$  é chamada de um- a- um se, para qualquer par  $a, b$  em  $X$  tal que  $f(a) = f(b)$ , então  $a = b$ . Além disso, se  $f: X \rightarrow Y$  e  $g: Y \rightarrow Z$  são duas funções, então a composição  $gf: X \rightarrow Z$  é a função definida por  $gf(a) = g(f(a))$ , para cada  $a$  em  $X$ . Note que a composição  $gf$  somente é definida se o domínio de  $f$  está contido no contradomínio de  $g$ ).

PROVA: Sejam  $a$  e  $b$  em  $X$  e assumamos que  $gf(a) = gf(b)$ . Assim,  $g(f(a)) = g(f(b))$ , e uma vez que  $g$  é um- a- um, então podemos concluir que  $f(a) = f(b)$ . Finalmente, uma vez que  $f$  é um- a- um, então  $a = b$ .

EXEMPLO 10: TEOREMA: Se  $r_1$  e  $r_2$  são duas diferentes raízes do polinômio  $p(x) = x^2 + bx + c$ , então  $r_1 + r_2 = -b$  e  $r_1 r_2 = c$ .

PROVA:

Todo polinômio  $p(x)$  de grau  $n$  e de raízes  $r_1, r_2, r_n$  pode ser fatorado assim  $p(x) = (x-r_1)(x-r_2)\dots(x-r_n)$ . No presente caso,  $n = 2$  e temos

$$p(x) = (x - r_1)(x - r_2)$$

Se expandirmos o lado direito temos

$$p(x) = x^2 - (r_1 + r_2)x + r_1 r_2$$

Comparando os coeficientes acima com os de  $p(x) = x^2 + bx + c$ , obtemos que  $r_1 + r_2 = -b$  e  $r_1 r_2 = c$ .

EXERCÍCIO 2: Prove que "Se  $a$  é um número inteiro, múltiplo de 4, então  $a$  é a diferença entre dois quadrados perfeitos."

EXERCÍCIO 3: Prove que "Se  $a$  e  $b$  são números reais, então  $a^2 + b^2 \geq 2ab$ ."

EXERCÍCIO 4: Prove que "A soma de dois números racionais é um número racional."

EXERCÍCIO 5: Prove que "Se duas funções onto podem ser compostas então a composição é onto (ou sobrejetiva)." (A função  $f: X \rightarrow Y$  é dita onto (ou sobrejetiva) se para cada  $b$  em  $Y$ , há um elemento  $a$  em  $X$  tal que  $f(a) = b$ )

EXERCÍCIO 6: Prove que "Se  $r_1, r_2, r_3$ , são três distintas raízes do polinômio  $p(x) = x^3 + bx^2 + cx + d$ , então  $r_1 r_2 + r_1 r_3 + r_2 r_3 = c$ ."

EXERCÍCIO 7: Se  $a$  divide  $b$  e  $a$  divide  $c$ , então  $a$  divide  $(b + c)$ . ( $a, b$ , e  $c$  são números positivos naturais).

### **Regras para Escrever Provas de Afirmações Universais "Se-Então" ("Se $P$ , então $Q$ ")**

A maioria dos teoremas que você deseja provar estão (explícita ou implicitamente) na forma "Se  $P$ , então  $Q$ ". No Exemplo 6 (transitividade da divisibilidade),  $P$  foi " $a$  divide  $b$ , e  $b$  divide  $c$ " e  $Q$  foi " $a$  divide  $c$ ". Esta é a forma mais usual de um teorema (embora possa estar disfarçada). Uma prova direta deve ser vista como um fluxo de implicações começando com  $P$  e terminando com  $Q$ :

$$P \rightarrow \dots \rightarrow Q$$

A maioria das provas são (e devem ser) provas diretas. Sempre tente primeiro prova direta, a menos que você tenha uma boa razão para não fazer isso.

As regras são:

**1. Expresse a afirmação a ser provada na forma  $\forall x \in D, P(x) \rightarrow Q(x)$ . [Geralmente feito mentalmente]**

2. Suponha que  $x$  é um elemento específico de  $D$  mas escolhido arbitrariamente, para o qual a hipótese  $P(x)$  é  $V$ . [Normalmente escreve-se “Suponha  $x \in D$  e  $P(x)$ ”]
4. Mostre que  $Q(x)$  é  $V$ , para isso usando definições, fatos (teoremas) já provados anteriormente, axiomas, e regras de inferência lógica.

EXEMPLO 11:

Prove: Se a soma de dois números inteiros é par, então a sua diferença também o é. Formalmente:  $\forall m, n \in \mathbf{Z}$ , se  $m + n$  é par então  $m - n$  é par.

PROVA:

Suponha  $m$  e  $n$  são inteiros [específicos mas escolhidos arbitrariamente] tais que  $m + n$  é par.

Deve-se mostrar que  $m - n$  é par.

Pela definição de par,  $m + n = 2k$  para algum inteiro  $k$ .

Subtraindo  $n$  dos dois lados,  $m$  pode ser expresso como:  $m = 2k - n$ . A diferença entre  $m$  e  $n$  pode ser expressa como

$$\begin{aligned} m - n &= (2k - n) - n && \text{substituindo } m \text{ pelo valor acima} \\ &= 2k - 2n \\ &= 2(k - n) \end{aligned}$$

O segundo fator,  $k - n$ , é um número inteiro que, multiplicado pelo primeiro fator, 2, resulta no lado direito da equação ser um inteiro par. C.Q.D.

EXEMPLO 12:

TEOREMA: Todo inteiro ímpar é a diferença de dois quadrados perfeitos (um quadrado perfeito é o quadrado de um inteiro).

PROVA: Suponha  $2a+1$  é um número inteiro ímpar, então

$$2a + 1 = (a + 1)^2 - a^2 \quad // \text{ Confira, faça as operações!}$$

#### 4.3.1.2. Divisão em Casos

EXEMPLO 13:

Prove que dois números inteiros consecutivos quaisquer têm paridades (par, ímpar) opostas.

PROVA:

Suponha que dois inteiros consecutivos [específicos mas escolhidos arbitrariamente] são dados. Chame esses números de  $m$  e de  $m + 1$ .

Deve-se mostrar que um dos números  $m$  e  $m + 1$  é par e o outro é ímpar.

Pela definição de par e ímpar, tem-se que ou  $m$  é par ou  $m$  é ímpar.

Vamos quebrar a prova em dois casos dependendo se  $m$  é par ou se é ímpar (note: estes são todos os casos possíveis).

Caso 1 ( $m$  é par): Neste caso,  $m = 2k$  para algum inteiro  $k$  e, assim,  $m+1 = 2k + 1$ , o que é ímpar [Pela definição de ímpar.] Neste caso um dos números do par ( $m$ ,  $m + 1$ ) é par e o outro é ímpar.

Caso 2 ( $m$  é ímpar): Neste caso,  $m = 2k + 1$  para algum inteiro  $k$  e, assim,  $m+1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$ . Como  $m+1$  é igual ao dobro de um número, então  $m + 1$  é par. Também neste caso, um dos números do par ( $m$ ,  $m + 1$ ) é par e o outro é ímpar.

Pode-se concluir que, independente de qual caso ocorre para valores específicos de  $m$  e de  $m + 1$  que são escolhidos, um dos números do par ( $m$  e  $m + 1$ ) é par e outro é ímpar.

EXEMPLO 14:

Prove que o quadrado de qualquer inteiro ímpar tem a forma  $8m+1$  para algum inteiro  $m$ .

PROVA:

Suponha que  $n$  é um inteiro ímpar [específico, mas escolhido arbitrariamente]. Lembra do teorema do quociente-resto “dado qualquer inteiro Dividendo e inteiro positivo Divisor, existem inteiros Quociente e Resto tais que  $\text{Dividendo} = \text{Divisor} \times \text{Quociente} + \text{Resto}$ , e  $0 \leq \text{Resto} < \text{Divisor}$ ”? Por esse teorema,  $n$  pode ser escrito em uma das seguintes formas:

$$4q \text{ ou } 4q+1 \text{ ou } 4q+2 \text{ ou } 4q+3,$$

para algum inteiro  $q$ . Como  $n$  é ímpar e  $4q$  e  $4q+2$  são pares,  $n$  deve se restringir a uma das duas formas:  $4q+1$  ou  $4q+3$ .

Caso 1 ( $n = 4q+1$ ): [Deve-se achar um inteiro  $m$  tal que  $n^2 = 8m + 1$ .] Como  $n = 4q + 1$ , temos

$$n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1$$

Caso 2 ( $n = 4q+3$ ): [Deve-se achar um inteiro  $m$  tal que  $n^2 = 8m + 1$ .] Como  $n = 4q + 3$ , temos

$$n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1$$

(note: estes são todos os casos possíveis).

#### 4.3.1.3. Exaustão (no Caso do domínio $D$ ser Finito ou Existir um Número Finito de Seus Elementos $x$ que

Satisfazem  $P(x)$ )

EXEMPLO 15:

Prove

$\forall n \in \mathbf{Z}$ , se  $n$  é par e  $4 \leq n \leq 30$ , então  $n$  pode ser escrito como a soma de dois números primos.

RESPOSTA:

$$\begin{array}{llll} 4 = 2 + 2 & 6 = 3 + 3 & 8 = 3 + 5 & 10 = 5 + 5 \\ 12 = 5 + 7 & 14 = 11 + 3 & 16 = 5 + 11 & 18 = 7 + 11 \\ 20 = 7 + 13 & 22 = 5 + 17 & 24 = 5 + 19 & 26 = 7 + 19 \\ 28 = 11 + 17 & 30 = 11 + 19 & & \end{array}$$

O método de prova por exaustão é pouco prático porque em geral os domínios não são finitos ou são muito grandes.

## 4.3.2. Provas Indiretas

### 4.3.2.1. Disprovando (por Contra-Exemplo)

Para provar a falsidade de uma afirmação da forma

$$\forall x \in D: P(x) \rightarrow Q(x)$$

ache um valor de  $x$  em  $D$  para o qual  $P(x)$  é V e  $Q(x)$  é F. O elemento  $x$  é chamado de contra-exemplo.

EXEMPLO 16:

Negue a seguinte afirmação:

$$\forall a, b \in \mathbf{R}: (a^2 = b^2) \rightarrow (a = b):$$

Contra-exemplo:

$$a = 1 \text{ e } b = -1.$$

EXEMPLO 17:

Seja

$$p(n) = n^2 + n + 41.$$

Prove ou disprove a conjectura:

$$\forall n \in \mathbf{N}: p(n) \text{ é primo.}$$

RESPOSTA:

$n$	0	1	-1	2	-2	3	-3	...	39	-39	40
$p(n) = n^2 + n + 41$	41 primo	43 primo	41 primo	47 primo	43 primo	53 primo	47 primo	...	1601 primo	1523 primo	1681 = $41^2$ : NÃO primo

Nos 79 cálculos para 0, 1, -1, ..., 39, -39, você achou resultados que eram primos, e você estava dizendo "Isto não pode ser somente uma coincidência! A conjectura deve ser verdadeira!" Mas não é:  $p(40) = 1681$ , que não é primo, pois é o quadrado de 41.

EXEMPLO 18:

Em 1769, Euler [pronuncie *óiler*] conjecturou que  $a^4 + b^4 + c^4 = d^4$  não tinha solução no conjunto dos números inteiros positivos. Consegue você achar um contra-exemplo para disprovar isso?

RESPOSTA:

Em 1987, Noam Elkies achou que

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

EXEMPLO 19:

Consegue você disprovar a conjectura

$$313(x^3 + y^3) = z^3 \text{ não tem solução no conjunto } \mathbf{Z}^+.$$

RESPOSTA:

Falso, mas o menor contra-exemplo tem mais de 1000 dígitos.

O computador mais "poderoso" não seria capaz de obter essa solução usando a estratégia baseada na força bruta.

Por que é importante resolver esse problema?

Achar soluções para tais equações é importante na área de curvas elípticas. Curvas elípticas são importantes no estudo de fatoração de inteiros "grandes". E fatorar inteiros "grandes" é importante no estudo de

sistemas criptográficos. E criptografia é a base de todos os sistemas seguros de comunicação atualmente!

#### EXEMPLO 20:

Prove ou disprove a seguinte afirmação:

Para todos inteiros não nulos  $a, b$ , se  $a|b$  e se  $b|a$  então  $a = b$ .

“DISPROVA”:

Suponha que  $a, b$  são inteiros não nulos [específicos mas escolhidos arbitrariamente] tais que  $a|b$  e  $b|a$ . Pela definição de divisibilidade, as condições  $b|a$  e  $a|b$  podem ser escritas como

$$b = ma \quad \text{e} \quad a = nb \quad \text{para inteiros não nulos } m, n.$$

Por substituição e álgebra temos que:

$$b = ma = m(nb) = (mn)b$$

Já que  $b|a$  e  $b \neq 0$ , tem-se que

$$1 = mn$$

Em outras palavras,  $m$  e  $n$  são divisores de 1. Mas os únicos divisores de 1 são 1 e -1. Logo,  $m$  e  $n$  são ambos 1 ou são ambos -1. Se  $m = n = 1$  então  $a = b = 1$ . Mas se  $m = n = -1$  então  $b = -a$  e assim  $a \neq b$ . Está disprovada a conjectura.

#### **Famosas Conjecturas sem contra-exemplo, mas ainda sem prova:**

- *Último Teorema de Fermat*: não existem inteiros positivos  $x, y, z$  e  $n \geq 3$  tais que  $x^n + y^n = z^n$ .
- *Conjectura de Goldbach*: todo inteiro maior que 2 pode ser representado como uma soma de dois primos.
- Há infinitos primos  $p$  tais que  $p+2$  também é primo.
- A Hipótese de Riemann: longa para ser aqui explicada, leia-a na internet.

#### **4.3.2.2. Prova por Contradição, Redução ao Absurdo**

Princípios (para provar “ $\forall x \in D$ ; se  $P(x)$  então  $Q(x)$ ”):

1. Suponha que a afirmação a ser provada é falsa (isto é, existe um elemento  $x \in D$  tal que  $P(x) \wedge \neg Q(x)$ .)
2. Mostre que essa suposição leva logicamente a uma contradição (isto é, leva a  $P(x) \wedge \neg P(x)$ , ou leva a  $Q(x) \wedge \neg Q(x)$ )
3. Conclua que a afirmação a ser provada é verdadeira.

EXEMPLO 21: TEOREMA: não existe um inteiro que seja o maior de todos.

PROVA (por contradição):

Suponha que exista um inteiro  $N$  que seja o maior de todos.

Tem-se então que  $N \geq n$  para cada inteiro  $n$ . Seja  $M = N + 1$ , que é um inteiro já que é a soma de inteiros. Tem-se também que  $M > N$  já que  $M = N + 1$ .

Logo,  $M$  é um inteiro que é maior que o maior dos inteiros,  $N$ , o que é uma contradição. [Essa contradição mostra que a suposição é falsa e, desta forma, o teorema é verdadeiro.]

EXEMPLO 22: TEOREMA: para todo  $n$ , se  $n^2$  é par então  $n$  é par

PROVA (por contradição):

Suponha que não.

Suponha que exista um inteiro  $n$  tal que  $n^2$  é par e  $n$  é ímpar. [Deve-se chegar a uma contradição.]

Já que  $n$  é ímpar,  $nn$  é também ímpar.

Isto contradiz a suposição que  $n^2$  é par. [Logo, a suposição é falsa e o teorema está provado.]

EXEMPLO 23: TEOREMA:  $\sqrt{2}$  é irracional.

PROVA (por contradição) (já foi vista, em 3.1. – Introdução):

Representemos  $\sqrt{2}$  por  $s$ , de modo que  $s = \sqrt{2}$ , ou seja,  $s^2 = 2$ .

Se  $s$  fosse um número racional, então poderíamos escrever  $s = p/q$  (onde  $p$  e  $q$  são inteiros positivos sem divisores em comum, exceto 1)

Portanto, a equação se transformaria em  $p^2 = 2q^2$ .

O teorema fundamental da aritmética garante que todo inteiro positivo tem uma representação única como o produto de números primos, portanto 2 tem que aparecer na fatoração do número  $p^2$  em primos (uma vez que aparece na expressão  $2q^2$ ). Então  $p^2$  é par. Então  $p$  é par. Desde que 2 é um número primo, 2 tem que aparecer na fatoração do número  $p$  em primos. Mas, então,  $2^2$  apareceria na fatoração de  $p^2$  em primos, e, portanto, em  $2q^2$ . Divisão por 2 faria ver que 2 também tem que aparecer na fatoração de  $q^2$  em primos. Como antes (com  $p^2$ ) poderíamos concluir que 2 é um fator primo de  $q$ . Mas agora teríamos  $p$  e  $q$  compartilhando um fator primo, ou seja, 2. Isso violaria o nosso pressuposto acima de que  $p$  e  $q$  não têm divisor em comum além de 1.



EXEMPLO 24: TEOREMA (de Euclides, cerca de 300 aC!): "há um infinito número de primos."

PROVA (por contradição) (será repetida, em VII - Teoria dos Números):

Suponhamos que o número de primos é finito e igual ao natural  $r$ . Chamemos o maior deles de  $p_r$ .

Ordenemos e demos nomes a todos os primos, assim:  $p_1=2 < p_2=3 < \dots < p_r$ . Seja  $P = (p_1 p_2 \dots p_r) + 1$ .

Evidentemente  $P$  é maior que cada um dos números primos. Temos duas possibilidades e veremos que ambas levam a uma contradição: Caso  $P$  seja primo, então, por ser maior que cada  $p_1, \dots, p_r$ , é um *novo* primo (diferente de  $p_1, \dots, p_r$ ), o que contradiz nossa suposição. E, caso  $P$  seja primo, <sup>tem que ser fatorável por primos (menores que ele mesmo)</sup>, e chamemos de  $p$  um dos primos (há pelo menos um deles) que divide  $P$ ; então,  $p$  não pode ser igual ao primo  $p_1=2$  porque o

primeiro múltiplo de  $p_1$  maior ou igual a  $P$  é  $(P-1)+p_1$ ; idem para o primo  $p_2$ ; e para o primo  $p_3$ ; ...; e para o primo  $p_r$ . (Isto é,  $P = (p_1 p_2 \dots p_r) + 1$  não é fatorável por nenhum dos primos  $p_1, \dots, p_r$ ). Portanto,  $p$  tem que ser um *novo* primo (diferente de  $p_1, \dots, p_r$ ), o que contradiz nossa suposição. Como as 2 hipóteses possíveis levaram a contradições da suposição, esta tem que ser falsa, impossível. Portanto, o número de primos é infinito. CQD.

(É um erro comum pensar que esta prova diz que o natural  $P = p_1 p_2 \dots p_r + 1$  é primo. [Um contra-exemplo é  $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ , que é divisível por 59. Desafio os, para lhes ajudar a entender melhor, que encontrem outro contra-exemplo, com  $P$  menor]. Na verdade, a prova somente usa o fato que, se  $P$  não for um primo *novo* [diferente de  $p_1, p_2, \dots, p_r$ ], então há um primo *novo* que divide  $P$ ).

Prova por contradição é frequentemente utilizada quando se pretende provar a impossibilidade de algo:

Você assume que é possível, e depois chegará a uma contradição. Nos exemplos abaixo, use essa ideia para provar a impossibilidade de certos tipos de soluções para algumas equações.

EXEMPLO 25: TEOREMA: não existem soluções inteiras positivas para a equação diofantina (isto, com soluções apenas nos inteiros)  $x^2 - y^2 = 1$ .

PROVA (por contradição):

Assuma, ao contrário, que há uma solução  $(x, y)$  onde  $x, y$  são inteiros positivos. Se for este o caso, pode-se decompor o lado esquerdo:  $x^2 - y^2 = (x + y)(x - y) = 1$ . Desde que  $x$  e  $y$  são números inteiros, segue-se que ou  $x-y = 1$  e  $x + y = 1$ , ou  $x-y = -1$  e  $x + y = -1$ . No primeiro caso, podemos adicionar as duas equações para obter  $x = 1$  e  $y = 0$ , contradizendo a suposição de que  $x$  e  $y$  são positivos. O segundo caso é semelhante, ficando  $x = -1$  e  $y = 0$ , novamente contradizendo nossa hipótese.

EXEMPLO 26:

Prove que não há soluções de número racionais para a equação  $x^3 + x + 1 = 0$ .

PROVA (Prova por contradição.):

Assuma, ao contrário, que existe um número racional  $p/q$ , em forma reduzida, com  $p$  diferente de zero, que satisfaz a equação. Em seguida, temos  $p^3/q^3 + p/q + 1 = 0$ . Depois de multiplicar cada lado da equação,  $q^3$ , obtemos a equação

$$p^3 + pq^2 + q^3 = 0$$

Há três casos a considerar. (1) Se  $p$  e  $q$  são ambos ímpar, então o lado esquerdo da equação acima é ímpar. Mas 0 não é ímpar, o que nos deixa com uma contradição. (2) Se  $p$  for par e  $q$  for ímpar, então o lado esquerdo é ímpar, uma vez mais uma contradição. (3) Se  $p$  é ímpar e  $q$  é par, temos a mesma contradição. O quarto caso -  $p$  e  $q$  ambos pares - não é possível porque assumimos que  $p/q$  está na forma reduzida. Isso completa a prova.

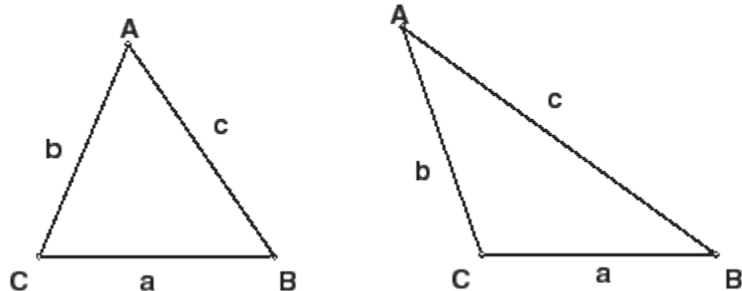
**A Recíproca de um TEOREMA:**

A recíproca de "Se  $P$ , então  $Q$ " é a afirmação "Se  $Q$ , então  $P$ ". Por exemplo, a recíproca de "Se o carro é meu, então é vermelho" é "Se o carro é vermelho, então é meu." Deve ficar claro, a partir deste exemplo, que não há garantia de que o inverso de um teorema (na forma de uma implicação) verdadeira seja verdade. Prova por Contradição é muitas vezes a maneira mais natural para provar a recíproca de um teorema já provado

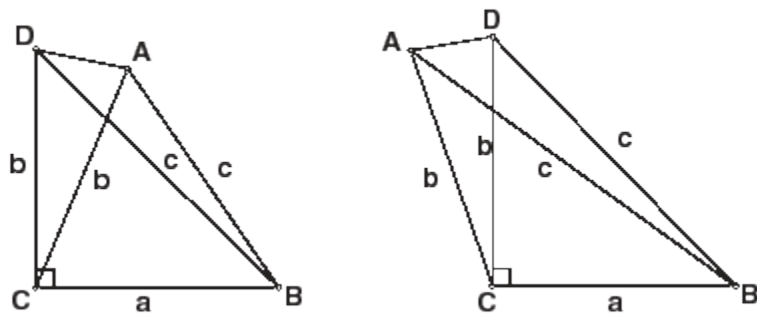
EXEMPLO 27: TEOREMA (recíproco do de Pitágoras): Se os comprimentos  $a, b, c$  (todos eles maiores que 0) dos lados de um triângulo satisfazem a relação  $a^2 + b^2 = c^2$ , então o triângulo é retângulo

PROVA (por contradição):

Suponha que o triângulo não é retângulo. Dê nome aos vértices  $A, B$  e  $C$  como mostrado abaixo (figura esquerda, caso o ângulo de  $C < 90$  graus; figura direita, caso o ângulo de  $C > 90$  graus)



Construa um segmento de reta CD, perpendicular a CB, como mostrado:



Pelo teorema de Pitágoras,  $BD^2 = a^2 + b^2 = c^2$ , portanto  $BD = c$ . Assim, temos triângulos isósceles ACD e ABD. Segue-se que temos ângulos congruentes  $CDA = CAD$ , e  $BDA = DAB$ . Mas isso contradiz as desigualdades aparentes (ver imagem)  $BDA < CDA = CAD < DAB$  (figura à esquerda) ou  $DAB < CAD = CDA < BDA$  (figura à direita).

EXERCÍCIO 8: Prove que a raiz cúbica de 2 é irracional.

EXERCÍCIO 9: Prove que não existem soluções inteiras positivas para a equação diofantina  $x^2 - y^2 = 10$ .

EXERCÍCIO 10: Prove que não há nenhum número racional que seja solução da equação  $x^5 + x^4 + x^3 + x^2 + 1 = 0$ .

EXERCÍCIO 11: Prove que se  $a$  é um número racional e  $b$  é um número irracional, então  $a + b$  é um número irracional

#### 4.3.2.3. Prova por Contrapositivo

Prova por contrapositivo aproveita a equivalência lógica entre " $P$  implica  $Q$ " e " $\text{Não } Q$  implica não  $P$ ". Por exemplo, a afirmação "Se é o meu carro, então é vermelho" é equivalente a "Se o carro não é vermelho, então ele não é meu". Então, provar "Se  $P$ , então  $Q$ " pelo método do contrapositivo significa provar "Se não  $Q$ , então não  $P$ ".

Princípios:

1. **Expresse a afirmação a ser provada na forma**  
 $\forall x \in D; \text{ se } P(x) \text{ então } Q(x)$
2. **Reescreva a afirmação na forma contrapositiva:**  
 $\forall x \in D; \text{ se } \neg Q(x) \text{ então } \neg P(x)$
3. **Prove o contrapositivo por uma prova direta:**
  - (a) Suponha  $x$  um elemento específico, mas escolhido arbitrariamente, de  $D$  tal que  $\neg Q(x)$  seja  $V$ .
  - (b) Mostre que  $\neg P(x)$  é  $V$ .

EXEMPLO 28: TEOREMA: dado qualquer inteiro  $n$ , se  $n^2$  é par então  $n$  é par.

PROVA (pelo contrapositivo): Seja  $n$  um inteiro que não é par. Deve-se mostrar que  $n^2$  não é par.

Sabe-se que o produto de dois números não pares é um número que não é par. Desta forma,  $n^2$  (que é igual ao produto  $nn$ ) não é par. C.Q.D.

EXEMPLO 29: TEOREMA: Dados dois inteiros quaisquer  $x, y$ , se  $x+y$  é par então  $x$  e  $y$  têm mesma paridade. PROVA: A versão contrapositiva deste teorema é "Se  $x$  e  $y$  são dois inteiros com paridade oposta, então a soma deles deve ser ímpar." Assim, assumamos que  $x, y$  têm paridade oposta. Uma vez que um desses inteiros é par e o outro é ímpar, não há nenhuma perda de generalidade em supor que  $x$  é par e  $y$  é ímpar. Assim, há inteiros  $k$  e  $m$  para os quais  $x = 2k$  e  $y = 2m + 1$ . Agora, em seguida, calcula-se a soma  $x + y = 2k + 2m + 1 = 2(k+m) + 1$ , que é um número inteiro ímpar, por definição.

EXERCÍCIO 12: Prove que "para qualquer primo  $p$ , se  $p$  divide  $n^2$  então  $p$  divide  $n$ ".

EXERCÍCIO 13: Prove que "se  $n$  é um inteiro positivo tal que  $n \bmod(4)$  é 2 ou 3, então  $n$  não é um quadrado perfeito."

EXERCÍCIO 14: Prove que "Se  $x$  e  $y$  são dois números inteiros cujo produto é par, então pelo menos um dos dois deve ser par."

EXERCÍCIO 15: Prove que "Se  $x$  e  $y$  são dois números inteiros cujo produto é ímpar, então ambos devem ser ímpar."

EXERCÍCIO 16: Prove que "Se  $n$  é um inteiro positivo tal que  $n \bmod(3) = 2$ , então  $n$  não é um quadrado perfeito."

EXERCÍCIO 17: Prove que "Se  $a$  e  $b$  são números reais tais que o produto  $ab$  é um número irracional, então  $a$  ou  $b$  tem que ser um número irracional."

#### **4.3.2.4. Relação Entre Prova Por Contradição e Prova Por Contraposição**

A diferença entre a prova por contrapositivo e a prova por contradição é sutil. Vamos examinar como os dois métodos de prova funcionam ao tentar provar "Se  $P$ , então  $Q$ ".

Método de contradição: Suponha  $P$  e não  $Q$ , e vá fazendo deduções sequenciais a partir disso, até chegar a algum tipo de contradição.

Método do contrapositivo: Suponha não  $Q$  e prove não  $P$ .

O método do contrapositivo tem a vantagem de que seu objetivo é claro: provar não  $P$ . No método da contradição, seu objetivo é provar uma contradição, mas nem sempre é claro, no início, o que a contradição vai ser.

Vantagens e desvantagens das provas por contrapositivo:

- + É fácil saber qual é a conclusão que deve ser provada: é a negação da hipótese.
- + Não é necessário obter a negação da afirmação.
- Só pode ser usado para afirmações com quantificadores existencial ou universal.

Vantagens e desvantagens das provas por contradição:

- + A prova termina assim que é achada uma contradição.
- A negação da afirmação é mais complexa.
- Pode ser mais difícil achar o caminho da prova.

### **4.4. PROVAS "SE- E- SOMENTE- SE"** (baseadas em Larry W. Cusick)

Muitos teoremas são apresentados na forma " $P$  se- e- somente- se  $Q$ ". Ou, equivalentemente: " $Q$  é condição necessária e suficiente para  $P$ ". Isso significa duas coisas: "Se  $P$ , então  $Q$ " e "Se  $Q$ , então  $P$ ". Então, **para provar um teorema "se- e- somente- se", você deve provar duas implicações: " $P \rightarrow Q$ ", depois " $Q \rightarrow P$ ".**

EXEMPLO 30: TEOREMA: "Se  $a$  é um inteiro, então  $a$  não é divisível por 3 se- e- somente- se  $a^2-1$  é divisível por 3."

PROVA:

- (sentido "**Se**"): Temos de provar " $a$  não é divisível por 3 se  $a^2-1$  não é divisível por 3". Assim, assume-se que 3 divide  $a^2-1 = (a-1)(a+1)$ . Uma vez que 3 é um número primo, 3 deve dividir ou  $(a-1)$  ou  $(a+1)$ . Em ambos os casos, deve ser aparente que 3 não pode dividir  $a$ .

- (sentido "**Somente- se**"): Temos de provar " $a$  não é divisível por 3 somente se  $a^2-1$  é divisível por 3." Isso

significa "Se  $a$  não é divisível por 3, então  $a^2 - 1$  é divisível por 3". Relembremos que, se MaiorOuIgual e Menor são dois inteiros, então existem outros dois números inteiros Quociente e Resto, onde  $0 \leq \text{Resto} < \text{Menor}$ , e tal que  $\text{MaiorOuIgual} = \text{Quociente} \times \text{Menor} + \text{Resto}$ . Por isso, podemos escrever  $a = 3q + r$ , onde  $q, r$  são inteiros e  $r = 0$ , ou 1, ou 2. O nosso pressuposto de que  $a$  não é divisível por 3 implica que  $r$  não pode ser 0. Se  $r = 1$ , então,  $a - 1 = 3q$  e assim, 3 divide  $a^2 - 1 = (a - 1)(a + 1)$ . Um argumento semelhante funciona se  $r = 2$ . C.Q.D.

Às vezes, você pode provar que uma asserção "Se e somente se" sem explicitamente dividir a prova em duas partes. O próximo exemplo ilustra como isso pode ser feito.

EXEMPLO 31 (regra de divisibilidade por 3): TEOREMA: Um inteiro positivo  $n$  é divisível por 3 se, e somente se, a soma dos dígitos de  $n$  é divisível por 3.

PROVA: Suponhamos que  $n$  é um número inteiro positivo cuja representação decimal é  $a_0 a_1 \dots a_k$ . Isto significa que  $n = a_0 + 10a_1 + \dots + 10^k a_k$ . A soma dos dígitos é  $s = a_0 + a_1 + \dots + a_k$ .

Agora,  $n - s = (a_0 + 10a_1 + \dots + 10^k a_k) - (a_0 + a_1 + \dots + a_k) = 9a_1 + 99a_2 + \dots + (99\dots9)a_k$  (onde o último termo tem  $k$  noves). Então, claramente,  $n - s$  é divisível por 3. Segue-se que  $n$  é divisível por 3 se, e somente se,  $s$  é divisível por 3. C.Q.D.

EXERCÍCIO 18: Prove "Se  $a$  é um inteiro, então  $a$  não é divisível por 5 se, e somente se,  $a^4 - 1$  é divisível por 5."

EXERCÍCIO 19: Prove "Para dois inteiros  $a$  e  $b$ ,  $a + b$  é ímpar se, e somente se, exatamente um dos inteiros,  $a$  ou  $b$ , é ímpar."

EXERCÍCIO 20: Prove "Para dois inteiros  $a$  e  $b$ , o produto  $ab$  é par se e somente se pelo menos um dos números inteiros,  $a$  ou  $b$ , é par."

EXERCÍCIO 21: Prove "Um inteiro positivo  $n$  é divisível por 9 se, e somente se, a soma dos dígitos de  $n$  é divisível por 9."

EXERCÍCIO 22: Prove "Um inteiro positivo  $n$  é divisível por 11 se, e somente se, a diferença das somas dos dígitos nas posições pares e ímpares em  $n$  é divisível por 11."

## **4.5. PROVANDO PROPOSIÇÕES EXISTENCIAIS**

Se queremos provar que existe algum elemento  $x$  (não somos obrigados a identificá-lo) num domínio  $D$ , tal que uma certa propriedade  $Q$  seja verdadeira com relação a  $x$  (isto é,  $Q(x) = V$ ), temos os seguintes possíveis métodos de prova:

- (a) Ache/apresente  $x \in D$  que faz  $Q(x)$  verdadeiro.
- (b) Mostre <sup>[isto é, ache e prove a corretude de um algoritmo]</sup> como achar  $x$  que faz  $Q(x)$  verdadeiro. (Isto é chamado de "Método de Prova Construtiva de Existência").

### **4.5.1. Achando Exemplo ("Adivinhando" o Elemento)**

EXEMPLO 32: TEOREMA: Existe pelo menos um inteiro par,  $n$ , que pode ser escrito de duas formas diferentes como a soma de dois números primos.

PROVA: Uma desses  $n$  tem o valor 10, pois  $10 = 5 + 5 = 7 + 3$

EXEMPLO 33: TEOREMA: Sejam  $r$  e  $s$  inteiros. Existe um inteiro  $k$  tal que  $22r + 18s = 2k$ .

PROVA: O inteiro  $k = 11r + 9s$  satisfaz isso, pois  $22r + 18s = 2(11r + 9s) = 2k$

### **4.5.2. Prova Construtiva de Existência**

Para provar que existe um elemento  $x$  num domínio  $D$  tal que uma certa propriedade  $Q$  seja verdadeira com relação a  $x$  (isto é,  $Q(x) = V$ ), mostre [isto é, ache e prove a corretude de um

**algoritmo] como achar x que faz  $Q(x)$  verdadeiro.**

EXEMPLO 34: TEOREMA: "dados os inteiros positivos  $a, b$ , existe um (e somente um) inteiro positivo  $c$  tal que  $c = \text{mdc}(a, b)$ " (mdc foi definido no exemplo 1 de (3.2)).

PROVA: Dados dois inteiros não negativos MaiorOuIgual, Menor (no máximo um deles podendo ser 0), você achou dois teoremas já demonstrados:

se  $\text{Menor} | \text{MaiorOuIgual}$ , então  $\text{mdc}(\text{MaiorOuIgual}, \text{Menor}) = \text{Menor}$ .

se  $\neg (\text{Menor} | \text{MaiorOuIgual})$ , então  $\text{mdc}(\text{MaiorOuIgual}, \text{Menor}) = \text{mdc}(\text{Menor}, \text{MaiorOuIgual} \% \text{Menor})$  // leia "%" como "módulo".

Juntando estes dois teoremas, você terá o algoritmo recursivo

$\text{mdc}(\text{MaiorOuIgual}, \text{Menor}) := \text{SE } \text{MaiorOuIgual} \% \text{Menor} = 0 \text{ ENTÃO } \text{Menor} \text{ SENÃO}$

$\text{mdc}(\text{Menor}, \text{MaiorOuIgual} \% \text{Menor})$

Exemplo:  $\text{mdc}(420, 378) = \text{mdc}(378, 42) = 42$

EXEMPLO 35: TEOREMA: Existem infinitas triplas  $(x, y, z)$  de números inteiros positivos tais que  $x^2 + y^2 = z^2$ .

PROVA: Basta mostrarmos como construir um conjunto infinito de triplas em que  $x^2 + y^2 = z^2$ , mesmo que esse conjunto não inclua algumas triplas com essa propriedade. Começemos com a tripla  $(3, 4, 5)$ . Ela atende à propriedade requerida, pois  $3^2 + 4^2 = 9 + 16 = 25 = 5^2$ . Consideremos agora as triplas da forma  $(3k, 4k, 5k)$ , com  $k$  assumindo qualquer valor inteiro positivo. Ora,  $(3k)^2 + (4k)^2 = 3^2k^2 + 4^2k^2 = (3^2 + 4^2)k^2 = (5^2)k^2 = (5k)^2$ . Portanto, todas as triplas da forma  $(3k, 4k, 5k)$  têm a propriedade desejada. Como há infinitos valores de  $k$ , então há infinitas triplas:  $(3, 4, 5), (6, 8, 10), (9, 12, 15), \dots$ . Note que, apesar de não incluir várias (infinitas) triplas válidas, como  $(5, 12, 13)$ , o conjunto construído é infinito, o que basta para provar o teorema.

EXEMPLO 36 (só para quem já pagou a disciplina Linguagens Formais): TEOREMA: "dado um autômato finito determinístico (AFD) para uma linguagem regular, existe um AFD equivalente e que garantidamente tem o menor número de estados. A demonstração do teorema já é um algoritmo que, executado, vai construindo o autômato minimizado. Ver [http://www.informatik.uni-bremen.de/agbs/lehre/ss05/pi2/hintergrund/minimize\\_dfa.pdf](http://www.informatik.uni-bremen.de/agbs/lehre/ss05/pi2/hintergrund/minimize_dfa.pdf)

### 4.5.3. Prova Não- Construtiva de Existência

(este tipo de prova é mais apropriadamente chamado "prova de <sup>[mera]</sup> existência". Não é o tipo mais importante para a Computação, Engenharia, ciência aplicada em geral)

Consiste em mostrar que:

(a) **A existência de um valor  $x$ , que faz com que  $Q(x)$  seja verdadeira, é garantida por um axioma ou teorema** (mesmo que não dê o valor de  $x$ ); ou

(b) **A suposição de que não existe um valor  $x$  leva a uma contradição.** (Isto é chamado de *prova por contradição* ou de *prova por redução ao absurdo*.)

Desvantagem deste tipo (não construtivo) de prova: pode não dar nenhuma "pista" de como ou onde  $x$  pode ser encontrado, portanto não é muito "útil". Nós (que trabalhamos com Ciência da Computação, com Matemática Computacional e Aplicada, com Engenharia, etc.) buscamos achar e implementar algoritmos que podem ser vistos como provas construtivas, e nos dão respostas objetivas para os problemas, tendo muito maior valor prático.

EXEMPLO 37: TEOREMA: existe um número racional  $z^y$  tal que ambos  $z$  e  $y$  são irracionais.

PROVA: Seja  $x = y = \sqrt{2}$  (porque sabemos que  $\sqrt{2}$  é irracional). Se  $\sqrt{2}^{\sqrt{2}}$  é racional, temos um número racional da forma desejada. Caso contrário, isto é se  $\sqrt{2}^{\sqrt{2}}$  é irracional, seja  $z = \sqrt{2}^{\sqrt{2}}$  e  $y = \sqrt{2}^{\sqrt{2}}$ . Então  $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^2 = 2$ , que é óbvio que é racional.

Note que provamos que há um número racional tal que ambos  $x$  e  $y$  são irracionais. Ou com  $\{x = y = \sqrt{2}\}$  ou com  $\{x = \sqrt{2}^{\sqrt{2}} \text{ e } y = \sqrt{2}\}$ , mas não sabemos qual.

EXERCÍCIO 23: Prove que "existe um número racional  $z^y$  tal que ambos  $z$  e  $y$  são irracionais" usando  $x = \sqrt{2}$  e  $y = \log_2 9$ .

#### 4.5.3.1. Prova de Existência Usando Contradição ou Redução ao Absurdo

EXEMPLO 38: TEOREMA: a equação  $\sin(3x) = x^3 - \pi$  tem solução, isto é, existe algum  $x$  real que a satisfaz.

PROVA 1 (por contradição): Assuma que não tem. Então,  $f(x) = \sin(3x) - x^3 + \pi$  nunca seria 0. Então, a

inversa desta função, isto é,  $g(x) = 1/(\sin(3x) - x^3 + \pi)$ , seria definida para todos os reais. Mas, usando um traçador (plotador) de funções (por exemplo <http://fooplot.com>) você verá que ela não o é para um ponto  $x \in [1.33 \text{ até } 1.34]$ .

PROVA 2 (pelo teorema do valor intermediário): Seja  $f(x) = \sin(3x) - x^3 + \pi$ .  $f(0) = \pi > 0$ ;  $f(2) = -8 + \pi < 0$ ; como a função é contínua no intervalo  $[0 \text{ até } 2]$ , então, pelo teorema do valor intermediário,  $f(x)$  tem uma raiz nesse intervalo.

## 4.6. QUE SIGNIFICA "BEM DEFINIDO"?

Cedo ou tarde, você terá que provar que algo é "bem definido". Então, o que isto significa?

"Em Matemática, uma expressão está bem definida se é inequívoca (inambígua) e seus objetos são independentes de sua representação. Mais simplesmente, isso significa que um enunciado matemático faz sentido e é definido.

Em particular, **uma função é bem definida se dá o mesmo resultado quando a forma (a maneira em que é apresentada), mas não o valor de entrada for alterada.**

O termo bem definido é também usado para indicar que uma afirmação lógica não é ambígua. ... Por exemplo, uma função que é bem definida terá o mesmo valor tanto quando 0,5 é a entrada como quando  $1/2$  é a entrada. Um exemplo de uma "função", que não está bem definida é " $f(x)$  = o primeiro dígito que aparece em  $x$ ". Para esta função,  $f(0,5) = 0$ , mas  $f(1/2) = 1$ . A "função", tal como está, de modo nenhum pode ser considerada uma verdadeira função, uma vez que uma função deve ter exatamente uma saída para uma determinada entrada.

(Um grupo é um conjunto de elementos associados a uma operação que combina dois elementos quaisquer para formar um terceiro, e faz isso obedecendo os axiomas de grupo: associatividade, identidade, e elementos inversos. Por exemplo, o grupo de simetrias de um quadrado; o grupo das permutações.) Em Teoria dos Grupos, o termo bem definido é frequentemente utilizado quando se lida com co-conjuntos (conjuntos complementares), onde uma função em um grupo quociente pode ser definida em termos de um representante do co-conjunto. Então, a saída da função deve ser independente de que co-conjunto representativo foi escolhido. Por exemplo, considere o grupo dos números inteiros módulo 2. Uma vez que 4 e 6 são congruentes módulo 2, uma função definida sobre os inteiros módulo 2 deve dar a mesma saída quando a entrada é de 6 que dá quando a entrada é de 4.

Uma função que não está bem definida não é a mesma coisa de uma função que não está definida. Por exemplo, se  $f(x) = 1/x$ , então  $f(0)$  é indefinido, mas isso não tem nada a ver com a questão de saber se  $f(x) = 1/x$  é bem definida. Ela o é, o problema, simplesmente, é que 0 não pertence ao domínio da função." <http://en.wikipedia.org/wiki/Well-defined>

EXEMPLO 39: TEOREMA: Adição módulo  $m$  é **bem definida**, isto é, se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $(a + c) \equiv (b + d) \pmod{m}$ . [Não continue antes de rever a definição de módulo e de congruência]

ESTRATÉGIA. O que temos que provar?  $(a + c) \equiv (b + d) \pmod{m}$ . O que isso significa? Isso significa que temos de mostrar que há um inteiro  $k$  tal que  $a + c = (b + d) + km$ . O que estamos assumindo?  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ . Isto significa que há inteiros  $k_1$  e  $k_2$  tais que  $a = b + mk_1$  e  $c = d + k_2m$ . O que vamos fazer? Podemos adicionar essas duas últimas equações em conjunto para obter:  $(a + c) = (b + d) + (k_1 + k_2)m$ . Então, se fizermos  $k = k_1 + k_2$ , teremos o que queremos. Ah, agora enxergamos o que devemos fazer, então escrevamos a prova.

PROVA. Pela nossa hipótese, existem inteiros  $k_1$  e  $k_2$  tais que  $a = b + mk_1$  e  $c = d + k_2m$ . A adição dessas duas equações em conjunto nos dá  $(a + c) = (b + d) + (k_1 + k_2)m$ , o que, por definição, significa  $(a + c) \equiv (b + d) \pmod{m}$ .

EXEMPLO 40 (Não É Bem Definido): Usando aritmética modular, considere a operação de divisão. Para inteiros faz sentido falar sobre  $x/2$  quando  $x$  é par. Será que isto faz sentido em módulo 2? Por exemplo, seja  $x = 2$ . Na aritmética mod (2), o "número"  $2/2$  deve ser a única solução ( $y$ ) para a equação  $2y \equiv 2 \pmod{2}$ . Mas, como você pode ver, qualquer inteiro  $y$  irá satisfazer esta equação. Isto é,  $x/2$ , não é bem definido.

EXEMPLO 41 (Funções Módulo  $m$ ): Nos dois exemplos anteriores, nós olhamos para os "números" módulo  $m$ . Neste sistema existem apenas  $m$  "números", representada por  $0, 1, \dots, m-1$ . Usualmente se dá a este conjunto o nome de  $\mathbb{Z}_m$ . Por exemplo,  $\mathbb{Z}_4$  tem quatro elementos, representados por  $0, 1, 2, 3$ . Lembre-se,

todos os outros inteiros são apenas outros nomes para estes 4. Por exemplo,  $13 = 1 \pmod{4}$ , e  $-13 = 3 \pmod{4}$ .

TEOREMA: A função  $f: \mathbf{Z}_4 \rightarrow \mathbf{Z}_4$ , dada por  $f(x) = 2x + 1$  é bem definida.

ESTRATÉGIA: É fácil de ver que  $f(0) = 1$ ,  $f(1) = 3$ ,  $f(2) = 5 = 1 \pmod{4}$ , e  $f(3) = 7 = 3 \pmod{4}$ . O que precisamos provar? Precisamos provar que  $f(a) = f(b) \pmod{4}$ . Isto é,  $f(a) - f(b)$  é divisível por 4, isto é,  $(2a + 1) - (2b + 1) = 2(a - b)$  é divisível por 4. Qual é a nossa suposição? Estamos assumindo  $a = b \pmod{4}$ . O que isso significa? Isso significa que  $a - b$  é divisível por 4. Podemos ver imediatamente que a nossa suposição implica  $2(a - b)$  é divisível por 4, que é o que queríamos.

PROVA: Se  $a = b \pmod{m}$ , então  $(a - b)$  é divisível por 4. Daí, também o é  $(2a + 1) - (2b + 1)$ , que é  $f(a) = f(b) \pmod{m}$ .

EXERCÍCIO 24: Prove que: a multiplicação é bem definida em aritmética módulo  $m$ . Isto é, se  $a = b \pmod{m}$  e  $c = d \pmod{m}$ , segue-se que  $(ac) = (bd) \pmod{m}$ .

EXERCÍCIO 25: Prove que: a função  $f: \mathbf{Z}_m \rightarrow \mathbf{Z}_m$  dada por  $f(x) = x^2 + x$  é bem definida.

## 4.7. O PRINCÍPIO DAS CASAS DE POMBOS [ou Princípio das Gavetas de Dirichlet]

O princípio das casas de pombos afirma que **se tivermos  $n$  casas para acomodar  $n+1$  pombos, então podemos afirmar que existe uma casa com pelo menos 2 pombos.** ...

Com este princípio tão simples é possível resolver vários exercícios curiosos. Vejamos alguns exemplos:

EXEMPLO 42) Se tivermos um grupo de 13 pessoas, então com certeza 2 delas fazem aniversário no mesmo mês. E, se o grupo aumentar para 32 pessoas, podemos afirmar também que existem no mínimo duas pessoas que fazem aniversário no mesmo dia.

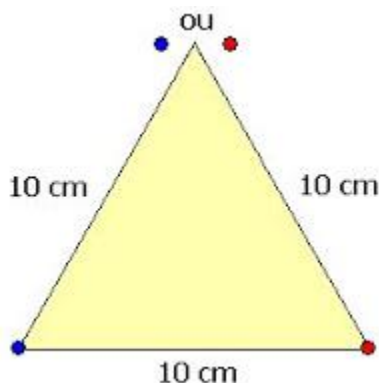
Solução: Pelo princípio das casas de pombos, se houvesse mais pessoas (13) do que meses (12) é certo que pelo menos duas pessoas terão nascido no mesmo mês e a explicação é análoga para o dia do mês.

EXEMPLO 43) Dado um cubo de lado 2 cm, mostre que ao marcarmos 9 pontos em seu interior, a distância entre pelo menos dois deles é menor ou igual a  $\sqrt{3}$  cm.

Solução: Para cada par de faces opostas desse cubo, tomamos um plano paralelo a essas faces e que passa pelo centro do cubo. Serão 3 planos que dividirão esse cubo em 8 cubinhos de arestas 1 cm. Cada um desses cubinhos será uma casa dos pombos e como temos 9 pontos, então pelo menos 2 pontos estarão no interior ou na superfície um cubo de aresta 1 cm. Sendo a maior distância entre dois pontos quaisquer num desses cubinhos igual ao comprimento da diagonal do cubo, ou seja,  $\sqrt{3}$  cm, temos o resultado desejado.

EXEMPLO 44) Todos os pontos de um plano são pintados de azul ou vermelho. Prove que podemos encontrar dois pontos da mesma cor que distam exatamente 10 cm.

Solução: Basta imaginarmos um triângulo equilátero de lado igual a 10 cm. Como são duas cores (casas) e três pontos (pombos). Pelo princípio da casa dos pombos teremos dois da mesma cor.



...

EXERCÍCIO 26: Quantos estudantes devem haver em uma turma para garantir que pelo menos dois estudantes possuam a mesma nota no exame final, se a nota do exame varia de 0 a 100? (As notas são

dadas em números inteiros).

**EXERCÍCIO 27:** Mostre que entre um grupo de 5 inteiros (não necessariamente consecutivos) existem dois com o mesmo resto quando divididos por 4.

**EXERCÍCIO 28:** Seja  $d$  um inteiro positivo. Mostre que entre qualquer grupo de  $d+1$  inteiros (não necessariamente consecutivos) existem dois com exatamente o mesmo resto quando divididos por  $d$ .  
<http://fatosmatematicos.blogspot.com.br/2009/07/o-principio-da-casa-dos-pombos.html>

**EXEMPLO 45: TEOREMA**

(<http://www.ufv.ca/media/assets/mathematics/putnamclub/Pigeonhole+Problems.pdf>): Entre os positivos inteiros  $N$ , existem dois deles, cuja diferença é divisível por  $N-1$ .

**PROVA:** Sejam  $a_1, a_2, \dots, a_N$  os números. Para cada  $a_i$ , seja  $r_i$  o resto que resulta da divisão de  $a_i$  por  $N-1$ . (Assim,  $r_i \equiv a_i \pmod{N-1}$  e  $r_i$  pode assumir apenas os valores  $0, 1, \dots, N-2$ ). Existem  $N-1$  valores possíveis para cada  $r_i$ , mas existem  $N$   $r_i$ 's. Assim, pelo princípio das casinhas de pombo, tem de haver dois dos  $r_i$  que são os mesmos,  $r_j \equiv r_k$  para algum par  $j$  e  $k$ . Mas, então, o que corresponde a  $a_j$  têm o restante mesmo quando dividido por  $N-1$ , e assim a sua diferença  $a_j - a_k$  é uniformemente divisível por  $N-1$ .

**EXERCÍCIO 29:** Se uma cidade tem 10.000 linhas telefônicas diferentes numeradas por números de 4 dígitos e mais da metade das linhas telefônicas estão no centro da cidade, segue-se que há dois números de telefone no centro da cidade e cuja soma é novamente o número de uma linha telefônica no centro.

**EXERCÍCIO 30:** Se houver 6 pessoas em uma festa, segue-se que três deles se conheciam antes da festa ou 3 deles eram completos estranhos antes da festa.

## 4.8. ERROS COMUNS NAS [pseudo] "PROVAS"

(Para mais detalhes, ver os interessantes artigos <http://math.stackexchange.com/questions/139503/in-the-history-of-mathematics-has-there-ever-been-a-mistake>,  
<http://www.math.vanderbilt.edu/~schectex/commerrs/>,  
<http://marathoncode.blogspot.com.br/2012/10/erros-comuns-em-provas-matematicas.html>)

**A) Argumentar a partir de exemplos:** Veja esta "prova" incorreta do teorema do Exemplo 1, acima: "Se  $m = 14$  e  $n = 6$  então  $m + n = 20$  que é par, e  $m - n = 8$  que também é par." Esta "prova" merece nota zero. É verdade que 1 contra-exemplo destrói uma conjectura de afirmativa universal, mas 1000 exemplos não a provam, pois poderia falhar no teste 1001 ...

**B) Usar a mesma letra para representar duas coisas diferentes**

Além da confusão que isto provavelmente causará no leitor, pode fazer com que você chegue a uma falsa conclusão.

**C) Pular "ilicitamente" para uma conclusão:**

Alegar a verdade de alguma coisa sem dar uma razão adequada. Veja esta "prova" incorreta do teorema do Exemplo 1, acima: "Suponha que  $m$  e  $n$  sejam inteiros e que  $m + n$  é par. Pela definição de par,  $m + n = 2k$  para algum inteiro  $k$ . Então  $m = 2k - n$  e, assim,  $m - n$  é par." É verdade que  $m - n$  é par, mas não pelo raciocínio apresentado. O passo "e, assim,  $m - n$  é par" não é sustentado pela regras de lógica. Poderia ter pulado para uma conclusão falsa. Nada foi realmente provado, esta "prova" merece nota zero.

**D) Usar a questão a ser provada:**

Assumir como verdadeiro o que deve ser provado - variação de pular para uma conclusão. Exemplo de "prova" do teorema "o produto de dois ímpares é um ímpar": "Suponha que  $m, n$  são números ímpares. Se  $mn$  é ímpar, então  $mn = 2k + 1$  para algum inteiro  $k$ . Também pela definição de ímpar, ( $m = 2a + 1$ ) e ( $n = 2b + 1$ ) são verdadeiros para inteiros  $a, b$ . Então  $mn = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$ , que é ímpar por definição.

**E) Uso incorreto do vocábulo SE:**

Às vezes, escrevemos "se" no sentido de "uma vez que" ou "em consequência de", não no sentido de condicional

EXEMPLO: "Se eu sou seu pai, então você deve me tratar com mais respeito." // Este "se" não exprime nenhuma dúvida geral.

EXEMPLO: Suponha que  $p$  é um número primo. Se  $p$  é primo, então  $p$  não pode ser escrito como o produto



de dois números menores que são inteiro.  
dúvida se de fato  $p$  é primo ou não.

// O vocábulo SE, nesta última sentença, coloca em

## **Recapitulando a unidade**

**Recapitulando a unidade:** Parabéns, você concluiu a unidade IV, portanto ultrapassou a metade da disciplina. Persevere esforçando-se cada vez mais para vencer com honestidade, garra e competência. Se você foi disciplinado e realmente estudou com todo afinho 4 a 8 h/semana, deve estar dominando os principais métodos de prova dedutiva formal: provas simples a partir somente das definições; provar/disprovar afirmações universais "se-então" (diretamente, ou por divisão em casos, ou por exaustão, ou por generalização de um elemento específico escolhido arbitrariamente); fazer provas indiretas, por contra-exemplo, contradição, redução ao absurdo, e uso do contrapositivo; fazer provas "se- e- somente- se" e provas (construtivas e não construtivas) de existência; prova de uma função ser bem construída; provas pelo princípio das casas de pombos.

Para você treinar ainda melhor, recomendamos a Lista de Exercícios sobre Métodos de Prova, Prof. Loureiro, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE3.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE3.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE3\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE3_Solucao.pdf).

Na próxima unidade, a V, você será introduzido à Análise Combinatória, que analisa estruturas e relações discretas procurando determinar métodos de enumeração ou contagem nelas: Você lembrará técnicas básicas de contagem (permutações, arranjos, combinações), relações de recorrência e coeficientes binomiais, e verá outras sequências de contagem e o teorema de Ramsey.

## UNIDADE V

# 5. Introdução à ANÁLISE COMBINATÓRIA

A **Análise Combinatória** (ou, simplesmente, *Combinatória*) é o ramo da Matemática que analisa estruturas e relações discretas, nelas procurando determinar métodos de contagem ou de enumeração, termos aqui usados no sentido de determinar o número de elementos de um conjunto e de atribuir números naturais a seus elementos.

**Nosso objetivo, nesta unidade,** é, primeiramente, você <sup>[relembrar e voltar a]</sup> dominar as técnicas de contagem e enumeração mais conhecidas (que são as de combinações, arranjos e permutações) de subconjuntos de um conjunto *finito* e que satisfazem certas condições dadas. (Como você, com suficiente carga horária e profundidade, já estudou isso no ensino médio e para o recente vestibular, faremos apenas uma sucinta e **rápida revisão, quase sem nenhuma prova de fórmulas e teoremas, e com poucos exemplos.**)

A seguir, procuraremos lhe dar um panorama informativo sobre alguns dos *outros* mais importantes métodos de contagem (**estes são difíceis para este seu primeiro período na universidade, não exigiremos completo domínio deles nos exames**).

A importância da Combinatória na Ciência da Computação decorre do fato de que um considerável número de problemas muito frequentemente encontrados são redutíveis a apenas alguns poucos problemas básicos de contagem, que se apresentam sob variados “disfarces”.

Repetimos: *Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, **cada semana dedicando 4 a 8 horas para estudar este livro.***

### Conteúdo desta unidade:

- 5.1. Técnicas Básicas de Contagem. Permutações, Arranjos, Combinações
- 5.2. Relações de Recorrência
- 5.3. Coeficientes Binomiais
- 5.4. Outras Sequências de Contagem
- 5.5. Teorema de Ramsey



Se você quiser ver o assunto mais explicada e profundamente, não precisará de mais que os livros textos da ementa da disciplina. Mas, devido à sua concisão e objetividade, pegamos o “jeitão”, o esqueleto mestre e ordem de apresentação, a escolha de tópicos do capítulo 6 do livro “Programming Challenges”, Steven S. Skiena and Miguel A. Revilla, muito útil, que pode ser encontrado na Internet para download gratuito. Recomendamos um livro específico no assunto, em <http://pt.scribd.com/doc/99378433/Analise-Combinatoria-e-Probabilidade-Augusto-Cesar-de-Oliveira-Morgado-Pedro-Fernandez-1991>, particularmente seu capítulo 2, que tem 24 ótimos exemplos, todos eles resolvidos, sobre combinações e permutações. **Este livro contém as provas de todas as fórmulas aqui usadas**, e elas também foram vistas no ensino médio, por isso as omitiremos e recomendamos que os eventuais interessados as vejam ali, ou nos livros texto desta disciplina ( $P(n)$ ,  $P_c(n)$ ,  $P_r(n,r)$ ,  $P(n,(n_a,n_b,\dots))$ ,  $K(n)$ ,  $A(n,r)$ ,  $A(n,n_1,r,r_1)$ ,  $C(n,r)$ ,  $Cr(n,r)$ , etc.). Agradecemos aos Profs. Paulo Roberto Rezende e Rômulo Garcia, do Projeto Rumo ao ITA, do Sistema Elite de Ensino, por muitos dos exemplos e problemas propostos, entendemos que são questões de passados vestibulares ao ITA e ao IME.

## 5.1. Técnicas Básicas de Contagem. Permutações, Arranjos, Combinações

• **Regra do Produto** (ou **Princípio Fundamental da Enumeração**): Se há  $|A|$  possibilidades no conjunto  $A$  e  $|B|$  possibilidades no conjunto  $B$ , então há  $|A| \times |B|$  maneiras de combinar uma possibilidade de  $A$  e uma de  $B$ .

Generalizando, se um evento  $A_i$  pode ocorrer de  $m_i$  maneiras diferentes, então o número de maneiras de ocorrerem os eventos  $A_1, A_2, \dots, A_n$  de forma sucessiva é  $m_1 \cdot m_2 \cdot \dots \cdot m_n$ .

Por exemplo, suponha que você possui 5 camisas e 4 calças. Então, há  $5 \times 4 = 20$  maneiras diferentes para você se vestir amanhã.

EXEMPLO 1 (Morgado-Carvalho-Carvalho-Fernandez): Quantos números naturais de três algarismos distintos (na base 10) existem?

RESPOSTA: O primeiro algarismo pode ser escolhido de 9 modos (não podemos usar o 0), o segundo de 9 modos (não podemos usar o algarismo utilizado anteriormente) e o terceiro de 8 modos (não podemos usar os dois algarismos já empregados anteriormente). A resposta é  $9 \times 9 \times 8 = 648$ . [Sempre devemos começar pelo conjunto de escolha sujeita a restrições decorrentes das outras escolhas, ou a escolha mais difícil e que, se adiada, ficará ainda pior depois. Isto é a escolha do primeiro algarismo: Se começássemos da direita para a esquerda, ao chegarmos ao primeiro algarismo teríamos 8 escolhas se o 0 já tivesse sido escolhido, e 7 em caso contrário.]

• **Regra da Soma**: Se há  $|A|$  possibilidades no conjunto  $A$  e  $|B|$  possibilidades no conjunto  $B$ , então há  $|A| + |B|$  formas para  $A$  ou  $B$  ocorrerem, assumindo-se que os elementos de  $A$  são diferentes dos de  $B$ . Generalizando, dados os conjuntos  $A_1, A_2, \dots, A_n$ , em que  $A_i$  tem exatamente  $a_i$  elementos, então o número de elementos da união  $A_1 \cup A_2 \cup \dots \cup A_n$  é dado por  $a_1 + a_2 + a_3 + \dots + a_n$ . Por exemplo, dado que você possui 5 camisas e 4 calças e a lavanderia telefona avisando que arruinou uma peça de suas roupas, sem dizer mais nada, então há 9 itens possíveis com a possibilidade de terem sido arruinados.

EXEMPLO 2: Uma senha de usuário de um sistema computacional pode ser formada por sequências de 5 a 13 caracteres, cada um (inclusive o primeiro) podendo ser letra maiúscula, letras minúscula, um dos 10 dígitos, sublinhado, ponto, hífen, e jogo da velha, totalizando  $26+26+10+4 = 66$  caracteres diferentes, sendo que repetições são permitidas. Quantas senhas diferentes existem?

RESPOSTA: O conjunto de todas as senhas é formado pelo subconjunto das senhas de 5 caracteres, união o subconjunto das senhas de 6 caracteres, união ... , união o subconjunto das senhas de 13 caracteres. O primeiro subconjunto tem  $66^5$  possibilidades, o segundo  $66^6$ , etc. A resposta é a soma:  $\sum_{i=5}^{13} 66^i \cong 4,57827 \times 10^{23}$ .

• **Fórmula da Inclusão-Exclusão**: A regra de soma é um caso especial de uma fórmula mais geral para quando dois conjuntos podem se sobrepor, a saber,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

A fórmula de inclusão-exclusão pode ser generalizada a três conjuntos e além, de uma forma natural:

[ Para quatro conjuntos:

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$$

Generalizando: o número de elemento da união é obtido quando somamos os elementos de cada conjunto, subtraímos o número de elementos das interseções 2 a 2, somamos o número de elementos das interseções 3 a 3, subtraímos o número de elementos das interseções 4 a 4 e, assim, sucessivamente.

]

EXEMPLO 3 (R. Garcia): Quantos são os anagramas da palavra CADERNO que têm C em 1º lugar, ou A em 2º lugar, ou D em 3º lugar ou E em 4º lugar?

RESPOSTA: Inicialmente, definamos os conjuntos:

$A_1$ : conjunto cujos elementos são os anagramas da palavra CADERNO que têm a letra C em 1º lugar

$A_2$ : conjunto cujos elementos são os anagramas da palavra CADERNO que têm a letra A em 2º lugar

$A_3$ : conjunto cujos elementos são os anagramas da palavra CADERNO que têm a letra D em 3º lugar

$A_4$ : conjunto cujos elementos são os anagramas da palavra CADERNO que têm a letra E em 4º lugar

Queremos determinar  $|A_1 \cup A_2 \cup A_3 \cup A_4|$ . Temos:

$$|A_1| = |A_2| = |A_3| = |A_4| = P_6 = 6! = 720 \text{ (fixar 1 letra e permutar as 6 demais)}$$

$$|A_1 \cap A_2| = |A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_3| = |A_2 \cap A_4| = |A_3 \cap A_4| = P_5 = 5! = 120 \text{ (fixar 2 letras e permutar as demais 5)}$$

$$|A_1 \cap A_2 \cap A_3| = |A_1 \cap A_2 \cap A_4| = |A_1 \cap A_3 \cap A_4| = |A_2 \cap A_3 \cap A_4| = P_4 = 4! = 24 \text{ (fixar 3 letras e permutar as demais 3)}$$

permutar as demais 4)

$$|A_1 \cap A_2 \cap A_3 \cap A_4| = P_3 = 3! = 6 \text{ (fixar 4 letras e permutar as demais 3)}$$

Pela Fórmula da Inclusão – Exclusão, temos:

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = 4 \times 720 - 6 \times 120 + 4 \times 24 - 6 = 2250.$$

Logo, temos 2250 anagramas da palavra CADERNO com as restrições impostas pelo enunciado.

[indevida] **dupla contagem** é um aspecto escorregadio da combinatória, o que pode tornar difícil a resolução de problemas através da Fórmula de Inclusão - Exclusão. Outra técnica poderosa é estabelecer uma bijeção.

• **Bijeção** é um mapeamento um- a- um entre [todos] os elementos de um conjunto e [todos] os elementos de outro. Sempre que você tem tal mapeamento, contar o tamanho de um dos conjuntos automaticamente lhe dá o tamanho do outro conjunto.

Por exemplo, se contarmos o número de todos os pares de sapatos que, neste instante, estão sendo usados em um determinado pelotão de soldados (e podemos assumir que cada soldado usa exatamente 1 par de sapatos), então isso nos diz qual é o número de soldados no pelotão. Isto funciona porque há um mapeamento um- a- um entre pares de sapatos e soldados, e poderia falhar se estivéssemos falando de relógios (alguns os usam, outros não).

Explorar bijeções obriga-nos a ter um repertório de conjuntos que sabemos como contar, para que possamos mapear outros objetos para eles. Os objetos combinatoriais básicos com os quais você deve estar familiarizado incluem os seguintes (e é útil ter um sentimento de quão rapidamente o número de objetos cresce, para saber quando busca exaustiva torna-se uma técnica inviável):

• **Subconjuntos:** Um subconjunto é uma seleção de elementos de  $n$  itens possíveis. **Existem  $2^n$  subconjuntos distintos de  $n$  coisas.** Por exemplo, existem  $2^3 = 8$  subconjuntos de três itens, a saber, 1, 2, 3, 12, 13, 23, 123, e o conjunto vazio (nunca esqueça o conjunto vazio). Para  $n = 20$ ,  $2^n = 1.048.576$ , então começamos a chegar aos limites [da viabilidade] da busca exaustiva.

• **Permutação Simples** é uma sequência (portanto a ordem, as posições importam) sem repetições, de comprimento  $n$ , de elementos tirados de um conjunto de  $n$  elementos distintos. O número dessas permutações distintas (pela ordem e posição dos elementos) é

$$P(n) = n!$$

// leia  $P(n)$  como “**permutação simples de  $n$  elementos distintos**”

A prova disso é consequência direta da aplicação da regra do produto. Note que, para  $n = 10$ ,  $n! = 3.628.800$ , então começamos a chegar aos limites [da viabilidade] da busca exaustiva.

EXEMPLO 4 (Morgado-Carvalho-Carvalho-Fernandez): De quantos modos 5 rapazes e 5 moças podem se sentar em 5 bancos de 2 lugares cada, de modo que em cada banco fique um rapaz e uma moça?

RESPOSTA: O 1º rapaz pode escolher seu lugar de 10 modos, o 2º rapaz de 8 modos, o 3º de 6 modos, o 4º de 4 modos, e o 5º de 2 modos. Colocados os rapazes, temos de colocar as moças nos 5 lugares que sobraram, o que pode ser feito de  $5!$  modos. A resposta é  $10 \times 8 \times 6 \times 4 \times 2 \times 5! = 460800$ .

A FORMAÇÃO das permutações de  $n \geq 1$  elementos pode ser feita assim (bottom-up, forward):

-- a permutação de 1 elemento é 1;

-- para formar as  $n!$  permutações de  $\{1, 2, \dots, n\}$ , tome cada uma das  $(n-1)!$  permutações de  $\{1, 2, \dots, n-1\}$  e, em cada uma, insira  $n$  antes dela e imprima, depois insira  $n$  entre o 1º e 2º elemento dela e imprima, etc., insira  $n$  depois da  $(n-1)^{\text{ésima}}$  posição dela e imprima.

POR EXEMPLO: as permutações de 1 elemento são somente uma: 1;

as permutações de 2 elementos são duas: 12, 21;

as permutações de 3 elementos são seis: 123, 132, 213, 231, 312, 321;

etc.

Os algoritmos mais simples têm um tempo de execução que, no pior caso, é assintoticamente proporcional a  $n!$ . Os mais sofisticados, têm  $O(\lg n!)$ , que deve ser entendido como  $O(\lg(n!))$

<http://journal.dyu.edu.tw/dyujournal/document/setjournal/s05-4-21-29.pdf>

DESAFIO só para sua satisfação, quando tiver tempo sobrando: Usando a regra de formação acima vista, prove por indução a fórmula  $P(n) = n!$ . Confira em algum livro (mas atenção, pode ser que ele use outra regra de formação).

DESAFIO só para sua satisfação, quando souber programar bem: Escreva e teste um programa que implemente a regra de formação acima.

DESAFIO só para sua satisfação, quando souber programar bem: Examine em <http://www.geeksforgeeks.org/lexicographic-permutations-of-string/> a regra de Dijkstra para gerar as permutações em ordem lexicográfica (muito interessante), e faça e teste um programa para isso, finalmente compare-o com o da mesma URL.

• **Permutação** <sup>[Simples]</sup> **Circular** é uma permutação simples de  $n$  elementos distintos colocados formando um círculo (se duas permutações coincidem girando-se o círculo, não são distintas). O número dessas permutações distintas é

$$\underline{Pc(n) = (n-1)!}$$

// leia  $Pc(n)$  como "permutação simples e circular de  $n$  elementos distintos"

EXEMPLO 5: Seja um conjunto com 10 amigos. De quantos modos distintos estes amigos podem sentar-se junto a uma mesa circular sem que haja repetição das posições relativas?

$$Pc(10) = (10-1)! = 9! = 362880$$

• **Permutação Podendo Repetir Elementos** é uma sequência (ou string, ou cadeia, ou sequência) de comprimento  $r$  que pode repetir elementos de um conjunto de  $n$  elementos distintos. O número dessas distintas permutações é:

$$\underline{Pr(n,r) = n^r}$$

// leia  $Pr(n,r)$  como "permutação podendo ter repetições de elementos tomados  $r$  a  $r$ "

EXEMPLO 6: Um teclado tem 40 teclas, cada uma com somente um símbolo. De quantas maneiras diferentes um macaco doido e cego pode formar uma sequência de 10 símbolos?

RESPOSTA:  $40^{10} = (4 \times 10)^{10} = 2^{20} \times 10^{10}$ , um número de 16 dígitos, na ordem de  $10^{16} = 10.000.000.000.000.000 = 10$  quintilhões.

• **Permutação de Elementos Nem Todos Distintos** é uma sequência (portanto a ordem, as posições importam) de elementos tirados de um grupo de elementos possivelmente repetidos. O número de distintas permutações de  $r$  elementos tirados de um grupo de  $n$  elementos (havendo  $n_a$  elementos  $a$ ,  $n_b$  elemento  $b$ , ..., e sendo  $n_a + n_b + \dots = n$ ) é:

$$\underline{P(n, (n_a, n_b, \dots)) = n! / (n_a! n_b! \dots)}$$

// leia  $P(n, (n_a, n_b, \dots))$  como "permutação de  $n$  elementos havendo  $n_a$  a's,  $n_b$  b's, etc."

EXEMPLO 7 (Morgado et al.): Quantos são os anagramas da palavra "MATEMÁTICA"?

RESPOSTA: Como temos 3 letras A, 2 letras M, 2 letras T, 1 letra C, 1 letra I e 1 letra E, a resposta é

$$P(10, (3, 2, 2, 1, 1, 1)) = 10! / (3! 2! 2! 1! 1! 1!) = 151200.$$

EXEMPLO 8 (Morgado et al.): Quantos são os anagramas de "URUGUAI" que começam por vogal?

RESPOSTA: Temos  $P(6, (2, 1, 1, 1, 1))$  começados com U,  $P(6, (3, 1, 1, 1))$  começados com A, e  $P(6, (3, 1, 1, 1))$  começados com I. A resposta é

$$P(6, (2, 1, 1, 1, 1)) + 2 \times P(6, (3, 1, 1, 1)) = 360 + 2 \times 120 = 600.$$

• **Permutação caótica** (ou **desordenada**) de  $n$  elementos é uma permutação em que nenhum de seus elementos está na posição inicial. Usando a Fórmula de Inclusão – Exclusão, demonstra-se que o número de Permutações Caóticas de  $(1, 2, 3, \dots, n)$  é dado por:

$$\underline{K(n) = n! \cdot [1/0! - 1/1! + 1/2! - 1/3! + \dots + (-1)^n / n!]}$$

(Importante: Prova-se que  $K(n)$  é o arredondamento (para o inteiro mais próximo, quer para baixo ou para cima) de  $n!/e = n!/2,718281828459045\dots$ )

( $K(n)$  também é escrito como  $!n$ , que é pronunciado como "caos fatorial" ou, em inglês "derangements" (desarrumações))

EXEMPLO 9 (R. Garcia): De quantas formas podemos permutar os algarismos do número 1234 de modo que nenhum número ocupe sua posição inicial?

RESPOSTA:  $K(4) = 4! [1/0! - 1/1! + 1/2! - 1/3! + 1/4!] = 4! [1/1 - 1/1 + 1/2 - 1/6 + 1/24] = 4! [24 - 24 + 12 - 4 + 1]/24 = 24 \times 9/24 = 9$ . Observe como a aproximação  $n!/2,718281828459045$  resulta em 8,83, que, arredondado para cima, dá 9.

• **Arranjo simples** é uma sequência (portanto a ordem, as posições importam) de  $r$  elementos distintos tirados de um conjunto de  $n$  elementos distintos. O número desses arranjos distintos é

$$\underline{A(n,r) = n!/(n-r)!}$$

// leia  $A(n,r)$  como "arranjo simples de  $n$  elementos

tomados  $r$  a  $r$ "

Se  $r = n$  então arranjos tornam-se o mesmo que permutações, e temos:

$$\underline{A(n,n) = n!}$$

Note que "arranjo simples de  $n$  elementos tomados  $r$  a  $r$ " também é conhecido, particularmente nos USA, como "permutação de  $n$  elementos tomados  $r$  a  $r$ ". Não definimos "arranjo podendo repetir elementos" porque iria ser o mesmo que "permutação podendo repetir elementos", acima. E não definimos "arranjo de elementos nem todos distintos" porque iria ser o mesmo que "permutação de elementos nem todos distintos", acima.

EXEMPLO 10: 7 pessoas estão apostando corrida. Quantos são os agrupamentos possíveis para os três primeiros colocados [diferenciando entre 1º, 2º e 3º lugares]?

RESPOSTA:  $A(7,3) = 7!/(7-3)! = 7!/4! = 7 \times 6 \times 5 = 210$ .

A FORMAÇÃO dos arranjos pode ser feita assim: forme as combinações de  $n$  elementos tomados  $r$  a  $r$ . Agora, tome cada combinação de  $r$  elementos e ache todas suas permutações.

EXEMPLO 11: Dados os elementos  $\{1,2,3,4\}$ , suas  $C(4,2) = n!/(r!(n-r)!) = 4!/(2!2!) = 6$  combinações 2 a 2 são: 12, 13, 14, 23, 24, 34. Portanto, os seus  $n!/(n-r)! = 4!/2! = 12$  arranjos 2 a 2 são: 12, 21, 13, 32, 14, 41, 23, 32, 24, 42, 34, 43.

• **Arranjo condicional:** Todos os  $n$  elementos podem aparecer em cada arranjo de  $r$  elementos, mas existe uma condição que deve ser satisfeita por  $r_1$  de  $n_1$  elementos. O número desses arranjos condicionais distintos é

$$\underline{A(n,n_1,r,r_1) = A(n_1,r_1) \cdot A(n-n_1,r-r_1)}$$

EXEMPLO 12: Quantos arranjos com  $r = 4$  elementos do conjunto de  $n = 7$  elementos  $\{A,B,C,D,E,F,G\}$ , começam com  $r_1 = 2$  letras escolhidas no subconjunto  $\{A,B,C\}$  de  $n_1 = 3$  elementos?

$$A(n,n_1,r,r_1) = A(3,2) \times A(7-3,4-2) = A(3,2) \times A(4,2) = 6 \times 12 = 72$$

• **Combinação Simples (ou Sem Repetição)** é um subconjunto com  $r$  elementos em um conjunto  $U$  que tem  $n$  elementos. Como é um conjunto, não há repetição de elementos em uma combinação. O número dessas combinações distintas é

$$\underline{C(n,r) = n!/(r!(n-r)!)}$$

// leia " $C(n,r)$ " como "combinação simples de  $n$  elementos

tomados  $r$  a  $r$ "

Note que  $C(n,r) = C(n,n-r)$

PROVA: O número de arranjos (a ordem dos elementos importa) simples é  $A(n,r)$ .

O número de maneiras de fazer permutações sobre um único desses arranjos é  $P(r)$ .

Como a ordem é desprezada nas combinações, então  $C(n,r)$  é o número de arranjos,  $A(n,r)$ , dividido pelo número ( $P(r)$ ) de modos de ordenar cada arranjo individual:

$$C(n,r) = A(n,r)/P(r) = [n!/(n-r)!] / r! = n!/(r!(n-r)!)$$

EXEMPLO 13 (Morgado et AL.): De quantos modos podemos escolher 6 pessoas, incluindo pelo menos 2 mulheres, a partir de um grupo de 7 homens e 4 mulheres?

RESPOSTA: As alternativas são:

4 homens, 2 mulheres

3 homens, 3 mulheres

2 homens, 4 mulheres

Portanto, a resposta é

$$C(7,4) \times C(4,2) + C(7,3) \times C(4,3) + C(7,2) \times C(4,4) = 7!/(4!3!) \times 4!/(2!2!) + 7!/(3!4!) \times 4!/(3!1!) + 7!/(2!5!) \times 4!/(4!0!) = 35 \times 6 + 35 \times 4 + 21 \times 1 = 371$$

A FORMAÇÃO das combinações pode ser feita assim: Representemos cada combinação colocando seus elementos em ordem crescente. Dado o conjunto  $a = \{1,2,\dots,n\}$  e dado  $r$  tal que  $0 \leq r \leq n$ ,

\* a 1ª combinação é  $\{1,2,\dots,r\}$  // se  $r=0$ , isto será  $\{\}$ , e terminamos

\* para gerar a próxima combinação para  $a_1 a_2 \dots a_r$ :

-- Ache o maior  $i$  tal que  $a_i \neq n-r+i$ .

-- Faça  $a_i = a_i + 1$ .

-- Para  $j = i$  até  $r$  faça  $a_j = a_{j-1} + 1$ .

POR EXEMPLO: Suponha que o conjunto é  $a = \{1,2,3,4,5,6,7,8,9\}$ ,  $n = 9$ ,  $r = 4$ :

Seja a 1ª combinação 1234	alguma combinação é 1458
a 2ª combinação é 1235	a próxima é 1459
a 3ª combinação é 1236	a próxima é 1467
...	...
alguma combinação é 1249	alguma combinação é 3789
a próxima é 1259	a próxima é 4567
....	....

Outra regra de FORMAÇÃO das combinações, agora partindo de um array de caracteres e usando strings binárias com s dígitos 0's e t dígitos 1's, 1 significando tomar o caractere originalmente correspondente à posição do bit, e 0 não tomar:

Enquanto for possível e não retornar à situação inicial: Identifique o menor prefixo terminando em 010 ou 011 (ou toda a string se não existe tal prefixo), e gire este prefixo 1 posição para a direita.

POR EXEMPLO, seja ABCDE o array inicial de caracteres. Para gerar todas as combinações de 5 elementos tomados 3 a 3 (portanto  $n=5$ ,  $s=2$ ,  $t=3$ ), parta de ABC, representada como 11100. Os passos serão:

11100 ABC, o prefixo desejado é toda a matriz, gire-o 1 posição para a direita

01110 BCD, o prefixo desejado é 011, gire-o 1 posição para a direita

10110 ACD, o prefixo desejado é 1011, gire-o 1 posição para a direita

11010 ABD, o prefixo desejado é 11010, gire-o 1 posição para a direita

01101 BCE, o prefixo desejado é 011, gire-o 1 posição para a direita

10101 ACE, etc.

Detalhes em <http://webhome.cs.uvic.ca/~ruskey/Publications/Coollex/coollexDMvanilla.pdf>

O algoritmo R de Knuth toma um tempo de execução que, no pior caso, é assintoticamente proporcional ao tamanho da saída, isto é,  $O(n \cdot n! / (r!(n-r)!))$ .

• **Combinação com Repetições** (ou **Completa**) é um agrupamento de  $r$  elementos com possíveis repetições, onde os elementos são distintos entre si apenas pela espécie e número mas não pela ordem, e foram de um conjunto de  $n$  elementos distintos. O número dessas distintas permutações é:

$$Cr(n,r) = C(n+r-1,r) = (n+r-1)! / (r!(n-1)!) \quad // \text{ leia "C(n,r)" como}$$

"combinação de  $n$  elementos distintos tomados  $r$  a  $r$  com possíveis repetições"

EXEMPLO 14 (R. Garcia): De quantos modos podemos comprar 3 doces em uma padaria que tem 4 tipos de doces diferentes?

RESPOSTA: A solução para esse problema não é  $C(4,3)$ . Seria, se ele afirmasse que deveríamos escolher 3 doces *diferentes* sabendo que temos a nossa disposição 4 tipos diferentes. Nesse caso, de 4 elementos diferentes, deveríamos escolher 3 diferentes desses elementos (sem que a ordem de escolha importe) e isso pode ser feito de  $C(4,3)$ . A resposta para esse caso é  $Cr(4,3)$ , isto é, de 4 tipos de doces diferentes queremos escolher 3 tipos de doces não necessariamente distintos. Portanto,  $(n+r-1)! / (r!(n-1)!) = (4+3-1)! / (3!(4-1)!) = 6! / (3!3!) = (6 \times 5 \times 4) / (3 \times 2) = 20$ .

## 5.2. Relações de Recorrência

Relações de recorrência facilitam a contagem em uma variedade de estruturas definidas de forma recursiva. Estruturas recursivamente definidas incluem árvores, listas, fórmulas bem formadas, e algoritmos divida-e-conquiste. Por isso, relações de recorrência surgem em [praticamente] tudo que os cientistas da computação fazem.

O que é uma relação de recorrência? É uma equação que é definida em termos de si mesma. Por que elas são uma boa coisa? Porque muitas funções naturais e usualmente encontradas são facilmente expressas como recorrências! Qualquer polinômio pode ser representado por uma recorrência, inclusive a função linear:

$$a_n = a_{n-1} + 1, a_1 = 1 \Rightarrow a_n = n$$

Qualquer exponencial pode ser representada por uma recorrência:

$$a_n = 2a_{n-1}, a_1 = 2 \Rightarrow a_n = 2^n$$

Finalmente, certas funções estranhas, mas interessantes, que não são facilmente representadas usando a notação convencional, podem ser [comodamente] descritas por recorrências:

$$a_n = na_{n-1}, a_1 = 1 \Rightarrow a_n = n!$$

Assim, as relações de recorrência são uma forma muito versátil para representar funções. É frequentemente

fácil encontrar uma recorrência como a resposta a um problema de contagem. *Resolver* a recorrência para obter uma agradável forma fechada pode ser um pouco de uma arte, mas técnicas avançadas de programação [conhecidas como Memoization e como Programação Dinâmica] podem fazer com que computadores facilmente avaliem o valor de uma dada recorrência, mesmo sem a existência de uma agradável forma fechada.

[Mais sobre recorrência e indução, inclusive exemplos e problemas, pode ser reestudado na unidade III deste livro. E agora, com mais experiência, você aproveitará mais ainda.]

## 5.3. Coeficientes Binomiais

A mais importante classe de contagem de números são os coeficientes binomiais, onde  $\binom{n}{k}$  conta o número de maneiras de escolher as  $k$  coisas a partir de  $n$  possibilidades [Leia “**número de combinações de  $n$  elementos tomados  $k$  a  $k$** ”]. O que eles contam [, por exemplo]?

• **Comitês** - Quantas maneiras existem para se formar um comitê de  $k$  membros a partir de  $n$  pessoas?

Resposta: Claramente, pela definição de coeficientes binomiais, é  $\binom{n}{k}$ .

• **Caminhos Atravessando uma Grade** - Quantas maneiras existem para se caminhar a partir do canto superior esquerdo de uma grade  $n \times m$  até o canto inferior direito, cada passo podendo ser apenas para baixo ou para a direita? Resposta: Cada caminho tem de consistir de  $n+m$  passos, sendo  $n$  para baixo e  $m$  para a direita; cada caminho com um conjunto diferente de movimentos para baixo é diferente; por isso, há  $\binom{n+m}{n}$  tais conjuntos / caminhos.

• **Coeficientes de  $(a + b)^n$**  - Observe que

$$(a + b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$$

Qual é o coeficiente do termo  $a^k b^{n-k}$ ? Resposta: Claramente, é  $\binom{n}{k}$ , porque isto conta o número de maneiras que podemos escolher os  $k$  termos “ $a$ ” a partir de  $n$  possibilidades.

• **Triângulo de Pascal** - Sem dúvida, você já brincou com esse arranjo de números no ensino médio. Cada número é a soma dos dois números imediatamente acima dele [um na direção ↖, outro na direção ↗]:

$$\begin{array}{ccccccc} & & & & 1 & & & & \\ & & & & 1 & & 1 & & \\ & & & 1 & & 2 & & 1 & \\ & & 1 & & 3 & & 3 & & 1 \\ & 1 & & 4 & & 6 & & 4 & & 1 \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

Por que você ou Pascal se incomodaram com isso? Porque esta tabela constrói os coeficientes binomiais! A linha  $(n+1)^{\text{ésima}}$  fornece os valores de  $\binom{n}{i}$  para  $0 \leq i \leq n$ . A melhor coisa sobre o triângulo é como ele revela determinadas identidades interessantes, tal como a soma das entradas na linha  $(n+1)^{\text{ésima}}$  ser igual a  $2^n$ .

Como você calcula os coeficientes binomiais? Seu primeiro pensamento foi lembrar que  $\binom{n}{k} = n! / ((n-k)!k!)$ ; assim, em princípio, você pode o calcular diretamente a partir dos fatoriais. No entanto, este método tem um sério desvantagem. Cálculos intermediários podem facilmente causar “estouro aritmético” mesmo quando o coeficiente final se encaixa confortavelmente dentro de um inteiro. Uma forma mais estável para calcular os coeficientes binomiais é a de utilizar a relação de recorrência implícita na construção do triângulo de Pascal, ou seja, que

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{para } 0 < k < n$$

Por que isso funciona? [Vamos explicar a lógica da equação.] Considere se o  $n^{\text{ésimo}}$  elemento aparece em um dos  $\binom{n}{k}$  subconjuntos de  $k$  elementos. Se aparece, podemos concluir o subconjunto escolhendo  $k-1$  outros itens a partir dos outros  $n-1$ . Se não aparece, temos que pegar todos os  $k$  itens dos restantes  $n-1$ . Não há sobreposição entre estes casos, e todas as possibilidades estão incluídas, de modo que a soma conta todos os subconjuntos de  $k$  elementos.

Nenhuma recorrência está completa sem casos base. Quais valores dos coeficientes binomiais sabemos sem computá-los? O termo à esquerda na soma eventualmente nos leva para baixo até  $\binom{n-k}{0}$ . Quantas maneiras há de escolher 0 coisas a partir de um conjunto? Exatamente 1 maneira, o conjunto vazio. Se isto não é convincente, então é igualmente bom aceitar que  $\binom{m}{1} = m$ . Já o termo à direita na soma nos leva para cima



até  $\binom{k}{k}$ . Quantas maneiras existem de se escolher k coisas a partir de um conjunto de k elementos?

Exatamente 1 maneira, escolher o conjunto completo. Juntamente com a recorrência, esses 2 casos base (abaixo) definem os coeficientes binomiais para todos os casos interessantes.

$$\binom{n-k}{0} = 1 \quad (\text{note que } n-k > 0)$$

$$\binom{k}{k} = 1 \quad (\text{note que } k > 0)$$

A melhor maneira de avaliar tal recorrência é a construção de uma tabela de todos os valores possíveis, pelo menos até o tamanho que você está interessado. Estude a função abaixo para ver como foi feito em

<http://www.cs.sunysb.edu/~skiena/392/programs/binomial.c>.

```
#define MAXN 100 /* o maior n ou m */
long binomial_coefficient(n,m)
int n,m; /* o computador recebe n e m */
{
    int i,j; /* contadores */
    long bc[MAXN][MAXN]; /* tabela de coeficientes binomiais */
    for (i=0; i<=n; i++) bc[i][0] = 1;
    for (j=0; j<=n; j++) bc[j][j] = 1;
    for (i=1; i<=n; i++)
        for (j=1; j<=i; j++)
            bc[i][j] = bc[i-1][j-1] + bc[i-1][j];
    return( bc[n][m] );
}
```

Aqui foi usada Programação Dinâmica, uma poderosa técnica algorítmica usada para avaliar recorrências de forma inigualavelmente eficiente, estudada no capítulo 11 do livro *Programming Challenges*. É muito poderosa, torna exequíveis problemas dantes intratáveis, mas é difícil para novatos e nem sempre pode ser aplicada.

## 5.4. Outras Sequências de Contagem

*(isto é difícil demais para seu primeiro período na universidade e para cobrarmos pesadamente em exame, foi incluído apenas para você tomar conhecimento da existência e das definições desses conceitos e, se precisar no futuro, ter por onde começar. Mas nossos alunos de Análise e Projeto de Algoritmos, a partir do 4º período, precisaram disso em vários problemas da UVA e nas Maratonas de Programação)*

Há várias outras sequências de contagem que repetidamente surgem em aplicações, e que são facilmente calculadas usando relações de recorrência. O experiente especialista em Análise Combinatória as mantém em mente sempre que eles têm que contar:

• **Números de Fibonacci** - definidos pela recorrência  $F_n = F_{n-1} + F_{n-2}$ , dados os valores iniciais  $F_0 = 0$  e  $F_1 = 1$ , surgem repetidas vezes, porque esta é, talvez, a mais simples relação de recorrência interessante.

EXEMPLO 15: Calcule os primeiros valores da sequência de Fibonacci:

RESPOSTA: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, . . .

Os números de Fibonacci se prestam a uma incrível variedade de identidades matemáticas, e é divertido brincar com eles. Por exemplo, pode ser provado que:

Dados os inteiros no intervalo  $[1,n]$ , o número de subconjuntos distintos deles e que não tenham dois inteiros consecutivos, é  $F_{n+1}$ .

Os números de Fibonacci têm a forma fechada (difícil de adivinhar, mas simples de computar):

$$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Esta forma fechada tem algumas implicações importantes. Uma vez que  $(1-\sqrt{5})/2$  está entre 0 e 1, elevando-a a qualquer potência deixa um número entre este intervalo. Assim, o primeiro termo,  $\varphi^n$ , onde  $\varphi = (1+\sqrt{5})/2 = 1,6180339887 4989484820 4586834365 6381177203 0917980576 2862135448 6227052604 6281890244 9707207204 1893911374 \dots$  (100 decimais. Pode ser baixado com 10 milhões de dígitos, de

<http://www.goldenratio.org/>) é a quantidade dominante, e pode ser utilizado para estimar  $F_n$  com imprecisão dentro de  $\pm 1$ .  $\Phi$  é chamada de **razão áurea**. (Veja em [http://pt.wikipedia.org/wiki/Proporção\\_áurea](http://pt.wikipedia.org/wiki/Proporção_áurea) como ela tem importantes aplicações na ciência e nas artes! Parece que tudo que é considerado *belo* segue essa proporção?). Quando  $n$  é muito grande, pode-se usar a aproximação assintótica  $f(n) \sim (\varphi^{n+2})/\sqrt{5}$

• **Números de Catalão** - a recorrência e a forma fechada a ela associada

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k} = \frac{1}{n+1} \binom{2n}{n}$$

definem os números de Catalão, que ocorrem em um número surpreendente de problemas em Análise Combinatória. Os primeiros termos são 2, 5, 14, 42, 132, 429, 1430, . . . quando  $C_0 = 1$ .

Quantas maneiras existem de se construir uma fórmula equilibrada a partir de  $n$  conjuntos de parênteses à esquerda e à direita?

EXEMPLO 16: Quantas diferentes maneiras existem de se construir uma fórmula equilibrada a partir de  $n = 3$  conjuntos de parênteses à esquerda e à direita?

RESPOSTA: De 5 cinco maneiras:  $((()))$ ,  $()(())$ ,  $((())())$ ,  $((())())$ , e  $()(())()$ . Isto coincide com a fórmula.

O parênteses mais à esquerda  $l$  corresponde a algum parâmetro à direita  $r$ , que deve particionar a fórmula em duas partes equilibradas (a parte entre  $l$  e  $r$ , e a parte à direita de  $r$ ). Se a parte à esquerda contém  $k$  pares, a parte direita deve conter  $n-k-1$  pares, desde que  $l, r$  representam um par. Ambas estas subformulas devem ser bem formadas, o que leva à recorrência vista acima, e surgem os números de Catalão.

Exatamente o mesmo raciocínio surge na contagem do número de triangulações de um polígono convexo, na contagem do número de árvores binárias enraizadas sobre  $n+1$  folhas, e na contagem do número de caminhos através de um reticulado que não suba acima da diagonal principal. Os números de Catalão têm a agradável forma fechada

$$C_n = \binom{2n}{n} / (n+1). \text{ [Uma aproximação, para } n \text{ grande, é } C_n \sim \frac{4^n}{n^{3/2} \sqrt{\pi}} \text{ ]}$$

• **Números de Euler** (pronuncie como "Óilêr") - Os números de Euler (ou Números Eulerianos)  $\langle n \rangle_m$  (também escritos  $A(n, m)$ ) contam o número de permutações de comprimento  $n$  onde exatamente  $m$  elementos são maiores que o elemento vizinho à esquerda (podem ser chamadas de "permutações com  $m$  degraus-subindo") (por exemplo, 524316 tem somente 2 degraus-subindo (um degrau-subindo é um par de vizinhos onde o da esquerda é menor que o da direita): o de 2 para 4, e a de 1 para 6).

EXEMPLO 17: Construa as 11 permutações de comprimento 4 com exatamente 1 degrau-subindo.

RESPOSTA:

1432 4132 4312  
2431 4231  
3421 4321 4231  
3421 3241 3214

EXEMPLO 18: Construa as 11 permutações de comprimento 4 com exatamente 2 degraus-subindo.

RESPOSTA:

4123 1243  
3124 1324 1243  
2134 1324 1342  
2134 2314 2341

Uma recorrência pode ser formulada por considerar cada permutação  $p$  de  $1, \dots, n-1$ . Há  $n$  lugares para inserir  $n$  elementos, e cada um divide um degrau-subindo já existente em  $p$ , ou ocorre imediatamente depois do último elemento de degrau-subindo existente, assim preservando a contagem daquele degrau-subindo. Assim,  $\langle n \rangle_m = m \times \langle n-1 \rangle_m + (n-m+1) \times \langle n-1 \rangle_{m-1}$ .

mas muitos preferem ir calculando os valores bottom up usando as equações recorrentes

$$\begin{aligned} A(n, 0) &= 1 && \text{para qualquer } n > 1 \\ A(n, m) &= (n-m) \times A(n-1, m-1) + (m+1) \times A(n-1, m) && \text{para quaisquer } n, m > 1 \end{aligned}$$

paulatinamente formando o **Triângulo de Euler**.

• **Números de Stirling** - Existem dois tipos diferentes de números de Stirling. O primeiro,  $\left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ , conta o

número de permutações de  $n$  elementos com exatamente  $k$  ciclos, onde, dada a função SeguidoPor:  $\mathbf{N} \rightarrow \mathbf{N}$ , um ciclo sob esta função é uma sequência  $(x_1, x_2, \dots, x_n)$  onde  $f(x_i) = x_{i+1}$  para  $1 \leq i \leq k-1$  e  $f(x_n) = x_1$ . Para formular a recorrência, observe se o  $n^{\text{ésimo}}$  elemento forma um ciclo de 1 só elemento, ou não. Se forma, há  $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$  maneiras para organizar o resto dos elementos para formar ciclos de  $k-1$  elementos. Se não forma, o  $n^{\text{ésimo}}$  elemento pode ser inserido em cada possível posição de cada ciclo das  $\begin{bmatrix} n-1 \\ k \end{bmatrix}$  maneiras de fazer ciclos de  $k$  elementos a partir dos  $n-1$  elementos. Assim,

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

Há 11 permutações de 4 elementos com exatamente 2 ciclos.

• **Partições de Conjunto** - o segundo tipo de número de Stirling  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  conta o número de formas de partição de  $n$  itens de modo a formarem  $k$  conjuntos. Por exemplo, existem 7 maneiras de partição de 4 itens em exatamente 2 subconjuntos [não vazios]: (1) (234), (12) (34), (13) (24), (14) (23), (123) (4), (124) (3), e (134) (2). O  $n^{\text{ésimo}}$  item pode ser inserido em qualquer um dos  $k$  subconjuntos de uma partição de  $(n-1)$  partes, ou pode formar um conjunto isolado e com 1 só elemento. Assim, por um argumento semelhante ao usado com os outros números de Stirling [acima], [os de agora] são definidos pela recorrência

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = K \times \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\}$$

O caso especial de  $\left\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \right\}$  é definido como  $2^{n-1}$ , uma vez que qualquer subconjunto próprio dos elementos 2 para  $n$  pode ser unido com (1) para definir a partição do conjunto. A segunda parte da partição consiste de exatamente os elementos que não estão nesta primeira parte.

• **Partições Inteiras** - uma partição inteira de  $n$  é um conjunto não ordenado de inteiros positivos que somam  $n$ . Por exemplo, existem 7 partições de 5, isto é, (5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1) e (1,1,1,1,1). A maneira mais fácil de contá-las é definir uma função  $f(n,k)$ , dando o número de partições inteiras de  $n$  com a maior parte sendo no máximo  $k$ . Em qualquer partição aceitável a maior parte alcança ou não alcança o limite, logo  $f(n, k) = f(n-k, k) + f(n, k-1)$ . Os casos bases são  $f(1,1) = 1$  e  $f(n,k) = 0$  quando  $k > n$ .

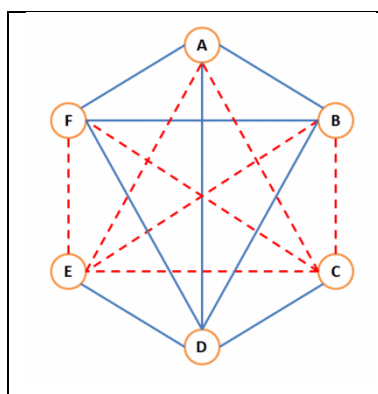
Sempre que você precisar, pode ir em <http://oeis.org> e lá dar entrada a um nome de cerca de 273 sequências, ou aos primeiros valores dela, e receber uma resumida aula enciclopédica sobre ela, código de programa, fórmula fechada, calculador, referências, etc.

## 5.5. Teorema de Ramsey

(isto é difícil demais para seu primeiro período na universidade e para cobrarmos pesadamente em exame, foi incluído apenas para você tomar conhecimento da existência e das definições desses conceitos e, se precisar no futuro, ter por onde começar.)

Primeiro, informalmente:

“dado um par de naturais  $s$  e  $t$ , existe um  $n$  suficientemente grande tal que, numa festa com  $n$  pessoas,  $s$  delas se conhecem ou  $t$  delas não se conhecem” (onde se conhecem é uma relação reflexiva:  $\text{se\_conhecem}(x,y) \Leftrightarrow \text{se\_conhecem}(y,x)$ ).



EXEMPLO: se exigirmos que sejam  $s = 3$  pessoas que se conhecem uma à outra e são  $t = 3$  pessoas tais que nenhuma conheça a outra, então basta a festa ter  $n = 6$  pessoas e estarão satisfeitas as exigências, isto é, sempre se pode encontrar 3 dessas 6 pessoas que se conhecem entre si, ou 3 dessas 6 pessoas onde nenhuma conhece as outras duas. Este exemplo equivale ao seguinte: se tomamos 6 pontos, e pintamos de preto ou vermelho cada segmento que une dois desses pontos, então necessariamente existe um triângulo cujos vértices são três desses pontos e cujos 3 lados são da mesma cor. Como os números são muito pequenos, você quer rabiscar num papel uns diagramas e se convencer e talvez fazer uma prova (que tal por contradição?) de que o teorema vale para este pequeno caso específico?

Uma vez que sempre existe  $n$ , uma pergunta natural é “Qual o menor inteiro  $n$ ?”. A prova da existência de  $n$ , por Ramsey, foi não construtiva, por isso achar  $n$  é difícil mesmo para casos específicos. Como assim é, muito mais difícil e desafiador tem sido achar fórmulas e algoritmos gerais (e de complexidade tolerável).

Agora, mais formalmente (em boa parte, baseamo-nos em <http://mathworld.wolfram.com/RamseysTheorem.html>):

• **Primeiro enunciado:** Para cada par de números inteiros positivos  $k$  e  $l$  existe um número inteiro  $R(k, l)$  (conhecido como o número Ramsey) de tal forma que qualquer grafo [ver unidade VI] com  $R(k, l)$  vértices contém um clique [um grafo completo, isto é, onde cada vértice se liga por uma aresta a cada dos outros vértices] com pelo menos  $k$  vértices, ou um conjunto independente com pelo menos  $l$  vértices.

• **Segundo enunciado:** para inteiros  $k, l \geq 2$ , existe pelo menos um número inteiro positivo  $R(k, l)$  de tal modo que não importa como o grafo é colorido com duas cores, irá conter um subgrafo (clique) verde  $K_k$  ou um subgrafo (clique) vermelho  $K_l$ .

• **Terceiro enunciado:** para todos  $k$  pertencente a  $\mathbb{N}$ , existe um  $l$  pertencente a  $\mathbb{N}$  tal que qualquer digrafo completo sobre os  $l$  vértices do grafos contém um subgrafo completo transitivo dos  $k$  vértices do gráfico.

• **Quarto enunciado:** para qualquer  $c$  dado inteiro, dados os inteiros  $n_1, \dots, n_c$ , há um número  $R(n_1, \dots, n_c)$  de tal forma que se arestas de um grafo completo de ordem  $R(n_1, \dots, n_c)$  são tingidos com  $c$  cores diferentes. Então, para algum  $i$  entre 1 e  $c$ , deve conter um subgrafo completo de ordem  $R(n_1, \dots, n_c)$  e cujas arestas são todas coloridas com a cor  $i$ .

EXEMPLO da dificuldade de se determinar qual é o valor de  $n$  (ou  $R(k, l)$ ), ao invés de apenas se saber que existe, sem se saber seu valor: Sabe-se que  $R(3, 3) = 6$  e que  $R(4, 4) = 18$ . Mas, quanto a  $R(5, 5)$ , só se conseguiu provar que está na faixa  $43 \leq R(5, 5) \leq 49$ . E, quanto a  $R(6, 6)$ , só se conseguiu provar que está na faixa  $102 \leq R(6, 6) \leq 165$ . Quanto  $k$  e  $l$  crescem,  $R(k, l)$  cresce astronômicamente, os limites dos intervalos em que devem estar podendo ter representações decimais com centenas ou milhares de dígitos. Foi provado que

$$2^{k/2} \leq R(k, k)$$

• **Teoria de Ramsey:** A ideia de achar uma certa ordem em configurações aleatórias dá origem à Teoria de Ramsey. Essencialmente, esta teoria diz que qualquer configuração suficientemente grande [usualmente números enormes, com centenas ou milhares de dígitos] conterà pelo menos um caso de qualquer outro tipo de configuração.

Os problemas da teoria de Ramsey são geralmente da forma: “Quantos itens deve conter uma estrutura para garantir a existência de uma propriedade particular?”

Um resultado típico da teoria de Ramsey começa com uma estrutura matemática que é depois dividida em partes. Qual o tamanho da estrutura original, a fim de assegurar que pelo menos uma das partes têm uma propriedade interessante dada? Por exemplo, considere um grafo completo (isto é, um clique) de ordem  $n$ , ou seja, existem  $n$  vértices e cada vértice é ligado a todos os outros  $n-1$  vértices através de uma aresta. (por exemplo, um grafo completo de ordem 3 é chamado um triângulo). Agora, cada aresta pode ter cor vermelha ou azul. Qual o tamanho de  $n$  fim de assegurar que há um triângulo azul ou um triângulo vermelho? A resposta é 6.

## **PROBLEMAS PROPOSTOS** (com respostas)

Retirados de

[http://www.rumoaoita.com/site/attachments/292\\_Exerc%C3%ADcios%20de%20An%C3%A1lise%20Combinat%C3%B3ria.pdf](http://www.rumoaoita.com/site/attachments/292_Exerc%C3%ADcios%20de%20An%C3%A1lise%20Combinat%C3%B3ria.pdf), agradecemos ao autor, Prof. Paulo Roberto Rezende. Entendemos que são questões de passados vestibulares ao ITA e ao IME.

01. Em um baile há seis rapazes e dez moças. Quantos pares podem ser formados para a dança:

a) sem restrição;

b) se Lúcia e Célia se recusam a dançar tanto com Manoel como com Cláudio, e Haroldo não quer dançar com Célia nem com Ana?

Resp.: a) 60; b) 54

02. Quantos números inteiros maiores que 53000, com algarismos distintos, podem ser formados com os

algarismos 0, 1, 2, 3, 4, 5, 6 e 7?

Resp.: 90360

03. Uma bandeira é formada de sete listras que devem ser pintadas de três cores diferentes. De quantas maneiras distintas será possível pintá-la de modo que duas listras adjacentes nunca estejam pintadas da mesma cor?

Resp.: 192

04. (IME) Quantos números de quatro algarismos distintos podem ser formados com os algarismos 0, 1, 2, 3, 4 e 5?

Resp.: 300

05. Um carro de montanha russa é formado por dez bancos de dois lugares cada um. De quantos modos dez casais se podem sentar nesse carro?

Resp.:  $3628800 \times 2^{10}$

06. De quantos modos podemos distribuir dez cartas de um baralho a dois parceiros, podendo eles receber quantidades desiguais de cartas, sendo que cada um deve receber ao menos uma carta?

Resp.: 1022

07. Quantos embrulhos é possível formar com cinco livros de Matemática, três de Física e dois de Química, não sendo diferentes os livros da mesma matéria?

Resp.: 71

09. Formam-se todos os números de seis algarismos, sem os repetir, com os algarismos do número 786.415. Colocando-se em ordem crescente, qual a posição do número dado?

Resp.: 597º

10. De quantos modos  $n$  pessoas podem sentar-se em  $n$  cadeiras enfileiradas:

- a) sem restrições;
- b) ficando A e B sempre juntas?
- c) sem que A e B fiquem juntas?
- d) ficando A, B e C juntas?
- e) ficando A, B e C juntas, e D e E separadas uma da outra?

Resp.: a)  $n!$ ; b)  $2 \times (n-1)!$ ; c)  $(n-2) \times (n-1)!$ ; d)  $6 \times (n-2)!$ ; e)  $6 \times (n-4) \times (n-3)!$

11. Em uma urna há  $2n$  bolas, numeradas de 1 a  $2n$ . Sacam-se, uma a uma, todas as bolas da urna.

- a) de quantos modos se pode esvaziar a urna?
- b) quantos são os casos em que os  $k$  últimos números ( $k < 2n$ ) aparecem nas  $k$  últimas sacadas?
- c) quantos são os casos em que as bolas de números ímpar aparecem nas sacadas de ordem

par?

Resp.: a)  $(2n)!$ ; b)  $2(n-k)!k!$ ; c)  $(n!)^2$

12. Determine o número de anagramas da palavra CAPÍTULO que não possuem vogais e nem consoantes juntas.

Resp.: 1152

13. De quantos modos se pode iluminar uma sala [a partir de um almoxarifado] com  $n$  lâmpadas [numeradas de 1 a  $n$ ]?

Resp.:  $2^n - 1$

14. De quantos modos se pode dispor doze objetos distintos em três grupos de quatro objetos?

Resp.: 5775

16. Em um congresso de professores há 30 professores de Física e 30 de Matemática. Quantos comissões de oito professores podem ser formadas:

- a) sem restrições;
- b) havendo pelo menos três professores de Física e pelo menos três de Matemática?

Resp.: a)  $C(60,8)$ ; b)  $2 \times C(30,3) \times C(30,5) + (C(30,4))^2$ .

17. Dados  $n$  pontos distintos de uma circunferência, quantos são os polígonos que podemos formar, *convexos*, cujos vértices são escolhidos entre esses pontos?

Resp.:  $2^n - (C(n,0) + C(n,1) + C(n,2)) = 2^n - (1 + n + n^2/2 - n/2) = 2^n - (1 + n/2 + n^2/2) = O(2^n)$

18. Quantas diagonais possui o dodecaedro regular?

Resp.: 100

19. Dados  $n$  pontos de um plano, não havendo 3 colineares, quantos são:

- a) os segmentos de reta cujas extremidades são escolhidas entre esses pontos?
- b) os triângulos cujos vértices são escolhidos entre esses pontos?
- c) os quadriláteros cujos vértices são escolhidos entre esses pontos?
- d) os polígonos de  $n$  lados cujos vértices são esses pontos?
- e) no máximo, os pontos de interseção das retas formadas por esses pontos, excluindo-se desse número os  $n$  pontos dados?

Resp.: a)  $C(n,2)$ ;    b)  $C(n,3)$ ;    c)  $3 \times C(n,4)$ ;    d)  $(n-1)!/2$ ;    e)  $3 \times C(n,4)$

20. Dados 7 pontos distintos de uma circunferência, quantos são os polígonos que podemos formar cujos vértices são escolhidos entre esses pontos?

Resp.: 1172

## **Recapitulando a unidade**

Que bom, você concluiu a unidade V, só faltam mais duas! E, se você foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter relembrado (ou aprendido) muitas coisas da parte básica de Análise Combinatória que já tinha visto no ensino médio, e deve ter aprendido mais um pouco. Tudo isto lhe será indispensável ou muito útil em todo o resto do curso e sua vida profissional. Você deve estar dominando: técnicas básicas de contagem (regras da multiplicação, da soma, e da inclusão- exclusão); permutações, arranjos, e combinações; relações de recorrência; coeficientes binomiais; e terá tido conhecimento de outras sequências de contagem e do teorema de Ramsey. Para você treinar ainda melhor, recomendamos a Lista de Exercícios sobre Análise Combinatória, pelo Prof. Loureiro, em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE7.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE7.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE7\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE7_Solucao.pdf).

Na próxima unidade, a VI (a penúltima!), você será introduzido aos conceitos básicos sobre árvores e grafos, começando a desenvolver a capacidade de modelar e implementar problemas reais usando tais ferramentas e de estruturas de dados. Só assim você poderá acompanhar algumas disciplinas posteriores e resolver muitos dos problemas reais com que se deparará em sua futura profissão de programador e analista.



## UNIDADE VI

# 6. Introdução a GRAFOS E ÁRVORES

**Nosso objetivo, nesta unidade,** é que você seja introduzido aos conceitos básicos sobre árvores e grafos, começando a desenvolver a capacidade de modelar problemas reais por meio deles, e capacitando-o a acompanhar disciplinas posteriores que o habilitarão a modelar mais complexos problemas reais usando tais ferramentas, e resolvê-los usando os algoritmos mais apropriados. Por falta de tempo, de espaço no livro, e de sua maior experiência com linguagens de programação, deixaremos a maioria dos tais algoritmos mais interessantes (e difíceis) para quando você fizer as disciplinas *Estruturas de Dados*, *Redes de Computadores*, e, talvez como ovinente, alguma disciplina na linha de *Análise* (da complexidade) e *Projeto de Algoritmos*, do Bacharelado em Ciência da Computação, da UFPB.

Sempre vamos lhe lembrar: *Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, cada semana dedicando 4 a 8 horas para estudar este livro.*

### Conteúdo desta unidade:

- 6.1. *Motivação e Introdução*
- 6.2. *Conceitos Básicos de Grafos e Digrafos*
- 6.3. *Percursos em Grafos em Geral e em Cliques*
- 6.4. *Árvores e Árvores Geradoras*



---

Agradecemos a permissão do Prof. Dr. *Lucídio dos Anjos Formiga Cabral* (DCC/ CI/ UFPB) para usarmos grande parte das 2 primeiras aulas de seu curso "*Introdução à Teoria dos Grafos*", que brevemente voltará a ser disponibilizado na Internet. Mas acrescentamos alguns problemas a resolver e alguns exemplos, e ocasionalmente mudamos algumas figuras (ou copiamos de fontes tais como Professora Sílvia Fernanda Martins Brandão da Uber <http://www.uber.com.br/silvia/MATD/>, e outras.), omitimos, ou acrescentamos algumas coisas. Se você quiser ver o assunto mais explicada e profundamente, não precisará de mais que os livros textos da ementa da disciplina. Mas há muitos e bons livros somente sobre grafos, alguns deles na Internet. Creditamos alguns dos exemplos e exercícios ao Prof. Christopher Strobel e ao Prof. Antônio Alfredo Ferreira Loureiro.

---

## 6.1. Motivação e Introdução

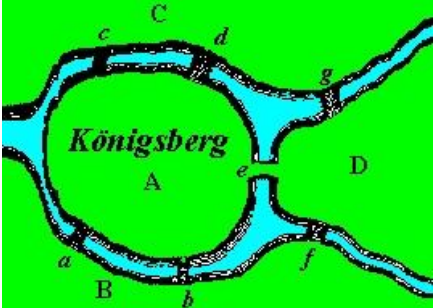
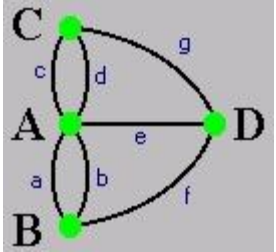
Por que estudar grafos? Porque são:

- Importante ferramenta matemática com aplicação em diversas áreas do conhecimento;
- Utilizados na definição e/ou resolução de problemas;
- Existem centenas de problemas computacionais que empregam grafos com sucesso.

Primeiras motivações na área:

- 1735, o **Problema das 7 Pontes de Königsberg** (atual Kaliningrad): Duas ilhas A e D, existentes no rio Pregel em Königsberg (Rússia), foram ligadas às margens do rio (B e C) através de 7 pontes. É possível iniciar uma caminhada a partir de um dos blocos de terra (A, B, C ou D), passar por cada uma das pontes exatamente uma vez, e voltar ao ponto de partida sem nadar pelo rio?



	
Situação real – o problema	Modelo do problema
Você tem que passar por cada um de a,b,c,d,e,f,g exatamente 1 vez	

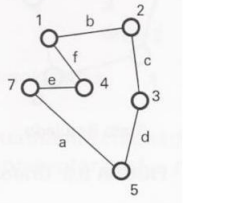
Resolvido pelo estudo da paridade dos nós: O problema não tem solução porque tem vértices com paridade ímpar [os termos serão definidos mais adiante, mas adiantamos que isto significa que há vértices com número ímpar de arcos incidentes].

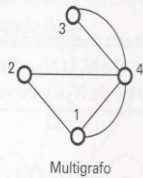
- 1847: G.R.Kirchnoff desenvolveu a teoria de árvores para trabalhar com aplicações em circuitos elétricos.
- 1852: F. Guthrie apresentou informalmente o problema das 4 cores: São apenas 4 cores suficientes para colorir qualquer mapa em superfície plana [fronteiras têm que ser linhas contínuas com comprimento maior que 0: não podem ser apenas um ponto], de maneira que regiões fronteiriças recebam cores distintas? [isto só conseguiu ser provado em  $\geq 1976$ ].
- 1859: Sir W.R. Hamilton inventou um jogo que consistia em um dodecaedro com 12 faces e 20 vértices, com cada face sendo um pentágono regular e três arestas se encontrando em cada vértice e os vértices foram rotulados com nomes de 20 cidades importantes. O objetivo do jogo é achar uma rota pelas arestas do dodecaedro passando por cada vértice apenas uma vez. (A solução para este problema específico é fácil de se obter. No entanto, ainda não se tem uma condição necessária e suficiente para se verificar a existência de um ciclo hamiltoniano [definição mais adiante] em um grafo arbitrário.)
- Depois desta época pouca coisa foi investigada em Teoria dos Grafos por quase um século.
- O interesse ressurgiu na década de 20 com os estudos de D. König que se transformaram em um livro, publicado em 1936.

<p>G      E      W</p> <p>A      B      C</p>	<p>• Problema das Utilidades</p> <p>Considere 3 casas (A,B,C), cada uma com três utilidades: água (W), gás (G) e eletricidade (E). As utilidades estão conectadas às casas por meio de fios e canos. Considerando que todos os fios e canos estão no mesmo plano, é possível fazer as instalações sem cruzá-los?</p>
---	--

## 6.2. Conceitos Básicos de Grafos e Digrafos

• Um **grafo**  $G$  é um objeto matemático constituído por um par  $(V,E)$ , onde  $V$  é um conjunto de elementos chamados de **vértices** (ou **nodos**) (que modelam locais ou estados ou tempos ou entidades, de problemas reais) e  $E$  é um conjunto de elementos chamados de **arestas** (ou **arcos**), cada aresta  $e_k$  modelando a relação de um vértice  $v_i$  para um vértice  $v_j$ , ditos **extremos** de  $e_k$ . Os vértices extremos de uma aresta são ditos **incidentes** nela, e as arestas que se ligam a um vértice são ditas **incidentes** nele. Dois vértices que são incidentes a uma (i.é, estão ligados a uma) mesma aresta são ditos **vértices adjacentes**. Duas arestas que são incidentes a um mesmo vértice são ditas **arestas adjacentes**.

	<p>Exemplo:</p> <p><math>G = (V,E)</math> (grafo)</p> <p><math>V = \{1, 2, 3, 4, 5, 7\}</math> (vértices)</p> <p><math>E = \{a, b, c, d, e, f\}</math> (arcos)</p> <p>5,7 são os extremos da aresta a.</p> <p>5,7 são incidentes na aresta a; a,d são incidentes no vértice 5.</p> <p>a,d são arestas adjacentes; 5,7 são vértices adjacentes.</p>
---	--

 <p>Multigrafo</p>	<ul style="list-style-type: none"> <li>• Um grafo <math>G = (V, E)</math> (como o ao lado) é um <b>multigrafo</b> se existem mais de uma aresta ligando o mesmo par de vértices.</li> <li>• Uma aresta do tipo <math>\{v_i, v_i\}</math> é denominada <b>auto-laço</b>.</li> <li>• Arestas que possuem os mesmos vértices extremos <math>v_i \neq v_j</math> são ditas <b>paralelas</b> ou <b>múltiplas</b>.</li> <li>• Um grafo (como o acima) sem auto-laços nem arestas paralelas é denominado <b>grafo simples</b>.</li> </ul>
---	--

- O número de vértices de um grafo  $G$  é denotado por  $n = |V|$ . O valor  $n$  também é conhecido como

**ordem** do grafo. (No multigrafo acima, é 4.)

- O número de arestas de um grafo é denotado por  $m = |E|$ . (No multigrafo acima, é 6.)
- Se  $|V|$  e  $|E|$  são finitos, o grafo  $G = (V, E)$  é **finito**. Caso contrário é dito **infinito**. Estudaremos apenas grafos finitos.

• O número de arestas incidentes a um vértice  $v$  é denominado **grau**( $v$ ) (ou **valência**) e representado por  $d(v)$ . (No multigrafo acima,  $d(4) = 5$ .)

•  $\delta(G)$  é o **grau mínimo** de  $G$ , o grau do vértice de menor grau. (No multigrafo acima, é 2.)

•  $\Delta(G)$  é o **grau máximo** de  $G$ , o grau do vértice de maior grau. (No multigrafo acima, é 5.)

• **Vértice isolado** é o vértice que não possui arestas incidentes (tem grau 0).

• Vértice **folha** ou **terminal** é o vértice que possui grau 1.

• **Vizinhos** de um vértice são os vértices adjacentes a ele. (No grafo acima, 3 e 4 são vizinhos.)

• Pares de vértices (ou de arestas) não adjacentes são denominadas **independentes**. (No grafo acima, qualquer uma das arestas de 3 para 4, e a aresta de 1 para 2, são independentes entre si.)

• Um conjunto de vértices (ou arestas) é **independente** se nenhum par de seus elementos é adjacente.

• **Teorema: Seja  $G = (V, E)$  um grafo simples com  $n$  vértices e  $m$  arestas. Então**

$$\sum_{v \in V} d(v) = 2m$$

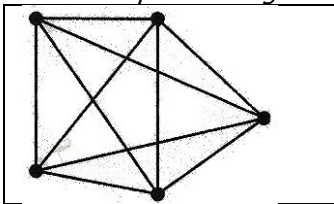
**Prova:**

Cada aresta  $e$  é incidente em dois vértices  $u$  e  $v$ , sendo contabilizada no cômputo do grau de  $u$  e também de  $v$ .

• **Auto-laço** é uma aresta com extremos idênticos ( $u, u$ ). **Link** é uma aresta com extremos diferentes  $v_i \neq v_j$ . Portanto, arestas múltiplas são links com mesmos extremos:

• Um grafo é **simples** se não possuir auto-laço nem arestas múltiplas.

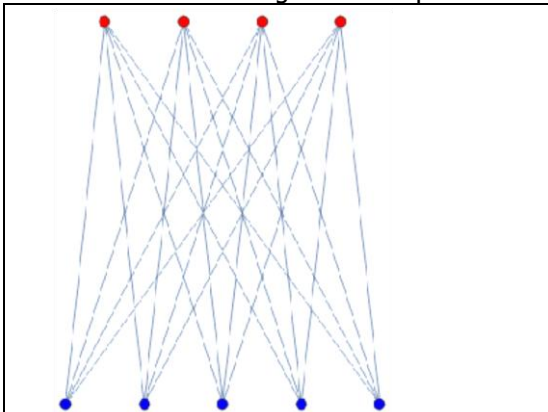
*Classes especiais de grafos:*



• **Grafo completo** de  $n$  vértices (também chamado de **n-clique**) é um grafo simples em que cada um dos seus  $n$  vértices se liga por 1 aresta a todos os outros  $n-1$  vértices, cada vértice tendo grau  $n-1$ . (O grafo ao lado é um 5-clique)

• **Grafo vazio** é um grafo sem arestas.

• **Grafo trivial** é um grafo com apenas um vértice.



• **Grafo bipartido** é aquele em que o conjunto de vértices pode ser particionado em dois subconjuntos  $X$  e  $Y$ , tal que cada aresta do grafo tem um extremo em  $X$  e o outro em  $Y$ . No exemplo ao lado,  $X$  ( $Y$ ) é o conjunto dos vértices vermelhos (azuis), os quais ficam na parte superior (inferior) do grafo.

• **Grafo bipartido completo:** é um grafo bipartido com bipartição  $(X, Y)$  em que cada vértice de  $X$  é adjacente a cada um de todos os vértices de  $Y$ . (Exemplo: ao lado). Se chamarmos  $|X|$  de  $m$  e  $|Y|$  de  $n$ , então denotamos tal grafo por  $K_{m,n}$ . (O exemplo ao lado é um grafo  $K_{4,5}$ .)

• **Grafo k-partido:** existe uma partição

$$P = \{Y_i \mid i = 1, \dots, k, Y_i \cap Y_j = \emptyset, i \neq j\}$$

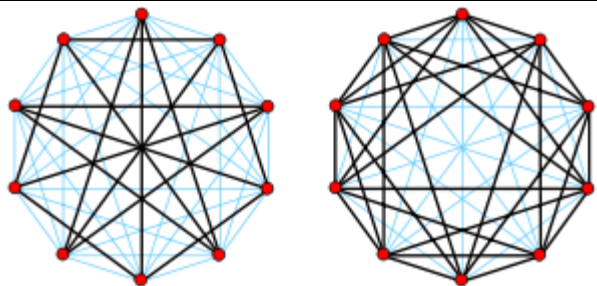
do seu conjunto de vértices, tal que não existam ligações entre elementos de um mesmo  $Y_i$ .

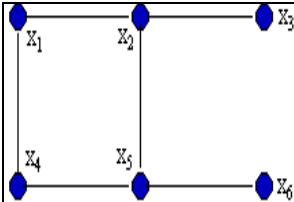
• **Grafo regular** é aquele em que todos os vértices têm mesmo grau. Se o grau for  $k$ , chamamos o grafo de **k-regular**. (Exemplo: o grafo bipartido completo, acima, é 4-regular)

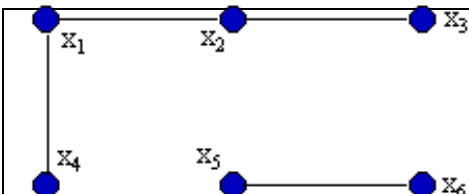
• **Grafo rotulado** em vértices (ou arestas) é aquele em que cada vértice (ou aresta) é atribuído um rótulo tal como Brasília (ou Ponte da Amizade) que será seu nome. (Exemplo: o primeiro grafo desta seção é rotulado nos vértices (1, 2, etc.), e também é rotulado nas arestas (a, b, etc.))

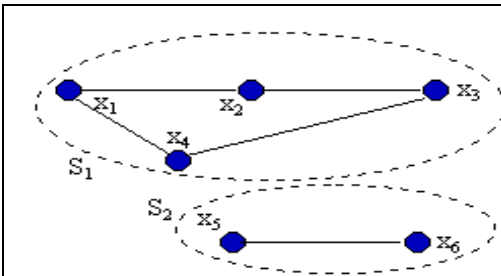
• **Grafo valorado** é aquele em que cada aresta (ou vértice) tem um número real associado a ele, representando um custo ou ganho em se passar por ele. (Exemplos bem mais abaixo, nas definições de problema do caminho mais curto e da árvore geradora mínima.)

• **Grafo altamente irregular** é aquele em que cada um de seus vértices é adjacente a vértices de graus diferentes entre si.

	<ul style="list-style-type: none"> <li>• Dado um grafo <math>G</math>, seu <b>grafo complementar</b> <math>\bar{G}</math> é o grafo que contém as ligações que não estão em <math>G</math>.</li> </ul> <p>Note que:</p> <ul style="list-style-type: none"> <li>- O complementar de um grafo sem arestas é um grafo completo e vice versa.</li> <li>- Um conjunto de vértices independentes em um grafo é um clique no grafo complementar e vice versa.</li> </ul>
---	---

	<ul style="list-style-type: none"> <li>• Um grafo é dito <b>conexo</b> se houver um caminho entre quaisquer dois de seus vértices,</li> </ul>
---	---

	<ul style="list-style-type: none"> <li>• e é dito <b>desconexo</b> se não houver um caminho entre quaisquer dois de seus vértices.</li> </ul>
---	---

	<ul style="list-style-type: none"> <li>• Um grafo desconexo é formado por pelo menos dois subgrafos conexos, disjuntos em relação aos vértices. Cada um destes subgrafos conexos é dito ser uma <b>componente conexa</b> do grafo.</li> </ul>
--	---

- Um vértice é chamado de um **vértice de corte** se sua remoção (juntamente com as arestas a ele conectadas) aumenta o número de componentes conexas do grafo. Exemplo: o vértice 4 na definição de multigrafo, acima.
- Uma aresta é chamada de **aresta ponte** (também conhecida por **aresta de corte** ou **istmo**) se sua remoção aumenta o número de componentes conexas do grafo. Exemplo: a aresta  $x_1x_2$  na definição de grafo conexo, acima.

- Dois grafos  $G$  e  $H$  são **idênticos** se
 
$$V(G) = V(H);$$

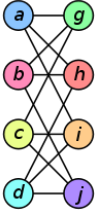
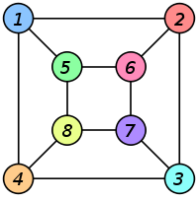
$$E(G) = E(H);$$
 e  $G$  e  $H$  têm a mesma sequência de graus.

Note que  $(u,v) \in E(G) \leftrightarrow (u,v) \in E(H)$

Grafos idênticos podem estar "graficamente distorcidos" e não ser muito fácil de você olhar para eles e logo perceber que são idênticos. Mas ambos podem ser representados por um mesmo diagrama. (Exemplo: os dois grafos abaixo, se já tivéssemos mudado os rótulos dos vértices do segundo grafo de 1,2,3,4,5,6,7,8 para a,h,d,i,g,b,j,c, respectivamente.)

- Um **isomorfismo** (denotado  $G \approx H$ ) entre dois grafos  $(G,H)$  é uma bijeção  $f$  de  $V(G)$  em  $V(H)$  tal que
 
$$(u,v) \in E(G) \leftrightarrow (f(u),f(v)) \in E(H)$$
 isto é, para quaisquer dois vértices  $u$  e  $v$  de  $G$ , eles são adjacentes em  $G$  se e somente se  $f(u)$  e  $f(v)$  são adjacentes em  $H$ . Dois digrafos são **isomórficos** se existe um isomorfismo entre os grafos a eles equivalentes e se é preservada a ordem dos vértices de cada arco.

Grafo G	Grafo H	Um isomorfismo entre G e H
---------	---------	----------------------------

		$f(a) = 1$ $f(b) = 6$ $f(c) = 8$ $f(d) = 3$ $f(g) = 5$ $f(h) = 2$ $f(i) = 4$ $f(j) = 7$
---	---	--

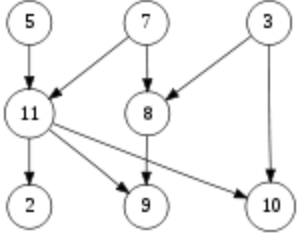
Compare esta definição com a de grafos idênticos. Obviamente, grafos idênticos são isomórficos. No entanto, o reverso não é verdade. (No exemplo acima, é possível alterar o nome dos vértices do grafo H de forma que este fique idêntico a G, mas isso nem sempre é possível. Exemplo: grafo G =  $\{(1,2), (1,3), (1,4), (2,3)\}$  e grafo H =  $\{(1,2), (1,3), (2,3), (3,4)\}$ . Desenhe os diagramas dos dois grafos explique porque são isomórficos, e porque não são idênticos.)

O isomorfismo de grafos preserva as propriedades:

- Simetria:  $G \approx H \leftrightarrow H \approx G$
- Reflexividade:  $G \approx G$
- Transitividade:  $(G \approx H) \wedge (H \approx I) \leftrightarrow (G \approx I)$

Se  $G \approx H$ , valem as seguintes proposições:

- G e H têm o mesmo número de vértices
- G e H têm o mesmo número de arestas
- G e H têm a mesma sequência de graus

	<p>• <b>Grafo direcionado</b> ou <b>digrafo</b> é aquele que tem todas suas arestas direcionadas. Prefere-se chamar de <b>arcos</b> as arestas direcionadas, e de <b>A</b> o conjunto desses arcos. Cada arco é representado por um par ordenado, onde o primeiro elemento é a origem do arco e segundo é seu final. No exemplo ao lado,</p> <p><math>G = (V, A)</math>  <math>V = \{2, 3, 5, 7, 8, 9, 10, 11\}</math>  <math>A = \{(3, 8), (3, 10), (5, 11), (7, 8), (7, 11), (8, 9), (11, 2), (11, 9), (11, 10)\}</math>.</p>
--	---

[Alguns autores descuidados escrevem "digrafo", com acento, o que é erro que você deve evitar, pois corresponde ao conceito "duas letras (di = dois; grafos = letra) com apenas um só fonema", enquanto "digrafo" é aportuguesamento do inglês "digraph" ("directed graph", "grafo direcionado")]

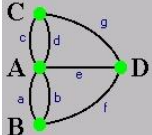
- **Digrafo simples** é um digrafo que não tem auto-laços e os arcos são todos distintos. (Exemplo acima.)
- Digrafo simples **acíclico** é um digrafo simples que não tem ciclos. (Exemplo acima.)
- O grafo G obtido removendo-se as orientações dos arcos de um digrafo D é chamado de **grafo equivalente** a D. Se D for simples, G pode não o ser. (Você mesmo ache um exemplo disso.)

Cada vértice  $v$  de um digrafo  $(V, A)$  tem um **grau de entrada**  $\text{grauent}(v)$  ou  $\text{grau}^+(v)$  (que é o número de arcos que chegam nele) e um **grau de saída**  $\text{grausai}(v)$  ou  $\text{grau}^-(v)$  (que é o número de arcos que saem dele), onde

$$\sum \text{grauent}(v_i) = \sum \text{grausai}(v_i) = |A|$$

- Um digrafo D é chamado de **fracamente conectado** (ou apenas **conectado**) se o grafo equivalente é um grafo conexo. Um digrafo é **fortemente conectado** ou **forte** se ele tem um caminho orientado de  $u$  a  $v$  e um caminho orientado de  $v$  a  $u$  para cada par de vértices  $u, v$ .

### Representação de grafos em computadores:

	Representação no computador (linhas abaixo):																																
<table><tr><td></td><td>A</td><td>B</td><td>C</td><td>D</td></tr><tr><td>A</td><td>0</td><td>2</td><td>2</td><td>1</td></tr><tr><td>B</td><td>2</td><td>0</td><td>0</td><td>1</td></tr><tr><td>C</td><td>2</td><td>0</td><td>0</td><td>1</td></tr><tr><td>D</td><td>1</td><td>1</td><td>1</td><td>0</td></tr></table>		A	B	C	D	A	0	2	2	1	B	2	0	0	1	C	2	0	0	1	D	1	1	1	0	<ul style="list-style-type: none"><li>• <b>Matriz de adjacência (<math>V \times V</math>):</b> as linhas e as colunas estão associadas aos vértices. O elemento da linha <math>i</math> e coluna <math>j</math> é o número de arestas ligando <math>v_i</math> a <math>v_j</math>. A matriz é simétrica (só a triangular superior precisa ser armazenada). Se não há auto-laços, a diagonal principal só tem 0's. Se, ademais, não há arestas paralelas (o grafo é direto), a matriz só tem 0's e 1's.</li></ul>							
	A	B	C	D																													
A	0	2	2	1																													
B	2	0	0	1																													
C	2	0	0	1																													
D	1	1	1	0																													
<table><tr><td></td><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td><td>f</td><td>g</td></tr><tr><td>A</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr><tr><td>B</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td></tr><tr><td>C</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td></tr></table>		a	b	c	d	e	f	g	A	1	1	1	1	1	0	0	B	1	1	0	0	0	1	0	C	0	0	1	1	0	0	1	<ul style="list-style-type: none"><li>• <b>Matriz de incidência (<math>V \times E</math>):</b> as linhas estão associadas aos vértices e as colunas estão associadas às arestas. Chamemos de <math>m_{ij}</math> ao elemento da linha <math>i</math> e coluna <math>j</math>. <math>m_{ij}</math> é o número de vezes que <math>v_i</math> e <math>e_j</math> são incidentes.</li></ul>
	a	b	c	d	e	f	g																										
A	1	1	1	1	1	0	0																										
B	1	1	0	0	0	1	0																										
C	0	0	1	1	0	0	1																										

D 0 0 0 0 1 1 1	
Adj[A]: $C \rightarrow C \rightarrow B \rightarrow B \rightarrow D \searrow$ Adj[B]: $A \rightarrow A \rightarrow D \searrow$ Adj[C]: $A \rightarrow A \rightarrow D \searrow$ Adj[D]: $A \rightarrow B \rightarrow C \searrow$	<ul style="list-style-type: none"> <li>• <b>Listas de Adjacência (<math>V \times V^*</math>):</b> um array Adj de <math> V </math> listas, uma para cada vértice de V. Para cada v em V, Adj[v] consiste da lista (em ordem arbitrária?) de todos os vértices adjacentes a v.</li> </ul>

### Representação de digrafos em computadores:

	Representação no computador (linhas abaixo):
<pre> 2 3 5 7 8 9 10 11 2 0 0 0 0 0 0 0 -1 3 0 0 0 0 1 0 1 0 5 0 0 0 0 0 0 0 1 7 0 0 0 0 1 0 0 1 8 0 -1 0 -1 0 1 0 0 9 0 0 0 0 -1 0 0 -1 10 0 -1 0 0 0 0 0 -1 11 1 0 -1 -1 0 1 1 0 </pre>	<ul style="list-style-type: none"> <li>• <b>Matriz de adjacência (<math>V \times V</math>):</b> as linhas ("De") e as colunas ("Para") estão associadas aos vértices. <math>m(v_i, v_j) = 1</math> se há aresta de <math>v_i</math> para <math>v_j</math>; <math>m(v_i, v_j) = -1</math> se há aresta de <math>v_j</math> para <math>v_i</math>; <math>m(v_i, v_j) = 0</math> no caso restante.</li> </ul>
Adj[2]: $\searrow$ Adj[3]: $8 \rightarrow 10 \searrow$ Adj[5]: $11 \searrow$ Adj[7]: $8 \rightarrow 11 \searrow$ Adj[8]: $9 \searrow$ Adj[9]: $\searrow$ Adj[10]: $\searrow$ Adj[11]: $2 \rightarrow 9 \rightarrow 10 \searrow$	<ul style="list-style-type: none"> <li>• <b>Listas de Adjacência (<math>V \times V^*</math>):</b> um array Adj de <math> V </math> listas, uma para cada vértice de V. Para cada v em V, Adj[v] consiste da lista (em ordem arbitrária?) de todos os vértices adjacentes a v no sentido da seta do arco.</li> </ul>

- Um grafo H é um **subgrafo** de G ( $H \subseteq G$ ) se  $V(H) \subseteq V(G)$  e  $E(H) \subseteq E(G)$ .
- Quando  $H \subseteq G$  e  $H \neq G$ , denotamos  $H \subset G$  e dizemos que H é **subgrafo próprio** de G.
- Se H é um subgrafo de G então G é um **supergrafo** de H
- Um **subgrafo gerador** de G é um subgrafo H com  $V(H) = V(G)$
- Seja  $V'$  um subconjunto não vazio de V. O subgrafo de G cujo conjunto de vértices é  $V'$  e o conjunto de arestas é o conjunto de todas as arestas de G com ambos extremos em  $V'$ , é chamado de **subgrafo de G induzido pelo conjunto de vértices  $V'$** . Denotamos por  $G[V']$  o subgrafo induzido de G por  $V'$ .
- Seja  $E'$  um subconjunto não vazio de arestas de E. O subgrafo de G cujo conjunto de vértices é o conjunto dos extremos das arestas em  $E'$  é chamado de **subgrafo de G induzido pelo conjunto de arestas  $E'$** .
- $G[V \setminus V']$ , também denotado por  $G - V'$ , é o subgrafo obtido a partir de G pela remoção dos vértices em  $V'$  e suas arestas incidentes.
- $G - E'$  é o subgrafo gerador de G com conjunto de arestas  $E \setminus E'$ .
- $G + E'$  é o grafo obtido a partir de G adicionando um conjunto de arestas  $E'$ .
- Sejam os subgrafos  $G_1, G_2 \subseteq G$ .  $G_1$  e  $G_2$  são **disjuntos (em vértices)** se  $V(G_1) \cap V(G_2) = \emptyset$ . E são **disjuntos (em arestas)** se  $E(G_1) \cap E(G_2) = \emptyset$ .

### GUIA DE ESTUDO:

No diagrama da definição do "problema do caminho mais curto" (abaixo): Quais são os vértices? E as arestas? Quais os extremos da aresta de maior peso? Que vértices incidem nessa aresta? Que vértices são adjacentes via essa aresta? Que arestas incidem no vértice A? Que arestas são adjacentes via esse vértice? Este é um multigrafo? Tem algum auto-laço? Tem arestas paralelas? É um grafo simples? É finito? Qual é a ordem do grafo? Qual o grau do vértice A? Qual o grau mínimo de G? Qual o grau máximo de G? Há algum vértice isolado? Há algum vértice folha ou terminal? Quais são os vizinhos do vértice A? Os vértices A e D são independentes ou vizinhos? As arestas de maior e de menor peso são independentes ou adjacentes? Sendo este um grafo simples, vale o teorema que diz que a soma dos graus dos vértices é o dobro do número das arestas?

Desenhe um grafo completo com 6 nodos e verifique se o número de arcos é  $(6+1) \times 6/2 = 21$  Desenhe um grafo 4-partido. Desenhe um grafo 2-regular com 6 vértices. Desenhe um grafo conexo. Desenhe um



grafo com 2 partições desconexas. Insira um vértice no grafo acima, depois acrescente o menor número de arestas que o torne conexo. Aponte um vértice de corte e uma aresta ponte, no grafo modificado.

Dê exemplo de dois grafos idênticos, mas um pouco difíceis de reconhecer isto à primeira vista.

Desenhe 2 grafos não idênticos mas isomórficos, depois prove que realmente são isomórficos.

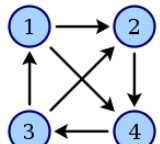
Dê exemplo de um digrafo que seja cíclico, outro que seja acíclico.

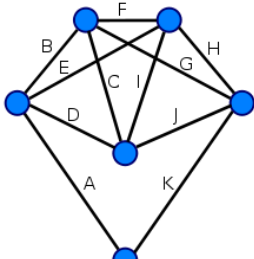
Dê exemplo de um digrafo conexo, outro de um desconexo. Escreva a matriz de adjacência e a lista de adjacência para o digrafo desconexo.

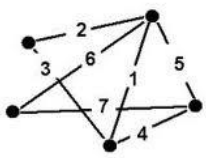
Divida um grafo de 7 vértices em  $G$ , com 4 vértices, e  $H$ , com 3 vértices, podendo ter uma pequena interseção entre eles. Agora, ache  $G \cap H$ .

## 6.3. Percursos em Grafos em Geral e em Cliques

- Um **passeio** (walk) é uma sequência qualquer de arestas (arcos) adjacentes que ligam dois vértices  $v_0$  e  $v_k$ . (Há uma sequência não nula  $W = v_0 e_1 v_1 e_2 v_2 \dots e_k v_k$  cujos termos são alternadamente vértices e arestas). (Note que não se proibiu passar mais de 1 vez pelo mesmo vértice). (Exemplo no grafo das 7 pontes de Königsberg:  $AcCdAbBbAeD$  é um passeio desde  $A$  até  $D$ .)
- Um **ciclo** é um passeio simples e fechado (o vértice inicial é o mesmo que o vértice final). (Exemplo no mesmo grafo:  $AcCdAbBbA$  é um ciclo desde  $A$  até  $A$ .)
- Um passeio é dito ser **elementar** se não passa duas vezes pelo mesmo vértice (Exemplo no mesmo grafo:  $AcCdGfB$  é um passeio elementar desde  $A$  até  $B$ .)
- Um passeio é dito ser **simples** (trilha) se não passa duas vezes pela mesma aresta. (Exemplo no mesmo grafo:  $AaBfDeAcGd$  é uma trilha desde  $A$  até  $D$ . Note que passou 2 vezes pelos vértices  $A$ ,  $D$ .)
- Em um digrafo, um **caminho** é um passeio no qual todos os arcos possuem a mesma orientação. (Exemplo no diagrama da definição de digrafo: 5, arco, 11, arco, 10) Um caminho não repete vértices nem arestas. Em um grafo não direcionado, a relação caminho é uma equivalência, pois é reflexiva ( $\text{caminho}(u,u)$ ), simétrica ( $\text{caminho}(u,v)$  ssse  $\text{caminho}(v,u)$ ) e transitiva ( $\text{caminho}(x,y)$  e  $\text{caminho}(y,z)$  implicam  $\text{caminho}(x,z)$ ).

	<ul style="list-style-type: none"> <li>Em um digrafo, um <b>circuito</b> é um caminho simples e fechado, retornando a qualquer vértice por onde o começemos. (Exemplo: no grafo ao lado, um circuito passará pelos vértices 1,2,4,3 e voltará ao vértice 1, sempre seguindo os arcos na direção correta.)</li> </ul>
---	--

	<ul style="list-style-type: none"> <li>Um grafo conexado <math>G(V,A)</math> é dito ser <b>euleriano</b> se existe um ciclo que contém todas as arestas de <math>G</math>. Exemplo1: Cada vértice do grafo ao lado tem um grau par, portanto este é um grafo euleriano; realmente, seguindo as arestas em ordem alfabética obtém-se um circuito/ciclo euleriano. Exemplo2: No clique <math>K_5</math> do Teorema de Ore (abaixo), se numerarmos os vértices como 1,2,3,4,5 no sentido dos ponteiros do relógio, o ciclo euleriano será 1,2,3,4,5,1,3,5,2,4,1.)</li> </ul>
---	---

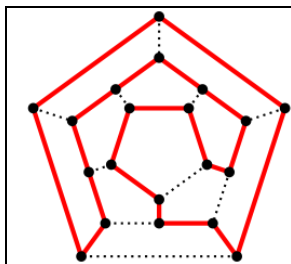
	<ul style="list-style-type: none"> <li>Um grafo conexado e não-euleriano, <math>G</math>, é <b>semi-euleriano</b> se existe um passeio simples contendo todas as arestas de <math>G</math>. No grafo ao lado, se seguirmos as arestas na ordem 1,2,3,4,5,6,7, teremos passado por todas as arestas, portanto o grafo é semi-euleriano. Mas não fizemos um circuito, pois passamos mais de 1 vez em alguns vértices. Na verdade, o grafo não é euleriano.</li> </ul>
---	---

• **Teorema (Euler 1736)** (pronuncie como "Óilêr"): Um grafo conexado  $G$  é euleriano se e somente se o grau de cada um de seus vértices é par.

• Corolário: Um grafo conexado  $G$  é euleriano se e somente se ele pode ser decomposto em ciclos.

• Corolário II: Um grafo conexado  $G$  é semi-euleriano se e somente se ele possui exatamente 2 vértices de grau ímpar.

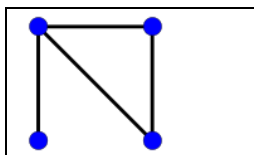
• **Teorema:** Um grafo completo de  $n$  vértices tem  $(n-1)!!$ s circuitos hamiltonianos.



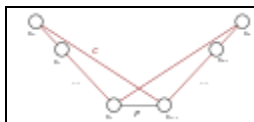
• Um grafo  $G(V,A)$  é dito ser **hamiltoniano** se existe um ciclo que passa exatamente uma vez em cada um dos vértices de  $G$ . (O ciclo é uma sucessão de arestas adjacentes que visita todos os vértices do grafo uma só vez, sendo o último vértice visitado adjacente ao primeiro.) Todo grafo completo (clique) que contém mais de 2 vértices é hamiltoniano.

Algoritmos fáceis para determinar o circuito hamiltoniano de menor custo num grafo ponderado (problema do caixeiro viajante, TSM, TSP):

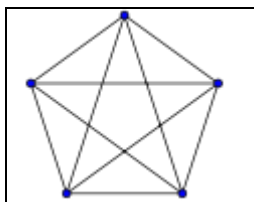
- **Alg. Força Bruta:** Ache todos os possíveis circuitos Hamiltonianos no grafo, encontre o peso total de cada um, forme uma lista de todos os circuitos e seus pesos totais, e escolha o melhor. Exato, mas leva um tempo impraticável.
- **Alg. Cidade (ou vizinho) Mais Próxima:** O vendedor escolhe um vértice de partida, e forma um circuito que começa e termina nele e sempre, à medida que visitava vértices, sempre escolheu a aresta de menor peso que saia do vértice que estivesse em foco, tendo o cuidado de nunca visitar um vértice duas vezes até que tenha visitado todos eles. Isso é rápido e fácil, e geralmente dá uma solução que é muito boa, embora não garanta que é a ótima.
- **Alg. Arestas Ordenadas** (de menor a maior): nesta ordem, "agarre" as arestas até que você tenha um circuito completo. A vantagem é que você pegará sempre a aresta com o menor peso que ainda não tinha sido agarrada, tendo cuidado para que o agarrar não irá formar um circuito que não passa por todos os vértices ou causará um vértice ser tocado por uma terceira aresta. Como o algoritmo de vizinho mais próximo, isso é rápido e fácil, e geralmente dá uma solução que é muito boa, embora não garanta que é a ótima.



• Um grafo  $G(V,A)$  é dito ser **semi-hamiltoniano** se não é hamiltoniano e existe um passeio que passa exatamente uma vez em cada um dos vértices de  $G$ .

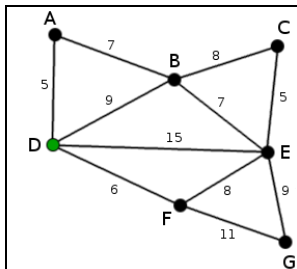


• **Teorema (Dirac 1952):** Uma condição suficiente, mas não necessária, para que um grafo simples  $G$  com  $n (>2)$  vértices seja hamiltoniano é que o grau de todo vértice de  $G$  seja  $\geq n/2$ .



• **Teorema (Ore 1960):** Uma condição suficiente, mas não necessária, para que um grafo simples  $G$  com  $n (>2)$  vértices seja hamiltoniano é que a soma dos graus de cada par de vértices não adjacentes seja no mínimo  $n$ .

(Exemplo: a condição é satisfeita no clique  $K_5$  ao lado. E, se numerarmos os vértices como 1,2,3,4,5 no sentido dos ponteiros do relógio, o ciclo será 1,2,3,4,5,1.)



• O **problema do caminho mais curto**: consiste na minimização do custo total de travessia de um grafo ponderado (com custos associados a cada aresta) desde um vértice origem até um vértice destino. Se for oferecida como optativa a disciplina Análise (da complexidade) e Projeto de Algoritmos (do Bacharelado em Ciência da Computação, da UFPB), você poderá aprender e implementar algoritmos (tais como o de **Dijkstra** e o de **Bellman-Ford**) que resolvem o problema de forma muito eficiente.  
(Exemplo: ao lado, o caminho mínimo entre D e E não é D-E, mas sim D-F-E, com uma custo total de  $6+4 = 14$ .)

• O **problema do carteiro chinês**: consiste em encontrar um caminho mais curto ou um circuito fechado que, pelo menos uma vez, visite cada aresta de um grafo conectado. (Sim, quando o grafo possui um circuito euleriano (um passeio fechado que abrange toda aresta uma vez), esse circuito é uma solução ótima.)

EXEMPLO: Grafo não direcionado. Você tem 4 vértices 1,2,3,4. Os arcos, não direcionados, têm

comprimentos:  $(1,2) = 3$ ;  $(1,3) = 12$ ;  $(1,4) = 10$ ;  $(2,3) = 4$ ;  $(3,4) = 5$ . Desenhe o grafo. O carteiro precisa sair do vértice 1 e voltar a ele no final, passando por cada arco pelo menos 1 vez. Qual o passeio de menor comprimento total? Resposta: passar nos vértices 1,2,3,4,1,2,3,2,1, percorrendo  $12+5+10+3+4+4+3 = 41$  unidades de comprimento.

• O **problema do caixeiro viajante**: (TSM = Travelling SalesMan; TSP = Travelling Sales Person) consiste na procura de um circuito que possua o menor comprimento total, começando numa cidade qualquer, entre várias, visitando cada cidade precisamente uma vez e regressando à cidade inicial. Ver algoritmo aproximado, acima.

EXERCÍCIOS: Faça os exercícios 1 até 13, que estão ao final da seção 6.4.

## 6.4. Árvores e Árvores Geradoras

Um grafo conexo que não contém ciclos é chamado de **árvore**. Um grafo que não contém ciclos é uma **floresta** (portanto, uma floresta é uma união disjunta de árvores; e corresponde a um grafo disjunto; note que estamos falando de grafos [não de digrafos], portanto as arestas não são direcionadas).

Seguindo o costume, chamaremos de **nodos** aos vértices de uma árvore. Uma árvore é denominada **enraizada** se um nodo é escolhido como especial, passando a ser chamado de **raiz** da árvore. Uma árvore que não é enraizada é denominada **livre**. Os nodos vizinhos à raiz são chamados de seus **filhos** ou ramos, e ela chamada de **pai** deles. Estes filhos levam a outros nodos que também possuem outros **filhos** deles, que os têm por **pais**. E assim por diante. Os nodos que não possuem filhos são conhecidos como **folhas** ou nodos- terminais. Para cada folha, existe um só caminho entre a raiz e ela.

**Teorema:** Num grafo que é uma árvore, toda sua aresta é uma aresta de corte (ver definição, acima).

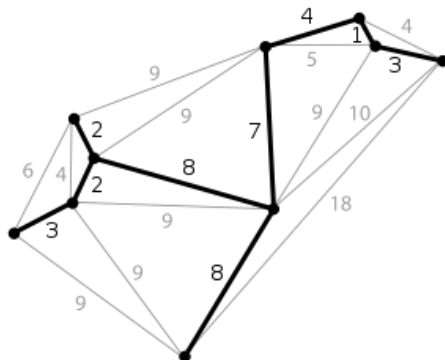
**Teorema:** Se  $G$  é uma árvore com  $n$  nodos, então  $G$  possui  $n-1$  arestas.

**Teorema:** Se  $F$  é uma floresta com  $n$  nodos e  $k$  componentes conexos, então  $F$  contém  $n-k$  arestas.

**Teorema:** Seja  $G$  um grafo de ordem  $n$ .  $G$  é uma árvore se, e somente se,  $G$  é conexo e contém  $n-1$  arestas.

**Teorema:** Seja  $G$  um grafo de ordem  $n$ .  $G$  é uma árvore se, e somente se,  $G$  não possui ciclos e contém  $n-1$  arestas.

**Teorema:** Seja  $T$  uma árvore [enraizada] de ordem  $n \geq 2$ . Então  $T$  possui no mínimo 1 folha.

 <p>Neste grafo, um peso aproximadamente igual ao seu comprimento foi atribuído a cada aresta. Uma árvore geradora mínima deste grafo está em negrito.</p>	<p>Dado um grafo conexo <math>G</math>, podemos sucessivamente remover uma qualquer aresta que esteja em um ciclo, até que não mais reste nenhum ciclo. Deste modo, teremos removido o menor número de arestas <math>( E  -  V  + 1)</math> necessário para transformar o grafo em acíclico e, portanto (uma vez que também é conexo), em uma árvore que contém todos os vértices de <math>G</math> e será chamada de <b>árvore geradora</b> (ou <i>árvore extensora</i>, ou <i>árvore de cobertura</i>) de <math>G</math>. Muitas árvores diferentes (e não serão isomórficas) podem ser geradoras de um mesmo grafo. Se o grafo for ponderado (cada aresta tendo um peso que representa quão desfavorável ela é), e se atribuirmos um peso à árvore geradora que seja calculado pela soma dos pesos das arestas que a compõem, então uma <b>árvore geradora mínima</b> (ou de peso total mínimo, ou de custo mínimo) é uma árvore geradora com peso menor ou igual a cada uma de todas as outras árvores geradoras possíveis. Qualquer grafo tem uma <b>floresta de árvores mínimas</b>, que é uma união de árvores geradoras mínimas de cada uma de suas componentes conexas.</p>
---	--

**Algoritmo de Kruskal** (não vamos exigir-lo nos exames) para geração da árvore geradora mínima para um grafo:

enquanto for possível:

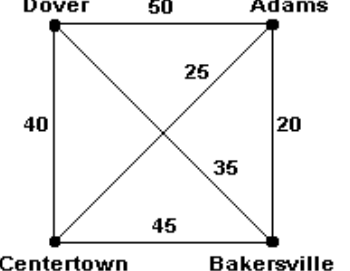
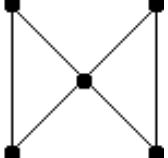
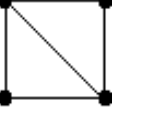
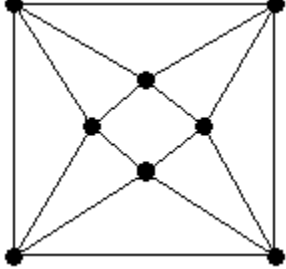
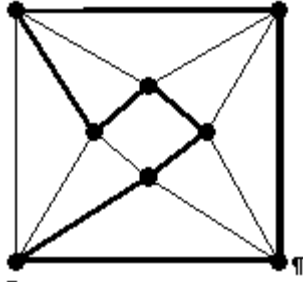
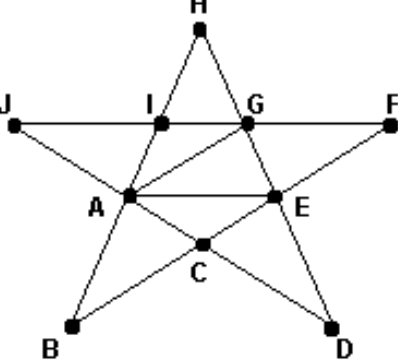



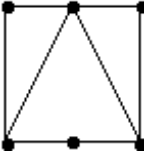
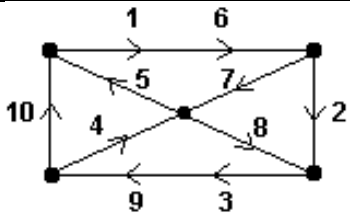
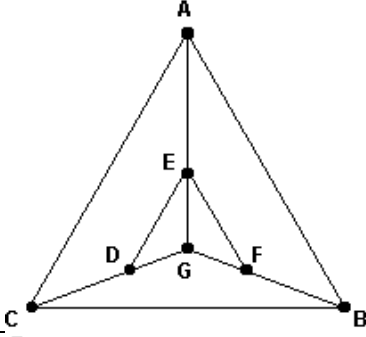
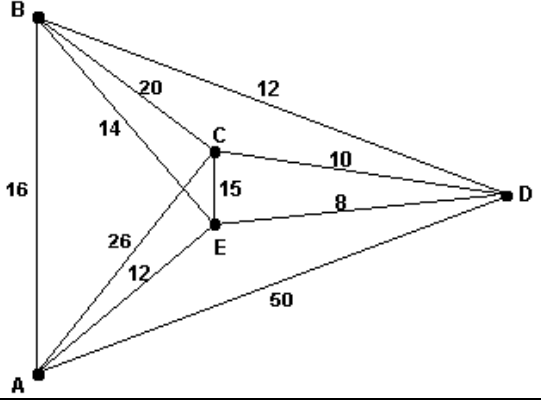
escolha uma aresta de menor peso que ainda reste no grafo e não forme um ciclo na árvore, e passe tal aresta, com seus vértices, para a árvore.

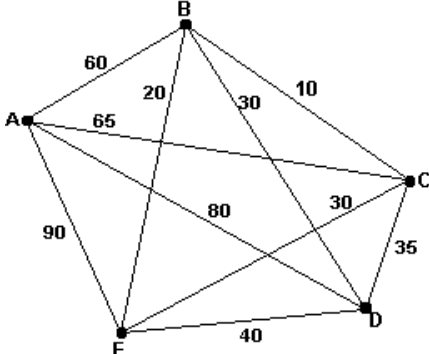
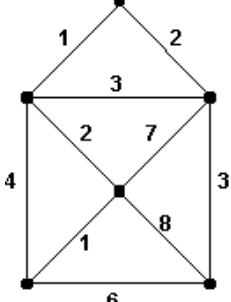
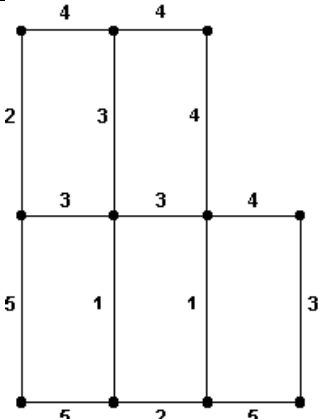
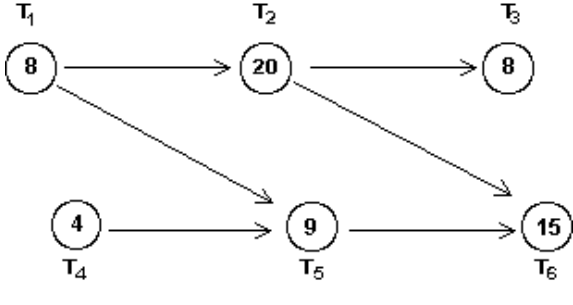
EXEMPLO: Na figura acima, escolha a aresta de peso 1, depois uma das duas arestas de peso 2, depois a outra aresta de peso 2, depois uma das de peso 3, depois a outra de peso 3. Agora, se você tentar escolher a aresta de peso 4 a NordEste, não poderá, pois fechará um ciclo; idem para a aresta de peso 4 a Oeste. Portanto, escolha a de peso 4 que fica no Norte. Neste ponto, você não poderá escolher nenhuma das arestas de peso 5 e 6, porque fechariam ciclos. Escolha a aresta de peso 7. Depois, escolha uma das arestas de peso 8, depois a outra. Agora, você será forçado a parar.

EXERCÍCIOS: resolva os exercícios abaixo, sem olhar as respostas. Só depois compare sua resposta com a deste livro (adapte a partir de

[http://christopherstrobel.cmswiki.wikispaces.net/file/view/Test%20Review%20Answer%20Key%20\(Spring%202012\).docx](http://christopherstrobel.cmswiki.wikispaces.net/file/view/Test%20Review%20Answer%20Key%20(Spring%202012).docx) )

	<p>1) Utilize o algoritmo de força bruta para resolver o problema do caixeiro viajante para o grafo das quatro cidades mostradas à esquerda.</p> <p>Resp.: Caminhos ABCDA e ACBDA têm custo 155. Caminho ABDCA tem o mínimo custo, 120.</p>
<p>Yes, for example</p> 	<p>2) Pode um grafo ter um circuito euleriano, mas não um hamiltoniano? Explique sua resposta.</p> <p>Resp.: Sim. Por exemplo, o grafo da esquerda.</p>
<p>Yes, for example</p> 	<p>3) Pode um grafo ter um circuito hamiltoniano, mas não um euleriano? Explique sua resposta.</p> <p>Resp.: Sim. Por exemplo, o grafo da esquerda.</p>
	<p>4) No grafo à esquerda, coloque em negrito arestas para indicar um circuito hamiltoniano.</p> <p>Resp.:</p> 
	<p>5) Qual é o grau (ou valência) do vértice A no grafo à esquerda?</p> <p>a) 3 b) 4 c) 5 d) 6</p> <p>Resp.: (d)</p>
	<p>6) Qual das seguintes afirmações sobre um grafo conexo sempre é verdade?</p> <p>A) Cada par de vértices é ligado por uma única aresta. B) Um caminho de arestas existe entre quaisquer</p>

	<p>dois vértices do gráfico.</p> <p>C) Há um número par de vértices do gráfico.</p> <p>D) Há um número par de arestas no gráfico.</p> <p>Resp.: B</p>
<p>I</p>  <p>II</p> 	<p>7) Qual dos grafos à esquerda tem um circuito euleriano?</p> <p>A) Gráfico I, pois há um número par de arestas em cada um de todos os seus nodos.</p> <p>B) Gráfico II, pois há um número par de arestas em cada um de todos os seus nodos.</p> <p>C) Ambos I e II</p> <p>D) Nem I nem II</p> <p>Resp.: A</p>
	<p>8) Considere o caminho representado pela sequência de arestas numerados no gráfico seguinte. Por que o caminho não representa um circuito de Euler (pronuncie como "Óilêr")?</p> <p>A) O caminho não inicia e para no mesmo vértice.</p> <p>B) O caminho não cobre todas as bordas do gráfico.</p> <p>C) O caminho utiliza algumas arestas mais do que uma vez.</p> <p>D) O caminho não toca cada vértice do gráfico.</p> <p>Resp.: C</p>
	<p>9) Se um gráfico tem 8 vértices de grau (valência) ímpar, qual é o número mínimo de arestas que têm de ser adicionadas (ou duplicadas) para que o grafo se transforme num euleriano ?</p> <p>A) 2</p> <p>B) 4</p> <p>C) 6</p> <p>D) 8</p> <p>Resp.: B</p>
	<p>10) Quais das seguintes sequências de letras descreve um circuito hamiltoniano para o grafo à esquerda?</p> <p>A) ABCDEFGA</p> <p>B) ACBAEGFDEA</p> <p>C) ACBFGDEA</p> <p>D) ABCDGEF</p> <p>Resp.: C</p>
	<p>11) Para o grafo à esquerda, qual é o custo do circuito hamiltoniano obtido usando o algoritmo do vizinho mais próximo (ainda não visitado), começando por A?</p> <p>A) 60</p> <p>B) 54</p> <p>C) 62</p> <p>D) 66</p> <p>Resp.: D (corresponde a AEDCBA)</p>
	<p>12) Para o problema do caixeiro viajante (TSM ou TSP) (circuito hamiltoniano) aplicado a seis cidades, quantas tours são possíveis (e quantas são únicas)?</p> <p>A) 60 possíveis</p> <p>B) 120 possíveis</p>

	<p>C) 360 possíveis D) 720 possíveis</p> <p>Resp.: A) 60 possíveis (<math>60/6 = 10</math> únicas)</p>
	<p>13) Para o grafo à esquerda, qual é o custo do circuito hamiltoniano obtido pelo algoritmo obtido usando o algoritmo das arestas ordenadas.</p> <p>A) 220 B) 225 C) 235 D) 295</p> <p>Resp.: C (corresponde a ACEBDA)</p>
	<p>(não vamos exigir isso nos exames:) 14) Use o algoritmo de Kruskal para achar a árvore geradora mínima para o grafo à esquerda. O custo da árvore encontrada é:</p> <p>A) 5 B) 9 C) 12 D) 15</p> <p>Resp.: B (corresponde a <math>1+1+2+2+3 = 9</math>)</p>
	<p>(não vamos exigir isso nos exames:) 15) Use o algoritmo de Kruskal para achar a árvore geradora mínima para o grafo à esquerda. O custo da árvore encontrada é:</p> <p>A) 22 B) 28 C) 32 D) 49</p> <p>Resp.: B (corresponde a: <math>1+1+2+2+3+3+3+4+4+5 = 28</math>)</p>
	<p>16) Se o digrafo especificando as restrições de ordem para uma coleção de tarefas é o mostrado à esquerda, então qual é o tempo mínimo para a conclusão do conjunto de tarefas?</p> <p>A) 64 minutos B) 43 minutos C) 36 minutos D) 28 minutos</p> <p>Resp.: B (que corresponde a <math>8+20+15 = 43</math> minutos)</p>

## Recapitulando a Unidade

Parabéns! Você concluiu a unidade VI, só falta mais uma unidade! E, se você foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter aprendido muitas coisas da parte básica da "Teoria dos Grafos" que lhe serão indispensáveis ou muito úteis em todo o resto do curso e sua vida profissional: conceitos básicos e propriedades de grafos; grafos completos (cliques), bi e k-partidos, regulares, rotulados, valorados, conexos, isométricos; conceitos básicos de digrafos; representações de grafos e digrafos em computadores; passeios, ciclos, trilhas, caminhos, circuitos, grafos eulerianos e hamiltonianos, problemas do caminho mais curto, do carteiro chinês e do caixeiro viajante. Muitas e importantes novidades. Para você treinar ainda melhor, recomendamos a Lista de Exercícios sobre Grafos, Prof. Antonio Alfredo Ferreira

Loureiro, [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE9.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE9.pdf), com soluções em [http://homepages.dcc.ufmg.br/~loureiro/md/md\\_LE9\\_Solucao.pdf](http://homepages.dcc.ufmg.br/~loureiro/md/md_LE9_Solucao.pdf).

Na próxima (e última!) unidade, a VII, você será introduzido à Teoria dos Números, um assunto teoricamente fascinante e desafiador, e também de importantíssimas aplicações práticas, por exemplo, na área de encriptação e segurança. Estudará propriedades dos números inteiros, particularmente as implicações em testar se um inteiro gigantesco é primo; divisibilidade, fatoração em primos; máximo divisor comum e mínimo múltiplo comum; aritmética modular, classes de equivalência, e congruências; exponenciação rápida; etc. Você vai gostar, e terá terminado de dominar esta disciplina!



## UNIDADE VII

# 7. Introdução à TEORIA DOS NÚMEROS



Perguntas para despertar e aguçar sua curiosidade e interesse:

1) Há algum inteiro  $n > 2$  tal que  $a^n + b^n = c^n$ , onde  $a, b, c$  são naturais? Faça umas tentativas.

2) Ao usarmos o Crivo de Eratóstenes, a cada vez mais naturais cortados vão ficando vizinhos em seqüências enormes, e os primos ficando mais extremamente raros e espaçados. Você acha que existe um natural a partir do qual não há mais nenhum primo maior que ele [todos os naturais maiores que eles formam uma seqüência de vizinhos crivados], de modo que o número de primos é finito? Por que sim ou por que não?

3) Você acha que determinar, com absoluta certeza, se um natural de 1000 dígitos é primo leva quanto tempo no mais rápido computador da loja da esquina? Horas? Anos? Milênios?

4) Você sabe uma maneira eficiente de calcular  $a^b \bmod m$  [todas as variáveis sendo naturais], quando a representação decimal de  $a$  pode ter até 10.000 dígitos,  $b$  até 8 dígitos,  $m$  até 4 dígitos?

**Nosso objetivo, nesta unidade:** é que, ao final dela, você domine as mais básicas noções e propriedades dos números inteiros, podendo responder às questões acima e outras, particularmente sabendo: como testar se um inteiro é primo ou não; de forma muito eficiente achar o máximo divisor comum (e o mínimo múltiplo comum) e onde podem ser usados em outros problemas; aritmética modular e congruências.

Mais uma vez vamos lhe lembrar: *Estamos torcendo por você. O fórum de alunos, os tutores, e eu (o professor) queremos e vamos ajudá-lo (nessa ordem), mas você tem que ser determinado e disciplinado, cada semana dedicando 4 a 8 horas para estudar este livro.*

### Conteúdo desta unidade:

#### 7.1. NÚMEROS PRIMOS

7.1.1. Testando primalidade de  $n$

7.1.2. Contando os Primos

7.1.3. Mais Algumas Poucas Coisas Sobre os Primos

#### 7.2. DIVISIBILIDADE

7.2.1. Máximo Divisor Comum (mdc) (Greatest Common Divisor. gcd)

7.2.2. Mínimo Múltiplo Comum (mmc) (Least Common Multiple. lcm)

#### 7.3. ARITMÉTICA MODULAR

7.3.1. Problema 374 do ACM Programming Contest (BigMod)

#### 7.4. CONGRUÊNCIAS

7.4.1. Operações Sobre Congruências

7.4.2. Resolvendo Congruências Lineares

7.4.3. Equações Diofantinas

#### 7.5. TRIPLAS PITAGÓRICAS



Embora os conteúdos tenham sido aprofundados usando outras fontes, os tópicos foram "pinçados" a partir do Cap. 7 "Number Theory" do livro "Programming Challenges" de Steven S. Skiena e Miguel A. Revilla (download gratuito de

[http://acm.cs.buap.mx/downloads/Programming\\_Challenges.pdf](http://acm.cs.buap.mx/downloads/Programming_Challenges.pdf)). Portanto, provavelmente só cobrimos os cerca de 30% mais fáceis da Teoria dos Números, mas que têm mais aplicação prática nas competições de programação. Uma referência mais abrangente e profunda é <http://mathworld.wolfram.com/topics/NumberTheory.html>, com centenas de artigos em dezenas de assuntos. Mas qualquer dos livros textos da disciplina cobre todas as suas 7 unidades.

## 7.0. DEFINIÇÃO: A TEORIA DOS NÚMEROS ...

[ou, simplesmente, "aritmética", ou "aritmética superior"] é o ramo da Matemática Pura que estuda propriedades dos números em geral e, em particular, dos números inteiros, bem como a larga classe de problemas que surge no seu estudo. Mesmo sendo da Matemática Pura, a Teoria dos Números tem uma extraordinária importância prática, sendo a base para toda a área de criptografia moderna (que possibilita segurança no trânsito de informações vitais pela internet), sendo também a base para se conceber alguns algoritmos aceitavelmente eficientes ao invés de impraticavelmente lentos.

Exemplo de um dos mais famosos resultados da Teoria dos Números: O **Último Teorema de Fermat**: **Não existe nenhum conjunto de inteiros positivos  $a, b, c, n$ , com  $n > 2$ , que satisfaça.**

$$a^n + b^n = c^n$$

A prova deste teorema, enunciado por Fermat em cerca de 1637, é tão difícil que somente foi achada por Wiles em 1995. E é muito longa e difícil para a discutirmos aqui.

[http://en.wikipedia.org/wiki/Fermat's\\_Last\\_Theorem#Wiles.27s\\_general\\_proof](http://en.wikipedia.org/wiki/Fermat's_Last_Theorem#Wiles.27s_general_proof) conta a história da evolução da prova ao longo dos séculos.

## 7.1. NÚMEROS PRIMOS

• **Número primo** é qualquer natural  $p \geq 2$  que somente seja divisível por si mesmo e por 1. Por exemplo: 7 é primo [porque só é divisível por si mesmo e por 1].

• **Número composto** é qualquer natural  $q \geq 2$  que não seja primo. (Isto é, além de divisível por 1 e por ele mesmo, é divisível pelo menos por algum outro natural.) Por exemplo: 6 é composto (isto é, não primo) [porque, além de divisível por si mesmo e por 1, o é por outros naturais: 2 e 3].

### Teorema Fundamental da Aritmética

([http://pt.wikipedia.org/wiki/Teorema\\_fundamental\\_da\\_aritm%C3%A9tica](http://pt.wikipedia.org/wiki/Teorema_fundamental_da_aritm%C3%A9tica)):

**Todos os números inteiros positivos maiores que 1 podem ser decompostos num produto de números primos, sendo esta decomposição única a menos de permutações dos fatores.** [Este

teorema foi exposto, pela primeira vez, no livro IX dos Elementos, de Euclides <sup>[13 volumes, escritos no ano de cerca de 300 aC]</sup>. Mais formalmente:

**Seja  $a > 1$  um inteiro positivo. Então, existem primos positivos  $p_1, p_2, \dots, p_t$  tais que  $a = p_1 p_2 \dots p_t$ , e essa decomposição é única.**

[chamamos  $p_1, \dots, p_t$  de **fatores primos** de  $a$ . Ao processo de encontrá-los, chamamos de **fatoração** (de  $a$ ) **em primos**] [Na fatoração de um número em primos poderá ser de utilidade a tabela dos primeiros 10000 números primos, em <http://primes.utm.edu/lists/small/10000.txt>]

### Demonstração:

#### Existência de uma decomposição

Será usado para esta demonstração o *Princípio da Indução Completa* (releia na Unidade III).

Para  $a=2$  existe apenas a decomposição trivial em números primos  $1 \times 2$ , já que 2 é primo. Suponhamos agora que existe uma tal decomposição para todo inteiro  $b$ ,  $2 \leq b < a$ . Mostraremos que também existe para  $a$ .

Se  $a$  é primo, admite somente a decomposição trivial  $a = 1 \times a$ .

Caso contrário, admite um divisor positivo  $b$  tal que  $1 < b < a$ . Isto é,  $a = bc$ , e temos também  $1 < c < a$ .

Pela hipótese indutiva,  $b$  e  $c$  podem ser escritos como produtos de primos, na forma  $m = p_1 p_2 \dots p_s$ ,  $c = q_1 q_2 \dots q_k$ . Substituindo, temos  $a = p_1 \dots p_s q_1 \dots q_k$ , e a referida decomposição também existe para  $a$ .

#### Unicidade da decomposição

Dado um inteiro  $a$ , ele poderia admitir, em princípio, mais de uma decomposição em produto de fatores primos. Chamemos de *comprimento de uma decomposição* o número de fatores que nela compõem. A demonstração será feita por indução no comprimento de uma decomposição de  $a$ .

Suponhamos que  $a$  admita uma decomposição do tipo  $a = p_1$ , onde  $p_1$  é primo, e que vale

$$a = p_1 = q_1 q_2 \dots q_s$$

em que  $q_1 \leq q_2 \leq \dots \leq q_s$  são primos positivos. Como  $q_1$  divide  $q_1 q_2 \dots q_s$ , então  $q_1$  também divide  $p_1$ , que é primo. Então, devemos ter  $p_1 = q_1$ . Cancelando, vem  $1 = q_2 \dots q_s$ . Se  $s > 1$ , teríamos que o primo  $q_2$  seria inversível, uma contradição. Assim,  $s = 1$  e, como já provamos que  $p_1 = q_1$ , o primeiro passo da indução está verificado.

Suponhamos agora o resultado verdadeiro para todo inteiro que admita uma decomposição de comprimento  $k \geq 1$ , e seja  $a$  um inteiro com uma decomposição de comprimento  $k+1$ . Se este inteiro  $a$  admitisse outra decomposição, teríamos

$$a = p_1 \dots p_{k+1} = q_1 \dots q_s,$$

em que  $q_1 \leq q_2 \leq \dots \leq q_s$  são primos positivos.

Como, na primeira parte,  $q_1$  divide  $p_1 \dots p_{k+1}$ , consequentemente temos que  $q_1$  divide  $p_i$  para algum  $i$  (Lema de Euclides). Como  $p_i$  é primo, devemos ter novamente que  $q_1 = p_i$ . Em particular,  $q_1 \geq p_1$ . De forma análoga, pode-se obter que  $p_1 = q_j$ , para algum  $j$ . Logo,  $p_1 \geq q_1$ . De ambas as desigualdades, vem que  $p_1 = q_1$ . Finalmente, cancelando em  $a = p_1 \dots p_{k+1} = q_1 \dots q_s$ , temos que

$$p_2 \dots p_{k+1} = q_2 \dots q_s.$$

Agora, o primeiro membro da igualdade tem uma decomposição de comprimento  $k$ , logo, da hipótese de indução, admite uma única decomposição. Assim, temos  $k = s-1$ , donde  $k+1 = s$  e  $p_i = q_i$ , para  $i = 2, \dots, k+1$ . Como já provamos que  $p_1 = q_1$ , ambas as expressões de  $a$  coincidem.

**Colorário:** Se um número primo divide o produto de dois números inteiros, então ele é divisor de um dos dois.

**Teorema de Euclides** (de cerca do ano 300 aC!): há um número infinito de primos.

**Prova:**

Suponhamos que o número de primos é finito e igual ao natural  $r$ . Chamemos o maior deles de  $p_r$ . Ordenemos e demos nomes a todos os primos, assim:  $p_1=2 < p_2=3 < \dots < p_r$ . Seja  $P = (p_1 p_2 \dots p_r) + 1$ . Evidentemente  $P$  é maior que cada um dos números primos. Temos duas possibilidades e veremos que ambas levam a uma contradição: Caso  $P$  seja primo, então, por ser maior que cada  $p_1, \dots, p_r$ , é um *novo* primo (diferente de  $p_1, \dots, p_r$ ), o que contradiz nossa suposição. E, caso  $P$  seja não primo, então  $P = (p_1 p_2 \dots p_r) + 1$  não é fatorável por nenhum dos primos  $p_1, \dots, p_r$  <sup>(\*)</sup>. Portanto,  $P$  tem que ser um *novo* primo (diferente de  $p_1, \dots, p_r$ ), o que contradiz nossa suposição. Como as 2 hipóteses possíveis levaram a contradições da suposição, esta tem que ser falsa, impossível. Portanto, o número de primos é infinito. C.Q.D.

/\* Explicação adicional: caso  $P$  seja não primo, tem que ser fatorável por primos (menores que ele mesmo), e chamemos de  $p$  um dos primos (há pelo menos um deles) que divida  $P$ ; então,  $p$  não pode ser igual ao primo  $p_1 = 2$  porque o primeiro múltiplo de  $p_1$  maior ou igual a  $P$  é  $(P-1)+p_1$ ; idem para o primo  $p_2 = 3$ ; e para o primo  $p_3 = 5$ ; ...; e para o primo  $p_r$ . Isto é,  $P = (p_1 p_2 \dots p_r) + 1$  não é fatorável por nenhum dos primos  $p_1, \dots, p_r$  \*/



(É um erro comum pensar que esta prova diz que o natural  $P = p_1 p_2 \dots p_{r+1}$  é primo. [Um contra exemplo é  $P = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$ , que é divisível por 59. Desafio-o, para lhes ajudar a entender melhor, que encontre outro contraexemplo, com  $P$  menor]. Na verdade, a prova somente usa o fato que, se  $P$  não for um primo *novo* [diferente de  $p_1, p_2, \dots, p_r$ ], então há um primo *novo* que divide  $P$ ).

### 7.1.1. Testando Primalidade de $n$ :

• **Primeira abordagem exata** simples- direta- ineficiente:

teste se  $n$  é divisível por cada um dos naturais 2,3,4,5,6, até  $(\sqrt{n})$  arredondado para baixo). No pior caso, o número de divisões é assintoticamente proporcional a  $\sqrt{n}$ , isto é, é  $O(\sqrt{n})$ .

• **Segunda abordagem exata**: ainda simples- direto- ineficiente: tente dividir por 2, depois por todos os ímpares 3,5,7,9,11,13,15, até  $(\sqrt{n})$  arredondado para baixo). No pior caso, o número de divisões ainda é assintoticamente proporcional a  $\sqrt{n}$ , isto é, é  $O(\sqrt{n})$ . Mas é 2 vezes mais eficiente que acima. Eis o programa:

```
prime_factorization(long x)
{
    long i; /* counter */
    long c; /* remaining product to factor */
    c = x;
    while ((c % 2) == 0) {
        printf("%ld\n", 2);
        c = c / 2;
    }
    i = 3;
    while (i <= (sqrt(c)+1)) {
        if ((c % i) == 0) {
            printf("%ld\n", i);
            c = c / i;
        }
        else
            i = i + 2;
    }
}
```



```

    }
    if (c > 1) printf("%ld\n", c);
}

```

### • Terceira abordagem exata:

Observe que todos os primos são de forma  $6k \pm 1$ , com 2 e 3 sendo as únicas exceções. Isto decorre do fato que todos os inteiros podem ser expressos como  $(6k + i)$  para algum inteiro  $k$  e para  $i = -1, 0, 1, 2, 3$ , ou 4; note que 2 divide  $(6k + 0)$ ,  $(6k + 2)$ ,  $(6k + 4)$ ; e 3 divide  $(6k + 3)$ . Portanto, um método mais eficiente é testar se  $n$  é divisível por 2, depois testar se é divisível por 3, então checar através de todos os números da forma  $6k \pm 1$ , até isto ultrapassar ( $\sqrt{n}$  arredondado para baixo). Isto é, checar para  $n = 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, \dots$ . No pior caso, o número de divisões ainda é assintoticamente proporcional a  $\sqrt{n}$ , isto é, é  $O(\sqrt{n})$ . Mas é 3 vezes mais eficiente que a 2ª abordagem, 6 vezes mais que a 1ª.

### • Outro teste exato de primalidade, ainda simples- direto- ineficiente:

Sabe-se que, com exceção dos números 2 e 3, todos os outros números primos são expressos pela fórmula  $6K \pm 1$ . Mas sabe-se que a imensa maioria dos números expresso pela fórmula  $6K \pm 1$  não é constituída de números primos [a relação é necessária, mas não suficiente]. O estudo dos não-primos da forma  $6K \pm 1$  leva à igualdade  $K = 6k_2k_3 \pm k_2 \pm k_3$ . {#} (ver 7.4.3. - Equações Diofantinas).

Então: dado um número inteiro positivo qualquer  $K$ :

- Se não ocorrer nenhum par de números inteiros *positivos*  $k_2, k_3$  {soluções de #} que satisfaça a igualdade acima, afirma-se que os números  $6K \pm 1$  são **números primos gêmeos** (números primos que diferem um do outro de apenas duas unidades). Ex: {29, 31}.  $K=5$ ; nenhum  $k_2, k_3$  positivos satisfazem {#}, portanto {29, 31} são primos gêmeos.

Se não ocorrer nenhum par  $k_2, k_3$  {soluções de #} com *sinas iguais* e ocorrer ao menos um par  $k_2, k_3$  com *sinas diferentes* que satisfaça a equação, afirma-se que  $6K+1$  é primo e  $6K-1$  não é primo.

Se não ocorrer nenhum par  $k_2, k_3$  {soluções de #} com *sinas diferentes* e ocorrer ao menos um par  $k_2, k_3$  com *sinas iguais* que satisfaça a equação, afirma-se que  $6K-1$  é primo e  $6K+1$  não é primo. Ex: {23, 25}.  $K=4$ ; onde  $k_2 = -1$ ,  $k_3 = -1$ ,  $6k_2k_3 + k_2 + k_3 = 6(-1)(-1) + (-1) + (-1) = 4$ . Portanto  $6K \pm 1 = \{23, 25\}$

### **Algoritmo [exato] AKS para Teste de Primalidade:**

Não vou exigir que você saiba mais que a existência e grande vantagem dele, mas veja em livros, artigos ou Internet o algoritmo [exato] AKS para testar primalidade, e que ele cai na **classe P (polinomial, em máquina determinística)**. É provado que, no pior caso, seu tempo de execução é assintoticamente proporcional a  $\log^{(12+\epsilon)}(n)$ , isto é, é  $O(\log^{(12+\epsilon)}(n))$ , onde  $\epsilon$  é um número pequeno. Em outras palavras, o algoritmo leva menos que uma constante vezes a 12ª potência (mais  $\epsilon$ ) do número de dígitos de  $n$ . Ainda não foi provado, mas a experiência prática sempre tem resultado em tempos de execução na ordem de **uma constante vezes a 6ª potência (mais  $\epsilon$ ) do número de dígitos de  $n$** .



### • **Teste [com altíssima probabilidade, mas não exatidão] de primalidade de Fermat** (adaptado de [http://pt.wikipedia.org/wiki/Teste\\_de\\_primalidade\\_de\\_Fermat](http://pt.wikipedia.org/wiki/Teste_de_primalidade_de_Fermat))

O Pequeno Teorema de Fermat, que originou o Teste de Primalidade de Fermat, oferece um teste simples e eficiente para ignorar números não primos. Qualquer número que falhe o teste não é primo.

#### **Pequeno Teorema de Fermat:**

**Se  $m$  é primo, então para qualquer  $a$  tal que  $\text{mdc}(a, m) = 1$ , temos:**

$$a^{m-1} \equiv 1 \pmod{m}$$

[notação explicada não muito longe, abaixo. Entenda assim: "em aritmética módulo  $m$ ,  $a^{m-1}$  é congruente com 1"]

[Atenção: Se  $m$  não é primo, ainda é possível (embora pouco provável) que o supradito se verifique.

Se  $m$  é ímpar composto, e  $a$  é um inteiro tal que  $\text{mdc}(a, m) = 1$ , e  $a$  passa no teste de primalidade de Fermat (isto é,  $a^{m-1} \equiv 1 \pmod{m}$ ), então se diz que " $m$  é **pseudoprimo** para a base  $a$ ". Isto equivale a se dizer " $a$  é um número não primo que passa o teste de Fermat".]

#### **Prova:**

Seja  $\text{mdc}(a, m) = 1$ ;

consideremos os conjuntos  $\{1, 2, 3, \dots, m-1\}$  e  $\{a, 2a, 3a, \dots, (m-1)a\}$

e percebamos que cada número em  $\{a, 2a, 3a, \dots, (m-1)a\}$  é não congruente com 0 (tudo isto mod  $m$ ) (i.é, nenhum desses novos números é múltiplo de  $m$ ).

Sejam  $i, j \in \{1, 2, 3, \dots, m-1\}$  e  $i \cdot a \equiv j \cdot a \pmod{m}$ ;

vemos que  $i \equiv j \pmod{m}$ , porque  $\text{mdc}(a, m) = 1$ ;

com isso, deduzimos que  $i = j$ , porque  $0 \leq (i-j) < m$ ;  
então, os números em  $\{a, 2a, 3a, \dots, (m-1)a\}$  são não congruentes com 0 (tudo mod  $m$ ) e também são não congruentes entre si (tudo mod  $m$ ).  
Então os números em  $\{a, 2a, 3a, \dots, (m-1)a\}$  são congruentes, em alguma ordem, com os números  $\{1, 2, 3, \dots, (m-1)\}$ , tudo isto mod  $m$ .  
Conclui-se que:  
 $(m-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (m-1) \equiv a \cdot 2a \cdot 3a \cdot 4a \cdot \dots \cdot (m-1)a$   
que implica que  $(m-1)! \equiv a^{(m-1)} \cdot (m-1)! \pmod{m}$   
Ora, já que  $\text{mdc}(m, (m-1)!) = 1$ ,  
podemos cancelar o fator  $(m-1)!$ , e obtemos:  
 $a^{m-1} \equiv 1 \pmod{m}$   
o que conclui a prova.



Infelizmente, existem números que passam o teste de Fermat para todas as bases para as quais são relativamente primos – são os chamados **números de Carmichael**, e são em número infinito (Tome conhecimento do problema <http://icpcres.ecs.baylor.edu/onlinejudge/external/100/10006.html>).



**Teste [Forte] de [Pseudo] Primalidade, de Miller-Rabin** (muito bom) (detalhes em <http://www.cin.ufpe.br/~tg/2009-2/abc.pdf>, que descreve e avalia todos os mais importantes testes de primalidade existentes em 2009. O AKS é o melhor teste exato, mas é muito custoso, por isso, na prática, todos usa mais testes probabilísticos, particularmente os de Miller-Rabin e seus aperfeiçoamentos):  
Algoritmo Miller-Rabin (versão base, inicial. Depois foi modificado):

Dado  $m$   
Escreva  $m-1 = 2^t t$ , em que  $t$  é ímpar  
Escolha aleatoriamente  $a \in [1, m[$   
Calcule  $h = a^t \pmod{m}$   
Se  $h = \pm 1$ , então  $m$  passa o teste  
Calcule  $h^i = a^{(2^i t)} \pmod{m}$  para  $i = 1, 2, \dots, 8$   
Se  $h^i = -1$  para algum  $i < 8$ , então  $m$  passa o teste  
Caso contrário  $m$  falha o teste.

O teste deve ser repetido para  $r$  bases diferentes. A probabilidade de um número composto  $m$  passar  $r$  testes é de 1 em  $4^r$ . Se  $m$  passar o teste para 100 bases diferentes, então a probabilidade de  $m$  ser um número composto é menor que  $10^{-60}$ .  
Código Python em <http://www.dzone.com/snippets/miller-rabin-primality-test>

### 7.1.2. Contando os Primos

Não somente há um infinito número de primos, como os primos são relativamente comuns:

**Teorema dos Números Primos** (Gauss, aos 15 anos (!) ):

$\Pi(n)$ , o número de primos menores que ou iguais a  $x$ , é grosseiramente aproximado por  $\frac{x}{\ln x}$ .  
<http://mathworld.wolfram.com/PrimeNumberTheorem.html> . Lembre que  $\ln x \approx 2,303 \log_{10} x$ , portanto o número de primos no intervalo  $[2, x]$  é aproximadamente  $x / (2,303 \log_{10} x) = 0,4342x / (\log_{10} x)$

### 7.1.3. Mais Algumas Poucas Coisas Sobre os Primos

- **Conjectura de Goldbach** [formulada em 1746 e até hoje não provada, apesar de ter sido verificada para números da ordem de  $4 \times 10^{14}$ .]: **Sempre se pode exprimir os números pares, maiores que 2, como a soma de dois números primos.**

- Outra conjectura (verificada, mas não provada): **os primos estão uniformemente distribuídos quanto seus últimos algarismos.** Isto é, dos infinitos primos, 1/4 termina com o algarismo 1, 1/4 com o 3, 1/4 com o 7, 1/4 com o 9

- Outra: **Há infinitos pares de números denominados primos gêmeos: números primos que diferem um do outro de apenas duas unidades**, como (3; 5), (71; 73) ou (1000000007; 1000000009)

• Outra: Há infinitos pares de primos sexy (do Latim sex, significando 6), isto é, **que diferem por 6 um do outro**: (5,11), (7,13), (11,17), (13,19), (17,23), (23,29), (31,37), (37,43), etc. O maior que já foi descoberto (em 2009) tem 11593 dígitos. Os primos são  $(p, p+6)$  e  $p = (117924851 \times 587502 \times 9001\# \times (587502 \times 9001\# + 1) + 210) \times (587502 \times 9001\# - 1)/35 + 5$ , onde 9001# é um *primorial*, isto é o produto de primos menores ou iguais a 9001, i.e.,  $9001\# = 2 \times 3 \times 5 \times \dots \times 9001$ .

• Há infinitas triplas  $\{p, p+6, p+12\}$  de primos sexy, onde  $(p-6)$  e  $(p+18)$  não são primos.

• Há infinitas quádruplas de primos sexy

• Há somente 1 quíntupla de primos sexy: 5,11,17,23,29. Em qualquer outra quintupla  $\{p, p+6, p+12, p+18, p+24, p+30\}$  (onde  $p > 5$ ), para todos os pares serem relativamente primos, um dos números tem que ser divisível por 5 (se um terminar em 1, o seguinte terminará com 7, o próximo com 3, o próximo com 9, o próximo com 5) e não será primo.

• Quando arranjamos os naturais em uma espiral (chamada de *Espiral de Ulam*) e destacamos os números primos, observamos um intrigante e não totalmente explicado padrão, com os primos se alinhando num *surpreendente padrão de segmentos de retas, em diagonal*. Veja em <http://mathworld.wolfram.com/PrimeSpiral.html> e em [http://en.wikipedia.org/wiki/Ulam\\_spiral](http://en.wikipedia.org/wiki/Ulam_spiral) e leia as conjecturas lá citadas

• Até 23.8.2008, o maior número primo encontrado é  $2^{43.112.609} - 1$ , um número com 12.978.189 dígitos, descoberto pelo projeto GIMPS (*The Great Internet Mersenne Prime Search*), que é um projeto de computação distribuída pela Internet que usa o tempo ocioso de computadores pessoais, na procura por números primos específicos, os chamados **primos de Mersenne**. Um primo de Mersenne é um número primo do tipo  $M_n = 2^n - 1$ , onde  $n$  é um natural. Atualmente, só descobrimos 45 deles: 3, 7, 31, 127, ...

• **Crivo De Eratóstenes** (que você conhece desde o ensino fundamental): **Solução Recursiva Com Memoization**

```
int sieve_memo[...];
int sieve(int n)
{ int i, j, c = 1;
  for(i = 3; i ≤ n; i+=2)
  { sieve_memo[i] = 1;
    sieve_memo[i - 1] = 0;
  }
  sieve_memo[2] = 1;
  for( i = 3; i ≤ n; i+=2)
    if(sieve_memo[i] == 1)
    { c++;
      for(j = i + i; j ≤ n; j+=i)
        sieve_memo[j] = 0;
    }
  return c;
}
```



[Em 1995] um estudante na École Polytechnique relatou que havia "quebrado" uma mensagem de desafio criptografada publicada na Web pela Netscape. A mensagem, uma transação eletrônica, tinha sido criptografada usando um algoritmo com uma variável [chave] de encriptação de 40 bits. O que o aluno fez foi particionar o espaço da variável [chave] de encriptação [ $2^{40} \approx 10^{12} = 1$  trilhão de chaves possíveis] através de um número de computadores aos quais lhe foi dado acesso, e colocá-los procurando a chave correta. Em outras palavras, ele executou um ataque de força bruta, teve sucesso, e achou a variável [chave] de encriptação usada na mensagem. Seu ataque durou cerca de 6 dias e processou cerca de 800.000 chaves por segundo [portanto, experimentou cerca de 417 bilhões de chaves possíveis]. Enquanto a maioria dos analistas não acreditava que uma variável [chave] de encriptação de 40 bits estava imune a um ataque de força bruta, o sucesso do aluno causou uma grande celeuma na imprensa. Além disso, o estudante postou seu programa em um site para que qualquer um pudesse copiar o programa e

executar o ataque. Veja os atuais desafios e prêmios em aberto, em [http://en.wikipedia.org/wiki/RSA\\_Factoring\\_Challenge](http://en.wikipedia.org/wiki/RSA_Factoring_Challenge)

Na RSA {<sup>\*</sup>} Data Security Conference, janeiro de 1997, foi anunciado que um estudante de Berkeley, usando o tempo ocioso de uma rede de 250 computadores, foi capaz de quebrar a mensagem criptografada de desafio da RSA, que usava uma chave de 40 bits, em [apenas] 3 1/2 horas. /\* RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do MIT (Massachusetts Institute of Technology), fundadores da atual empresa RSA Data Security, Inc., Ronald Rivest, Adi Shamir e Leonard Adleman, que inventaram este algoritmo — até a data (2008), a mais bem sucedida implementação de sistemas de chaves assimétricas, e fundamenta-se em teorias clássicas dos números. É considerado dos mais seguros, ... . Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em criptografia de chave pública. \*/



[Em 1997] um ataque de força bruta foi completado contra uma mensagem [desafio] na página web do DES [Data Encryption Standard]. Citamos [parte de] o comunicado de imprensa da equipe do Desafio DES (encontrado na [www.frii.com/~rtv/despr4.htm](http://www.frii.com/~rtv/despr4.htm)): LOVELAND, COLORADO (18 de junho de 1997). Dezenas de milhares de computadores, através de todo os EUA e Canadá, ligaram-se entre si através da Internet, em um sem precedentes esforço de supercomputação cooperativa para decifrar uma mensagem codificada com o Data Encryption Standard (DES), endossado pelo governo [dos EUA]. Respondendo a um desafio, incluindo um prêmio de 10.000 dólares, oferecidos pela RSA Data Security, Inc., o esforço DESCHALL obteve êxito em decodificar a mensagem secreta da RSA. De acordo com Rocke Verser, um programador contratado [por outra empresa, claro] e consultor, que desenvolveu o software especializado em seu tempo livre, "Dezenas de milhares de computadores trabalharam cooperativamente para vencer o desafio". É melhor você ver em <http://gilchrist.ca/jeff/distrib-des.html>

EXEMPLO 1: Em termos aproximados, quantos primos há com o máximo de 500 dígitos? E com o máximo de 501 dígitos? E com o máximo de 5000 dígitos?

RESPOSTA: De acordo com Gauss, o número de primos no intervalo  $[2, x]$  é aproximadamente  $0,4342 \times x / (\log_{10} x)$ .

Para até 500 dígitos, temos  $0,4342 \times 10^{500} / 500 = 0,8684 \times 10^{497}$ ; (para comparação, o número de prótons no universo observável é na ordem de  $10^{80}$ )

Para até 501 dígitos, temos  $0,4342 \times 10^{501} / 501 = 0,8667 \times 10^{498}$ ;

Para até 5000 dígitos, temos  $0,4342 \times 10^{5000} / 5000 = 0,8684 \times 10^{4997}$ ;

EXEMPLO 2: Você quer dividir o intervalo entre 2 e  $10^{400}$  em 100 segmentos que tenham aproximadamente o mesmo número de primos. Como você fará?

RESPOSTA: O número de primos no intervalo total é de cerca de  $0,4342 \times 10^{400} / (\log_{10} 10^{400}) = 0,4342 \times 10^{400} / 400 = 0,1086 \times 10^{398}$ . Portanto, cada um dos 100 intervalos deve ter cerca de  $0,1086 \times 10^{396}$  primos.

O 1º intervalo deve ir de 2 até  $n_1$ , onde  $0,4342 n_1 / (\log_{10} n_1) = 1 \times 0,1086 \times 10^{396}$ . Resolva  $n_1$ , mesmo que de forma aproximada.

O 2º intervalo deve ir de  $n_1$  até  $n_2$ , onde  $0,4342 n_2 / (\log_{10} n_2) = 2 \times 0,1086 \times 10^{396}$ . Resolva  $n_2$ , mesmo que de forma aproximada.

O 3º intervalo deve ir de  $n_2$  até  $n_3$ , onde  $0,4342 n_3 / (\log_{10} n_3) = 3 \times 0,1086 \times 10^{396}$ . Resolva  $n_3$ , mesmo que de forma aproximada.

...

EXEMPLO 3: Você quer encontrar um primo que pode chegar a ter até 400 dígitos, e quer dividir (de uma vez por todas, sem refazer a divisão) o trabalho entre  $10^4$  computadores. Suponha que, uma vez que o computador sugira um primo para ser testado, o teste é dispendioso. Como você fará? Dará a cada computador um intervalo de mesmo comprimento de inteiros, para ele analisar? (isto é, dirá ao computador 1 para procurar entre 2 e  $10^{400-4}$ , ao computador 2 para começar daí e ir até  $2 \times 10^{400-4}$ , ..., ao computador 10.000 para ir de  $(10.000-1) \times 10^{396}$  até  $10^{400}$ )? Por que sim? Por que não? Ou você teria uma melhor divisão de trabalho entre os computadores (supondo que a divisão só pode ser feita uma vez)? Qual?

RESPOSTA: Eu não usaria o esquema proposto porque a "densidade" dos primos vai diminuindo, de modo que os últimos computadores vão achar muito menos primos para testar (supondo que o teste é dispendioso) do que os primeiros que acharão muitos mais primos em seus intervalos).

Lembrando que o número de primos menores que ou iguais a  $x$ , é grosseiramente aproximado por  $(x / \ln x)$ , eu usaria o esquema de divisão das tarefas proposto no exemplo 2.

Exercícios propostos, do livro do Prof. Manoel Lemos em

[http://www.impa.br/opencms/pt/biblioteca/pm/PM\\_04.pdf](http://www.impa.br/opencms/pt/biblioteca/pm/PM_04.pdf) . Escolha e faça pelo menos 1/3 deles, espaçados, de diferentes tipos.

PROBLEMA 1. Mostre que todo número natural composto  $n$  possui um divisor menor ou igual a  $\sqrt{n}$ .

PROBLEMA 2. Fatore os seguintes números como produto de primos:  $5^{16} - 1$ ;  $7^{12} - 1$ ; e  $2^{15} + 1$

PROBLEMA 3. Um número primo da forma  $2^n - 1$ , para  $n \in \mathbf{N}$ , é dito de Mersenne. Quando isto ocorre, mostre que  $n$  tem de ser primo.

PROBLEMA 4. A recíproca do exercício anterior vale? Isto é, se  $n$  é primo, então  $2^n - 1$  tem que ser primo?

PROBLEMA 5. Um número primo da forma  $2^n + 1$ , para  $n \in \mathbf{N}$ , é dito de Fermat. Quando isto ocorre, mostre que  $n$  tem de ser uma potência de 2.

PROBLEMA 6. Encontre o expoente da maior potência de 2 que divide  $100!$  (100 fatorial).

PROBLEMA 7. Seja  $p$  um número primo e  $n$  um inteiro positivo. Mostre que o expoente da maior potência de  $p$  que divide  $n!$  é  $\sum_{i=1}^n \frac{n}{p^i}$

PROBLEMA 8. Qual dentre os números 501, 521, 541, 561 e 581 é de Carmichael?

PROBLEMA 9. Mostre que todo número de Carmichael é divisível por pelo menos três primos distintos.

PROBLEMA 10. Encontre todos os números de Carmichael da forma  $3pq$ , onde  $p$  e  $q$  são números primos distintos.

PROBLEMA 11. Para um natural  $k$ , suponha que  $6k+1$ ,  $12k+1$  e  $18k+1$  são todos primos. Mostre que  $n_k = (6k+1)(12k+1)(18k+1)$  é de Carmichael.

PROBLEMA 12. Encontre todos os números de Carmichael da forma  $n_k$ , para  $k \leq 10$ .

## 7.2. DIVISIBILIDADE

$b$  **divide**  $a$  (denotado  $b|a$ ) se  $bk = a$ , para algum inteiro  $k$ .  $b$  é chamado de um **divisor** de  $a$ ,  $a$  é chamado de um **múltiplo** de  $b$ .

### Ache todos os divisores de um dado inteiro $x$ :

A partir do Teorema Fundamental da Aritmética, sabemos que  $x$  é unicamente representado pelo produto de seus fatores primos. (use <http://primes.utm.edu/lists/small/10000.txt>.) Cada divisor é o produto de algum subconjunto desses fatores primos. Tais subconjuntos podem ser construídos usando técnicas de backtracking, assim, por exemplo:

$$165 = 3 \times 5 \times 11. \text{ Seus divisores são } 1, 3, 5, 11, 15, 33, 55, 165$$

mas devemos ter cuidado com fatores primos duplicados. Por exemplo, a fatoração de 12 em primos tem três termos (2, 2, e 3), e poderia parecer que 12 tem  $2^3 = 8$  divisores (correspondente ao conjunto potência, o conjunto vazio correspondente ao divisor 1), mas 12 tem apenas 6 divisores (1, 2, 2, 3, 4, 6, 12) (backtracking mal feito contaria  $2 \times 2$  de duas maneiras, e contaria o resultado de  $2 \times 3$  como diferente do resultado de  $3 \times 2$ , resultando em  $\{1, 2, 2, 3, 2, 2, 3, 4, 6, 6, 12\}$ )

### 7.2.1. Máximo Divisor Comum (mdc) (Greatest Common Divisor. gcd)

O maior divisor comum de dois ou mais números é chamado de **máximo divisor comum (mdc)** desses números.

Propriedades:

- Cada divisor comum de  $a$  e  $b$  é um divisor de  $\text{mdc}(a, b)$ .
- $\text{mdc}(a, b)$ , onde  $a$  e  $b$  não são ambos zero, pode ser definido, alternativamente e equivalentemente, como o menor número inteiro positivo  $d$  que pode ser escrito da forma  $d = ap + bq$ , onde  $p$  e  $q$  são números inteiros. Esta expressão é denominada **identidade de Bézout**. Números  $p$  e  $q$  como este pode ser calculados com o algoritmo estendido de Euclides.

- $\text{mdc}(a,0) = |a|$ , para  $a \neq 0$ , uma vez que qualquer número é um divisor de 0, e o maior divisor de  $a$  é  $|a|$ . Isto é usado geralmente como o caso base no algoritmo de Euclides.
- $\text{mdc}(x,x) = x$  /\* idempotência
- Se  $a$  divide o produto  $b.c$ , e  $\text{mdc}(a,b) = d$ , então  $a/d$  divide  $c$ .
- Se  $m$  é um inteiro não negativo, então  $\text{mdc}(m.a, m.b) = m.\text{mdc}(a,b)$ .
- Se  $m$  é um número inteiro qualquer, então  $\text{mdc}(a + m.b, b) = \text{mdc}(a,b)$ .
- Se  $m$  é um não nulo divisor comum de  $a$  e  $b$ , então,  $\text{mdc}(a/m, b/m) = \text{mdc}(a,b)/m$ .
- O  $\text{mdc}$  é uma **função multiplicativa** no seguinte sentido: se  $a_1$  e  $a_2$  são relativamente primos, então  $\text{mdc}(a_1.a_2,b) = \text{mdc}(a_1,b).\text{mdc}(a_2,b)$ .
- O  $\text{mdc}$  é uma **função comutativa**:  $\text{mdc}(a,b) = \text{mdc}(b,a)$ .
- O  $\text{mdc}$  é uma **função associativa**:  $\text{mdc}(a, \text{mdc}(b,c)) = \text{mdc}(\text{mdc}(a,b), c)$ .
- O  $\text{mdc}$  de três números pode ser calculado como  $\text{mdc}(a, b, c) = \text{mdc}(\text{mdc}(a,b),c)$ , ou, de algum modo diferente, aplicando comutatividade e associatividade. Isso pode ser estendido a qualquer número de números.
- $\text{mdc}(a, b)$ , está estreitamente relacionada com o mínimo múltiplo comum  $\text{mmc}(a, b)$ : temos  

$$\text{mdc}(a,b).\text{mmc}(a, b) = a.b.$$

Esta fórmula é muitas vezes usada para computar mínimo múltiplos comuns: primeiro se calcula a  $\text{mdc}$  com o algoritmo de Euclides, e então se divide o produto dos números indicados por seu  $\text{mdc}$ .
- As seguintes versões da **distributividade** são verdadeiras:  

$$\text{mdc}(a, \text{mmc}(b,c)) = \text{mmc}(\text{mdc}(a,b), \text{mdc}(a,c))$$

$$\text{mmc}(a,\text{mdc}(b,c)) = \text{mdc}(\text{mmc}(a,b), \text{mmc}(a,c)).$$
- É útil se definir  $\text{mdc}(0, 0) = 0$  e  $\text{mmc}(0,0) = 0$ , porque então os números naturais tornam-se um reticulado distributivo completo com  $\text{mdc}$  como operação supremo (também chamada de join, mesmo símbolo de "or") e  $\text{mmc}$  como operação ínfimo (também chamada de "meet", mesmo símbolo de "and").

**Primeiro método, simples- direto- ineficiente, de calcular mdc de dois naturais:**

Suponhamos que os números são  $a = 126$  e  $b = 420$ ;

Ache todos os divisores do menor dos números ( $a = 126$ . Fatorando em primos

[<http://primes.utm.edu/lists/small/10000.txt>],  $a = 2 \times 3 \times 3 \times 7$ ; achando os produtos das combinações distintas deles, os divisores de  $a$  são, ordenados crescentemente  $\{1,2,3,6,7,9,14,18,21,42\}$ ;

Depois, em ordem decrescente, teste cada um deles até achar o maior deles que divida o outro número. (tente 42 e obterá sucesso.)

Ou, somente muito pouco diferente:

Suponhamos que os números são  $a = 126$  e  $b = 420$ ;

Decomponha cada um em seus fatores primos (use <http://primes.utm.edu/lists/small/10000.txt>):  $126 = 2^1 \times 3^2 \times 5^0 \times 7^1$ ;  $420 = 2^2 \times 3^1 \times 5^1 \times 7^1$

O resultado será o produto de cada fator que aparece *em comum* na fatoração de  $a$  e de  $b$ , tomado com seu *menor* expoente  $2^1 \times 3^1 \times 5^0 \times 7^1$   
 $= 42$

Outro exemplo (vou realçar os quocientes quando se aplicarem a todos os números):

mdc(70,90,120)

70	90	120	2
35	45	60	2
35	45	30	2
35	45	15	3
35	15	5	3
35	5	5	5
7	1	1	7
1	1	1	

Ao final, multiplicamos somente os quocientes realçados

**Algoritmo de Euclides** (1º algoritmo interessante em toda a História, que “quebrou barreiras”, muito mais eficiente  $[O(\log n)]$  que todos os rivais) (é o avô de todos os algoritmos: tem mais de 2300 anos e não existe melhor):

Baseado em 2 propriedades (prove-as em casa?):

Se  $b|a$ , então  $\text{mdc}(a,b) = b$ .

Se  $a = bt + r$  para inteiros  $t, r$ , então  $\text{mdc}(a,b) = \text{mdc}(b, r)$ .

Aprendemos no Ensino Fundamental:

**mdc(maior, menor) := if menor = 0 then maior else mdc(menor, resto da divisão inteira maior/menor)**

Quocientes ArguEsq divinteira ArguAbaixo (primeira célula vazia)

Argumentos (inicialmente {maior, menor} )

Multiplicação ArguDir×QuocDir

Resto = ArguAcima - MultiplicaçãoAcima (transferir para ser ArguDir)

-	1	9	-
420	378	<b>42</b>	...0
378	378	...	...
42	0	...	...

Outro exemplo:

Quocientes ArguEsq divinteira ArguAbaixo (primeira célula vazia)

Argumentos (inicialmente {maior, menor} )

Multiplicação ArguDir×QuocDir

Resto = ArguAcima - MultiplicaçãoAcima (transferir para ser

ArguDir)

-	5	4	1	1	2	
120	23	5	3	2	<b>1</b>	0
115	20	3	2	2		
5	3	2	1	0		

### Algoritmo de Euclides iterativo:

**AlgoritmoDeEuclides(a: inteiro; b: inteiro): inteiro**

**variáveis**

divisor: inteiro

dividendo: inteiro

c: inteiro

**início**

dividendo = a

divisor = b

enquanto resto(dividendo/divisor) ≠ 0

**início**

c = resto(dividendo/divisor)

dividendo = divisor

divisor = c

**fim-enquanto**

AlgoritmoDeEuclides = divisor

**fim-função**

### Algoritmo de Euclides recursivo:

**AlgoritmoDeEuclides(a: inteiro; b: inteiro): inteiro**

**início**

se b = 0 então

AlgoritmoDeEuclides = a

senão

AlgoritmoDeEuclides = AlgoritmoDeEuclides(b, resto(a,b))

**fim-se**

**fim-função**

**Implementação de Euclides em C** (cuidado para prever o caso  $p=q=0$ ):

```

/* Find the gcd(p,q) and x,y such that p*x + q*y = gcd(p,q) */
long gcd(long p, long q, long *x, long *y)
{
    long x1,y1; /* previous coefficients */
    long g; /* value of gcd(p,q) */
    if (q > p) return(gcd(q,p,y,x));
    if (q == 0) {
        *x = 1;
        *y = 0;
        return(p);
    }
    g = gcd(q, p%q, &x1, &y1);
    *x = y1;
    *y = (x1 - floor(p/q)*y1);
    return(g);
}

```

### Algoritmo de Euclides estendido:

Além de encontrar o máximo divisor comum de inteiros  $a, b$ , como o algoritmo de Euclides faz, também encontra números inteiros  $x, y$  (um dos quais é tipicamente negativo) que satisfazem a **identidade de Bézout**

$$ax + by = \text{mdc}(a,b)$$

Por exemplo:

$120 \times (-9) + 23 \times (47) = \text{mdc}(120,23)$ . Aqui,  $a = 120$ ,  $b = 23$ ,  $x = -9$ ,  $y = 47$ . Realmente,  $-1080 + 1081 = 1 = \text{mdc}(120,23) = \text{mdc}(23,5) = \text{mdc}(4,3) = \text{mdc}(3,1) = 1$

O algoritmo estendido de Euclides é particularmente útil quando  $a$  e  $b$  são **relativamente primos** (também chamados de **coprímos** e ditos serem **primos entre si**),

[dois números  $a, b$  são **coprímos** se o único fator comum entre eles é 1.

10 e 21 são coprímos, porque  $10 = 5 \times 2 \times 1$  e  $21 = 7 \times 3 \times 1$ , e esses números só têm 1 como fator em comum]

uma vez que  $x$  é o inverso multiplicativo de  $a \bmod b$ , e  $y$  é o inverso multiplicativo de  $b \bmod a$ .

[ $x$  é o inverso multiplicativo módulo  $m$  de um inteiro  $a$  {e pode ser escrito  $a^{-1} \bmod m$ } se  $(ax \equiv 1) \bmod m$ . /\* definição de " $\equiv$ " em (7.4) \*/

Por exemplo, se  $m = 3$ , então 2 é o inverso multiplicativo de 23, porque  $(23 \times 2) \bmod 3 = ((23 \bmod 3) \times (2 \bmod 3)) \bmod 3 = (2 \times 2) \bmod 3 = 4 \bmod 3 = 1$ ]

[No exemplo lá em cima,  $-9$  é o inverso multiplicativo de  $120 \bmod 23$ , pois  $(23 - 9) = 14$  e  $(14 \times 120) \bmod 23 = \dots = 1$

$(47 \text{ é o inverso multiplicativo de } 23 \bmod 120, \text{ pois } (47 \times 23) \bmod 120 = \dots = 1]$

$$\text{mdc}(120,23) = 120 \times (-9) + 49 \times (23) = -1080 + 1081 = 1$$

### Euclides Estendido, Algoritmo Recursivo:

```

function extended_gcd(a, b) // retorna um par [(x,y), de modo que ax + by = mdc(a,b)]
    if b = 0
        return (1, 0)
    else
        q := a div inteira b
        r := a - b*q
        (s, t) := extended_gcd(b, r)
        return (t, s - q*t)

```

### Euclides Estendido, Código em C:

```

#include <stdio.h>
#include <stdlib.h>

```

*/\* Aritmética modular é também considerada como o "algoritmo do relógio".*

*Ao extrair o modulo 12, como resposta possível pode-se ter números de 0 a 11.*

*Nunca negativo, pois a ideia é de um relógio com 12 posições, sendo a primeira o*



zero e a última o 11.

Porém o operador de módulo do C (operador %) computa apenas o resto da divisão e gera números negativos. Em C:

```
-2 mod 12 = -2 (não está entre 0 e 11)
2 mod -12 = 2 (não está entre -11 e 0)
```

O C dizer que  $-2 \bmod 12$  é  $-2$  significa dizer que ele está a  $-2$  de distância do final do relógio, ou seja, está em 10 (o início e também o final do relógio é o zero).

Dizer que  $2 \bmod -12$  significa um relógio ao contrário (0, -1, -2, -3, .. -11, andando no sentido anti-horário) e que o valor 2 está a 2 posições de distância do 0, ou seja, está em -10.

Nesta aritmética modular o resultado da operação *PRECISA SER* do mesmo sinal do divisor.

Observou-se que o operador de módulo do Python (%) não tem este comportamento, calculando o módulo não negativo. A biblioteca *bn.h* do *openssl* possui ambos, tanto a função *BN\_mod* que simplesmente retorna o resto da divisão (comportamento igual ao % do C) como a função *BN\_nnmod* que calcula o módulo não negativo.

Nesta versão em C resolveu-se fazer uma pequena correção na resposta dada pelo operador de módulo, pois o algoritmo de Euclides precisa do módulo positivo.

```
*/
long mod(long a, long b)
{
    long r = a % b;

    /* Uma correção é necessária se r e b não forem do mesmo sinal */

    /* se r for negativo e b positivo, precisa corrigir */
    if ((r < 0) && (b > 0))
        return (b + r);

    /* Se r for positivo e b negativo, nova correção */
    if ((r > 0) && (b < 0))
        return (b + r);

    return (r);
}

long euclides_ext(long a, long b, long c)
{
    long r;
    r = mod(b, a);
    if (r == 0) {
        return (mod((c / a), (b / a))); // retorna (c/a) % (b/a)
    }
    return ((euclides_ext(r, a, -c) * b + c) / (mod(a, b)));
}

int main(int argc, char *argv[])
{
    long p, q, e, qq, n, d;

    /* O objetivo desta implementação do algoritmo de Euclides estendido é o
    cálculo do valor do D da chave privada correspondente a Ke=(n,e)
    http://www.vivaolinux.com.br/artigo/Criptografia-assimetrica-com-o-RSA/ para isto são necessários fornecer
    o p, o q e o valor de e */
    if (argc != 4) {
        fprintf(stderr, "ERRO. faltou passar valor de p, q, e\n");
        fprintf(stderr, "Forma de uso:\n");
        fprintf(stderr, "\t%s p q e\n", argv[0]);
        return (1);
    }
}
```

```

/* pegando os valores de p, q e n fornecidos como argumentos do main */
p = atol(argv[1]);
q = atol(argv[2]);
e = atol(argv[3]);

/* calculando o n */
n = p * q;

/* calculando o quociente de Euler, chamado aqui de qq */
qq = (p - 1) * (q - 1);

/* chamando a função que calcula o d. Ela retorna um número que case na
expressão: (d*e) mod qq = X para que M^(d*e) mod N = M
Tem-se o e e o qq. Para o RSA o X deve ser 1, pois d*e mod qq = 1
*/
d = euclides_ext(e, qq, 1);

printf("\nVALORES CALCULADOS:\n");
printf("N = %10li\nE = %10li\nqq = %10li\nD = %10li\n", n, e, qq, d);
printf("\n*** Verifique com ***\n");
printf("\techo \"(%li * %li) %% %li\"|bc\n\n", d, e, qq);
printf("\t(deve resultar em 1)\n\n\n");

```



Veja, em [http://pt.wikibooks.org/wiki/Teoria\\_de\\_n%C3%BAmeros/Divisibilidade](http://pt.wikibooks.org/wiki/Teoria_de_n%C3%BAmeros/Divisibilidade), úteis regras de divisibilidade por 2,3,4,5,6,7,8,9,10,11. Porque funcionam pode ser visto em <http://webpace.ship.edu/msrenault/divisibility/StupidDivisibilityTricks.pdf> ou suas referências.

### 7.2.2. Mínimo Múltiplo Comum (mmc)

(Least Common Multiple, lcm)

O **mínimo múltiplo comum** (mmc) de dois inteiros  $a$ ,  $b$  é o menor inteiro positivo que é múltiplo simultaneamente de  $a$  e de  $b$ . Se não existir tal inteiro positivo, por exemplo, se  $a = 0$  ou  $b = 0$ , então definimos que  $\text{mmc}(a, b) = 0$ .

É evidente que  $\text{mmc}(x, y) \geq \max(x, y)$ . Do mesmo modo, uma vez que  $x \cdot y$  é um múltiplo de ambos  $x$  e  $y$ , então  $\text{mmc}(x, y) \leq x \cdot y$ . A única maneira pela qual pode haver um múltiplo comum menor que  $xy$  é se há algum fator não trivial (i.e., diferente de 0 e de 1) partilhado entre  $x$  e  $y$ . Esta observação, juntamente com o algoritmo de Euclides, oferece uma maneira eficiente para computar mínimo múltiplo comum: se nem  $a$  nem  $b$  são zero, o mínimo múltiplo comum pode ser computado usando o Algoritmo de Euclides (para mdc):

**se nem  $a=0$  nem  $b=0$ , então**  $\text{mmc}(a,b) = (a \cdot b) / \text{mdc}(a,b)$   
**senão,**  $\text{mmc}(a,b) = 0$

Sempre use a regra “cancelar antes de multiplicar”:  $\text{mmc}(24000, 36000)$ , simplificado dividindo por 12000, dá  $12000 \times \text{mmc}(2,3) = 12000 \times 6 = 72000$ .

Considerado como operação binária, o mmc de dois inteiros positivos tem as propriedades

comutativa	$\text{mmc}(a,b) = \text{mmc}(b,a)$
e associativa	$\text{mmc}(a,\text{mmc}(b,c)) = \text{mmc}(\text{mmc}(a,b),c)$
é idempotente	$\text{mmc}(a,a) = a$
1 é o elemento neutro	$\text{mmc}(a,1) = a$
e a multiplicação é distributiva com o mmc:	$a \times \text{mmc}(b, c) = \text{mmc}(ab, ac)$

Mínimo múltiplo comum surge quando queremos calcular a periodicidade simultânea de dois distintos eventos periódicos. Quando é o próximo ano (após 2000) em que a eleição presidencial (que acontece a cada 4 anos) vai coincidir com o censo (que acontece a cada 10 anos)? Os eventos coincidem cada vinte anos, porque  $\text{mmc}(4,10) = 20$ .

Aprendemos no Ensino Fundamental:

Suponhamos que os números são  $a = 126$  e  $b = 420$ ;

Decomponha cada um em seus fatores primos (use <http://primes.utm.edu/lists/small/10000.txt>):  $126 = 2^1 \times 3^2 \times 5^0 \times 7^1$ ;  $420 = 2^2 \times 3^1 \times 5^1 \times 7^1$

O resultado será o produto de cada fator (não precisa ser *em comum*) tomado com seu *maior* expoente  $2^2 \times 3^2 \times 5^1 \times 7^1 = 1260 = 42$

Outro exemplo:

$\text{mmc}(70, 90, 120)$

70	90	120	2
35	45	60	2
35	45	30	2
35	45	15	3
35	15	5	3
35	5	5	5
7	1	1	7
1	1	1	

O mmc é o produto de todos os fatores:  $\text{mmc}(70, 90, 120) = 2^3 \times 3^2 \times 5 \times 7 = 2520$

EXEMPLO 1 (mdc): Etapa por etapa (usando a fórmula recursiva ou a construindo a tabela) mostre qual é o máximo divisor comum (mdc) de 11025 e 3872. Que mais pode você dizer sobre esses números?

RESPOSTA (vamos resolver de vários modos):

Como aprendemos mais ou menos aos 10 anos de idade, tudo à mão, sem calculadora:

quociente			2	1	5	1	1	4	2	1	9	2
números	<b>11025</b>	<b>3872</b>	3281	591	326	265	61	21	19	2	<b>1</b>	
multiplicações	-7744	-3281	-2955	-326	-265	244	42	-19	-18	2		
restos	3281	591	326	265	61	21	19	2	1	0		

Ou, depois que começamos a usar calculadora que tinha a função módulo:

Números	11025	3872	3281	591	326	265	61	21	19	2	<b>1</b>
NorOeste mod Norte		3281	591	326	265	61	21	19	2	1	0

(por exemplo, na segunda célula da linha de baixo:  $11025 \bmod 3872 = 3281$ )

Doutro modo, usando a fórmula recursiva:

$\text{mdc}(\text{Maior}, \text{Menor})$	$= \text{mdc}(\text{Menor}, (\text{Maior} \% \text{Menor}))$
$\text{mdc}(11025, 3872)$	$= \text{mdc}(3872, (11025 \% 3872)) =$
$\text{mdc}(3872, 3281)$	$= \text{mdc}(3281, (3872 \% 3281)) =$
$\text{mdc}(3281, 591)$	$= \text{mdc}(591, (3281 \% 591)) =$
$\text{mdc}(591, 326)$	$= \text{mdc}(326, (591 \% 326)) =$
$\text{mdc}(326, 265)$	$= \text{mdc}(265, (326 \% 265)) =$
$\text{mdc}(265, 61)$	$= \text{mdc}(61, (265 \% 61)) =$
$\text{mdc}(61, 21)$	$= \text{mdc}(21, (61 \% 21)) =$
$\text{mdc}(21, 19)$	$= \text{mdc}(19, (21 \% 19)) =$
$\text{mdc}(19, 2)$	$= \text{mdc}(2, (19 \% 2)) =$
$\text{mdc}(2, 1)$	$= \text{mdc}(1, (2 \% 1)) =$
$\text{mdc}(1, 0)$	$= 1$

Doutro modo, fatorando os números em fatores primos, depois tomando em menor expoente os fatores primos comuns aos dois números:

$$11025 = 3^2 \cdot 5^2 \cdot 7^2$$

$$3872 = 2^5 \cdot 11^2$$

$$\text{mdc}(11025, 3872) = 1$$

(note que, para enormes números cujas fatorações podem exigir tentativas de divisão por grande número de primos, o algoritmo de Euclides é o mais eficiente de todos os que vimos)

## 7.3. ARITMÉTICA MODULAR

- Algumas vezes não estamos interessados no resultado completo de operações aritméticas sobre números “quilométricos”, mas somente nela módulo alguma coisa.

EXEMPLO 0: hoje é domingo. Que dia da semana será daqui a 1 milhão de dias? Bem,  $1.000.000 \bmod 7 = 1$ , portanto cairá num domingo + 1, ou seja, numa segunda-feira. Quanto é ((número de 10 trilhões de dígitos) elevado a (número de 3000 dígitos)) módulo (número primo de 400 dígitos)?

### Propriedades da Aritmética Modular:

$$(x + y) \bmod n = ((x \bmod n) + (y \bmod n)) \bmod n$$

EXEMPLO:  $(90012 + 80053) \bmod 5 = ((90012 \bmod 5) + (80053 \bmod 5)) \bmod 5$

/\* note que para calcularmos  $n \bmod 5$  basta nos ocuparmos do último dígito de  $n$  \*/

$$= (2 + 3) \bmod 5 = 5 \bmod 5 = 0$$

$$(x - y) \bmod n = ((x \bmod n) - (y \bmod n)) \bmod n$$

EXEMPLO:  $(90012 - 80053) \bmod 100 = ((90012 \bmod 100) - (80053 \bmod 100)) \bmod 100$

$$= (12 - 53) \bmod 100 = -41 \bmod 100 = 59 \bmod 100 = 59$$

$$(xy) \bmod n = ((x \bmod n)(y \bmod n)) \bmod n$$

EXEMPLO:  $((90012 \times 80053)) \bmod 100 = ((90012 \bmod 100) \times (80053 \bmod 100)) \bmod 100$

$$= (12 \times 53) \bmod 100 = 636 \bmod 100 = 36$$

[para divisão, ver abaixo, em “Congruências”]

### Aplicações da Aritmética Modular:

*1ª Aplicação) Achar o último dígito* — Qual é o último dígito de (longa expressão aritmética [por enquanto sem divisão], com grandes inteiros)?

*2ª Aplicação) Cálculos a Respeito de Calendários*

*3ª Aplicação) Exponenciação modular:* Pela definição de potência, podemos calcular  $a^n$  assim:

```
function exposeq(a,n)
  r := a
  for i := 1 to n-1 do r := a*r
  return r
```

Mas isto é muito ruim pois, no pior caso, o número de multiplicações é assintoticamente proporcional a  $n$ , isto é, é  $O(n)$ .

Uma conhecida técnica geral para solução de problemas é a “Divida e Conquiste”:

Se o tamanho do problema é suficientemente pequeno, então resolva-o diretamente senão

divida-o em 2 ou mais subproblemas menores de tamanhos os mais iguais possíveis;  
resolva-os;  
retorne a apropriada junção dessas soluções dos subproblemas

Usando a técnica de “Divida e Conquiste”, a exponenciação modular fica bem mais eficiente:

```
function expoDC(a,n) // recursivo
  if n = 1 then return a
  if par(n) then return (expoDC(a, n/2))^2
  return a * expoDC(a, n-1)
```

OU

```
function expoiter(a,n) // tempo semelhante expoDC
  i := n; r := 1; x := a
  while i > 0 do
    if i ímpar(i) then r := r*x
    x := x^2
    i := i÷2 {divisão inteira}
  return r
```

Melhorou muito, pois o número de multiplicações caiu para  $O(\log n)$

Mas, em MUITAS aplicações, a base  $a$  tem milhões de dígitos e temos que usar os lentos módulos de aritmética de precisão “infinita” embutidos da biblioteca da linguagem (BigInt), e a potência  $n$  tem milhares de dígitos, levaria séculos para fazer os cálculos; mas só precisamos do resultado módulo um número de algumas centenas ou milhares de dígitos, e tudo pode ser feito extraordinariamente mais rápido (em microssegundos?), usando aritmética modular.

## 7.3.1. – Problema 374 do ACM Programming Contest (BigMod)

(No exame, no máximo, no máximo, poderá haver alguma pergunta conceitual do tipo “que significa... qual a vantagem... qual a diferença... como funciona... qual a



EXEMPLO 2: Qual é o último dígito de 1234567890123456789 elevado a 1025?

RESPOSTA: A palavra "dígito" significa que a aritmética é a da base 10. Para sabermos o último dígito, só precisamos operar na aritmética de módulo 10, e a fórmula é  $(a^b) \bmod c = ((a \bmod c)^b) \bmod c$ . Aqui,  $a = 1234567890123456789$ ,  $b = 1025$ ;  $c = 10$ . Temos  $a \bmod c = 9$ . Começamos a operar com este valor, e sempre aplicamos mod 10 a cada multiplicação. Usando divida e conquiste, temos:

$$a^2 \bmod 10 = ((a \bmod 10)(a \bmod 10)) \bmod 10 = 81 \bmod 10 = 1$$

$$a^4 \bmod 10 = ((a^2 \bmod 10)(a^2 \bmod 10)) \bmod 10 = 1 \bmod 10 = 1$$

$$a^8 \bmod 10 = ((a^4 \bmod 10)(a^4 \bmod 10)) \bmod 10 = 1 \bmod 10 = 1$$

$$a^{16} \bmod 10 = ((a^8 \bmod 10)(a^8 \bmod 10)) \bmod 10 = 1 \bmod 10 = 1$$

...

$$a^{1024} \bmod 10 = ((a^{512} \bmod 10)(a^{512} \bmod 10)) \bmod 10 = 1 \bmod 10 = 1$$

$$a^{1025} \bmod 10 = ((a^1 \bmod 10)(a^{1024} \bmod 10)) \bmod 10 = (9 \times 1) \bmod 10 = \underline{9}$$

PROBLEMA 1: Compute  $2^{70} \bmod 1001$  usando exponenciação modular. Mostre todas as etapas.

## 7.4. CONGRUÊNCIAS

[além dos livros texto, às vezes inspiramo-nos no bom sumário do livro *Programming Challenges* (Skiena, Revilla) <http://www.inf.ufrgs.br/~comba/inf1056-files/class01.pdf>]

• Sejam dois inteiros  $b, c$ , e seja um natural  $m$  (chamado de modulus). **Se  $b \bmod m = c \bmod m$**  (ou, equivalentemente, se  $b - c$  é divisível por  $m$ ), então escreve-se  **$b \equiv c \pmod{m}$** , que é lido " **$b, c$  são congruentes módulo  $m$** ". (Às vezes o modulus  $m$  é entendido pelo contexto e pode ser omitido, ficando apenas implícito, de modo que se escreve apenas  $b \equiv c$ , tendo-se o cuidado de não se confundir  $\equiv$  com o sinal de equivalência.)

• Congruências são ["*apenas*"] uma notação alternativa para a aritmética modular, mas, mesmo assim, a notação é importante, pois nos faz pensar sobre o *conjunto* de números inteiros  $b$ 's com um mesmo resto,  $r$ , quando divididos por  $m$ , e nos dá equações para representar o conjunto.

• Podemos ver  $b \equiv c \pmod{m}$  como a classe de equivalência (o *conjunto*) onde qualquer elemento arbitrariamente escolhido,  $x$ , satisfaz  $x \bmod m = b \bmod m$  (também igual a  $c \bmod m$ ), e a diferença entre dois quaisquer elementos  $x, y$  do conjunto é um múltiplo de  $m$ .

EXEMPLO: Que inteiros  $x$  satisfazem a congruência  $x \equiv 3 \pmod{9}$ ? RESPOSTA:  $\{\dots, -33, -24, -15, -6, 3, 12, 21, 30, 39, 48, \dots\} = 9k + 3$ , em que  $k$  é um número inteiro qualquer.

EXEMPLO Que inteiros  $x$  satisfazem  $(2x \equiv 3 \pmod{9}) \text{ e } (2x \equiv 3 \pmod{4})$ ? Resposta:  $\{6, 15, 24, 33, 42, \dots\} \cap \{\} = \{\}$

### 7.4.1. Operações Sobre Congruências

• *Adição e Subtração* —

Suponha que  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ . Então,  $(a + c) \equiv (b + d) \pmod{n}$ . Também,  $(a - c) \equiv (b - d) \pmod{n}$

Por exemplo, suponha que eu sei que  $4x \equiv 7 \pmod{9}$  e  $3x \equiv 3 \pmod{9}$ . Então,  $(4x - 3x) \equiv (7 - 3) \pmod{9}$ . Portanto,  $x \equiv 4 \pmod{9}$

• *Multiplicação* —

É evidente que  $a \equiv b \pmod{n}$  implica que  $(a \cdot d) \equiv (b \cdot d) \pmod{n}$ , adicionando a congruência reduzida para si mesma,  $d$  vezes. Na verdade, a multiplicação geral também é válida, ou seja,  **$(a \equiv b \pmod{n})$  e  $(c \equiv d \pmod{n})$  implicam  $(a \cdot c) \equiv (b \cdot d) \pmod{n}$** .

• *Divisão* —

No entanto, não podemos impensadamente cancelar fatores comuns de congruências. Note-se que  $(6 \times 2) \equiv (6 \times 1) \pmod{3}$ , mas claramente é falso que  $2 \equiv 1 \pmod{3}$ .

Para ver o que o problema é, note que podemos redefinir divisão como multiplicação por uma inversa, então  $x/y$  é equivalente a  $x(y^{-1})$ . Assim, podemos calcular  $a/b \pmod{n}$  se podemos encontrar um inverso  $b^{-1}$  tal que  $b(b^{-1}) \equiv 1 \pmod{n}$ . Este inverso nem sempre existe – tente encontrar uma solução [inteira, claro] para  $(2 \cdot x) \equiv 1 \pmod{4}$ .

Sim, *podemos* simplificar uma congruência  $(a \cdot d) \equiv (b \cdot d) \pmod{d \cdot n}$  para uma  $a \equiv b \pmod{n}$ , de modo que podemos dividir todos os três termos por um fator comum, se houver. Assim,  $170 \equiv 30 \pmod{140}$  implica

que  $17 \equiv 3 \pmod{14}$ . No entanto <sup>[, dado  $(a,d) \equiv (b,d) \pmod{(n)}$ ,]</sup>, a congruência  $a \equiv b \pmod{n}$  deve ser falsa (ou seja, não tem solução) se  $\text{mdc}(a,n)$  não divide  $b$ .

### 7.4.2. Resolvendo Congruências Lineares

Uma congruência linear é uma equação da forma  $(a.x) \equiv b \pmod{n}$ . Resolver essa equação significa identificar quais os valores de  $x$  que a satisfazem.

Nem todas essas equações têm soluções. Vimos números inteiros que não têm inversos multiplicativos em relação a um dado módulo, o que significa que  $(a.x) \equiv 1 \pmod{n}$  não tem uma solução. Na verdade,  $(a.x) \equiv 1 \pmod{n}$  tem uma solução se e somente se o módulo e o multiplicador são relativamente primos, ou seja,  $\text{mdc}(a,n) = 1$ . Podemos utilizar o algoritmo de Euclides para encontrar esta inversa através da solução para  $a'.x + n.y' = \text{mdc}(a,n) = 1$ . Assim,  $[(a.x) \equiv 1 \pmod{n}] \rightarrow [(a.x) \equiv (a.x' + n.y') \pmod{n}]$ .

Claramente  $(n.y') \equiv 0 \pmod{n}$ , então na verdade este inverso é simplesmente o  $x'$  do algoritmo de Euclides. Em geral, existem três casos, dependendo da relação entre  $a$ ,  $b$ , e  $n$ :

- $\text{mdc}(a,b,n) > 1$ . Então, podemos dividir todos os três termos por este divisor para obter uma congruência equivalente. Isso nos dá um única solução mod a nova base; ou; equivalentemente;  $\text{mdc}(a,b,n)$  soluções  $\pmod{n}$ .
- $\text{mdc}(a,n)$  não divide  $b$ . Então, como descrito acima, a congruência pode não ter nenhuma solução.
- $\text{mdc}(a,n) = 1$ . Então há uma solução  $\pmod{n}$ . Além disso,  $x = (a^{-1}).b$  funciona, uma vez que  $(aa^{-1}b) \equiv b \pmod{n}$ . Como mostrado acima, este inverso existe e pode ser encontrado utilizando o algoritmo de Euclides.

#### EXEMPLO 1:

Resolva o seguinte *sistema de congruências simultâneas*, onde os módulos são iguais:

$$4a + b \equiv 17 \pmod{26}$$

$$19a + b \equiv 3 \pmod{26}$$

#### RESPOSTA:

Resolva as equações normalmente - você vai acabar com

$$15a \equiv -14 \equiv 12 \pmod{26}.$$

Para resolver  $15a \equiv 12 \pmod{26}$ , você divide tudo por 3 e obtém  $5a \equiv 4 \pmod{26}$ . Agora, use força bruta para achar um múltiplo de 5 que lhe dê 4 em módulo 26 <sup>(eu tenho certeza que há uma maneira mais elegante, mas fico satisfeito com a maneira que se segue)</sup>. Este múltiplo é 6, veja:  $5 \times 6 = 30 \equiv 4 \pmod{26}$ . Assim,  $a \equiv 6$ .

Aplicando isso na 1ª equação,  $4a + b = 17$ , você obtém  $b = 17 - 24 = -7 = 19 \pmod{26}$ .

Juntando tudo, as respostas são:  $a \equiv 6 \pmod{26}$ , e  $b \equiv 19 \pmod{26}$ .

**O Teorema Chinês do Resto** <sup>(que não vamos cobrar em exames)</sup> nos dá uma ferramenta para trabalhar com sistemas de congruências sobre módulos diferentes. Suponha que existe um inteiro  $x$  tal que  $x \equiv a_1 \pmod{m_1}$  e  $x \equiv a_2 \pmod{m_2}$ . Então  $x$  é unicamente determinado  $\pmod{m_1 m_2}$  se  $m_1$  e  $m_2$  são relativamente primos. Para encontrar esse  $x$ , e, assim, resolver o sistema de duas congruências, começamos por resolver as congruências lineares  $m_2 b_1 \equiv 1 \pmod{m_1}$  e  $m_1 b_2 \equiv 1 \pmod{m_2}$  para encontrar  $b_1$  e  $b_2$ , respectivamente. Em seguida, pode ser facilmente verificado que  $x = a_1 b_1 m_2 + a_2 b_2 m_1$  é uma solução para ambas as congruências originais.

Além disso, o teorema prontamente se estende aos sistemas de um número arbitrário de congruências cujos módulos são todos pares relativamente primos, analisados par a par.

Se  $m_k$  é um inteiro positivo e  $\text{mdc}(m_i, m_j) = 1$  ( $i \neq j$ ) (números primos entre si) então o sistema de congruências lineares:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

$$x \equiv a_4 \pmod{m_4}$$

$$x \equiv a_5 \pmod{m_5}$$

$$x \equiv a_6 \pmod{m_6}$$

...

$$x \equiv a_{n-1} \pmod{m_{n-1}}$$

$$x \equiv a_n \pmod{m_n}$$

Tem uma única solução:  $x \equiv X \pmod{m}$   $m = m_1 m_2 m_3 \dots m_{n-1} m_n$

O valor de  $X$  pode ser encontrado utilizando-se o Teorema Chinês do Resto:

$$X = a_1.M_1.x_1 + a_2.M_2.x_2 + a_3.M_3.x_3 + a_4.M_4.x_4 + \dots + a_n.M_n.x_n$$

$M_a$  é o produto de todos os  $m_k$  com exceção de  $m_a$  (Exemplo:  $M_1 = m_2.m_3 \dots m_n$ )

$x_a$  é o número que torna  $M_a.x_a \equiv 1 \pmod{m_a}$

### 7.4.3. Equações Diofantinas

**Equações Diofantinas** (no exame, no máximo, no máximo, poderá haver alguma pergunta conceitual do tipo "que significa... qual a ideia básica... etc.") são fórmulas em que as variáveis são restritas a números inteiros.

Por exemplo, o último teorema de Fermat refere-se a respostas para a equação  $a^n + b^n = c^n$ . Resolver tal equação para os números reais não é grande coisa. É somente se todas as variáveis forem restritas a números inteiros que o problema se torna difícil.

Equações diofantinas são difíceis de trabalhar, pois a divisão não é uma operação de rotina com fórmulas para inteiros. No entanto, existem algumas classes de equações diofantinas que são conhecidos como sendo solúveis e estas tendem a surgir frequentemente.

A classe mais importante é a de equações lineares diofantinas da forma

$ax - ny = b$ , em que  $x, y$  são variáveis inteiras, e  $a, b, n$  são constantes inteiras.

Pode ser prontamente demonstrado que essas equações são equivalentes à solução da congruência  $ax \equiv b \pmod{n}$  e, conseqüentemente, podem ser resolvidas usando as técnicas da seção anterior.

Análises diofantinas mais avançadas estão além do escopo deste pequeno livro de introdução à Matemática Discreta. Se você quiser ver mais sobre análises diofantinas, comece pelas referências- padrão na Teoria dos Números, tais como [Niven e Zuckerman 1991], [Hardy e Wright 1979], etc., depois siga para as referências adicionais que dão sobre tais análises. Depois, peça de um especialista referências mais novas e específicas.

**PROBLEMA 1:** Faça as tábuas de adição e multiplicação para  $\mathbf{Z}_6$ . ( $\mathbf{Z}_m$  é o conjunto das classes dos restos módulo  $m$ , isto é,  $\{0, \bar{1}, \dots, \bar{m}\}$ , onde  $\bar{y}$  é a classe  $\{x \in \mathbf{Z} \mid x \equiv y \pmod{m}\}$  )

**PROBLEMA 2:** Encontre o resto da divisão de  $7^{256}$  por 15.

**PROBLEMA 3:** Estabeleça a validade do critério para decidir se um inteiro é divisível por 3 (três) que você aprendeu na quarta série do ensino fundamental.

**PROBLEMA 4:** Mostre a validade da "prova dos nove" que foi ensinada na segunda série do ensino fundamental.

**PROBLEMA 5:** Considere a seguinte afirmativa sobre um natural  $n$ : "Um natural é divisível por  $n$  se- e- somente- se a soma de seus dígitos, quando representado na base 10, é divisível por  $n$ ". Para que naturais  $n$  esta afirmativa é verdadeira?

**PROBLEMA 6:** Liste todos os divisores de zero de  $\mathbf{Z}_{45}$ .

**PROBLEMA 7:** Encontre todos os valores inteiros de  $X$  que satisfazem cada uma das congruências abaixo:

- (i)  $5X \equiv 3 \pmod{9}$ ;
- (ii)  $6X \equiv 3 \pmod{9}$ ;
- (iii)  $6X \equiv 4 \pmod{9}$ ;
- (iv)  $2X + 3 \equiv 5X \equiv 9 \pmod{13}$ ;
- (v)  $X^2 \equiv 1 \pmod{16}$ .

## 7.5. TRIPLAS PITAGÓRICAS:

**Triplas Pitagóricas** são três inteiros positivos  $a, b, c$  tais que  $a^2 + b^2 = c^2$ .

Infinitas Triplas Pitagóricas podem ser obtidas a partir de uma, cada vez multiplicando-se esta por uma diferente constante positiva. Por isso, estamos interessados em Triplas Pitagóricas **Primitivas**, onde  $a, b, c$  não têm fator comum (são primos entre si).

**Teorema das Triplas Pitagóricas:** Cada Tripla Pitagórica Primitiva ( $a, b, c$ ) (assume-se que  $a$  é ímpar,  $b$  é par,  $a$  e  $b$  são primos entre si) pode ser encontrada assim:

$a = s \cdot t$ , onde  $s > t \geq 1$  são escolhidos como inteiros ímpares sem fatores comuns

$b = (s^2 - t^2)/2$  (note que, assim,  $b$  será par)

$c = (s^2 + t^2)/2$

Ver prova na seção 2 de [http://ssli.ee.washington.edu/~halloj3/math\\_sen\\_synth07.pdf](http://ssli.ee.washington.edu/~halloj3/math_sen_synth07.pdf). Mas o artigo em <http://mathworld.wolfram.com/PythagoreanTriple.html> é mais específico sobre o assunto.



EXEMPLO 1: Se você escolher  $s = 3$ ;  $t = 1$ ; achará a Tripla Pitagórica Primitiva que tem  $a = s.t = 3 \times 1 = 3$ ;  $b = (9-1)/2 = 4$ ;  $c = (9+1)/2 = 5$

EXEMPLO 2: Se você escolher  $s = 9$ ;  $t = 7$ ; achará a T.P. Primitiva que tem  $a = s.t = 9 \times 7 = 63$ ;  $b = (s.s - t.t)/2 = (81-49)/2 = 16$ ;  $c = (s.s+t.t)/2 = (81+49)/2 = 65$ .

EXEMPLO 3: Se você escolher  $s = 5$ ;  $t = 3$ ; achará a T.P. Primitiva que tem  $a = s.t = 15$ ;  $b = 8$ ;  $c = 17$ .

EXEMPLOS 4 (vários exemplos):

$$r = 2, s = 1, (a,b,c) = (3,4,5).$$

$$r = 3, s = 2, (a,b,c) = (5,12,13).$$

$$r = 4, s = 1, (a,b,c) = (15,8,17).$$

$$r = 4, s = 3, (a,b,c) = (7,24,25).$$

$$r = 5, s = 2, (a,b,c) = (21,20,29).$$

$$r = 5, s = 4, (a,b,c) = (9,40,41).$$

$$r = 99, s = 62, (a,b,c) = (5957,12276,13645).$$

EXEMPLO 5: Triplas Pitagóricas são formadas por 3 inteiros  $(a,b,c)$  tais que  $a^2 + b^2 = c^2$ . Estamos interessados somente nas Triplas Pitagóricas *Primitivas*, onde  $a,b,c$  não têm nenhum divisor em comum (são primos entre si). Prove que ou  $a$  ou  $b$  é ímpar e o outro é o par, e que  $c$  é sempre ímpar.

RESPOSTA:

--  $a$  e  $b$  não podem, simultaneamente, ser par: se o fossem,  $c$  também seria par. Isto significa que  $a, b, c$  e teriam um fator comum de 2, e assim  $(a, b, c)$  não seria uma T.P. Primitiva. Portanto,  $a$  e  $b$  não podem, simultaneamente, ser par.

--  $a$  e  $b$  não podem, simultaneamente, ser ímpar: Se o fossem, então  $c$  seria par. Isto significa que  $a = 2x + 1$ ,  $b = 2y + 1$ , e  $c = 2z$ , para alguns números  $x, y$ , e  $z$ . Substitua  $a = 2x + 1$ ,  $b = 2y + 1$ , e  $c = 2z$  na equação  $a^2 + b^2 = c^2$  e simplifique até obter  $2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2$ . O lado esquerdo é ímpar e o lado direito é par (portanto a equação é falsa), de modo que  $a$  e  $b$  não podem ser simultaneamente ímpar.

--  $c$  é ímpar: se um elemento do par  $(a,b)$  é par e o outro é ímpar, então a soma de seus quadrados é ímpar. Portanto,  $c$  é ímpar.

EXEMPLO 6: Triplas Pitagóricas são formadas por 3 inteiros positivos  $(a,b,c)$  tais que  $a^2 + b^2 = c^2$ . Estamos interessados somente nas Triplas Pitagóricas *Primitivas*, onde  $(a,b,c)$  não têm nenhum divisor em comum (são primos entre si). Prove que  $a$  e  $b$  não podem ambos ser par, nem podem ambos ser ímpar.

RESPOSTA: Ora, este é o mesmo exemplo 5, mas vamos conceder em resolvê-lo de novo, com palavras um pouquinho diferentes, talvez lhe ajude a compreender melhor algumas coisas de provas:

--  $a$  e  $b$  não podem ambos ser par, porque  $a^2$  e  $b^2$  seriam pares, portanto a soma deles ( $c^2$ ) teria que ser um par, portanto  $a, b, c$  seriam divisíveis por 2 e a tripla não seria primitiva.

--  $a$  e  $b$  não podem ambos ser ímpar, porque, então, os seus quadrados deixariam resto 1 quando divididos por 4 (porque  $(2n+1)^2 = 4n^2 + 2 \times 2n + 1$ ), então  $a^2 + b^2$  deixaria resto 2 quando dividido por 4. Isto implicaria que  $c$  é par, assim  $c^2$  é divisível por 4. Esta é uma contradição:  $c^2$  não pode deixar restos de ambos 0 e 2 quando dividido por 4. Assim não ambos de  $a$  e  $b$  são ímpar.

EXEMPLO 7: Prove que, **em cada T.P. Primitiva, um dos números é divisível por 3, um dos números é divisível por 4, e um dos números é divisível por 5.**

RESPOSTA:

Reescrevamos o Teorema das Triplas Pitagóricas Primitivas:

**Se  $(x,y,z)$  é uma T.P. Primitiva, então sejam os inteiros  $a > b \geq 1$  escolhidos: 1) como primos entre si; 2) que não são, ambos, ímpares; 3) que satisfaçam**

$$x = 2ab$$

$$y = a^2 - b^2$$

$$z = a^2 + b^2$$

1) Provemos que  $x = 2ab$  é divisível por 4.

$a$  e  $b$  podem ser (ambos pares) XOR (um par e outro ímpar). (Se eles fossem ambos ímpares, isto contradizeria uma de nossas suposições originais.) Em qualquer caso, um deles tem que ser par.

Digamos que o número par é o  $a$ . Assim,  $a = 2n$ , para algum número inteiro  $n$ , e  $x = 2ab = 2(2n)b = 4nb$  é divisível por 4. O mesmo vale se  $b$  é par.

2) Provemos que um número ( $x$  ou  $y$  ou  $c$ ) é sempre divisível por 3.

Qualquer inteiro  $n$  pode ser escrito na forma:  $n \equiv p \pmod{3}$ , onde  $p$  é 0, 1 ou 2.

Se  $n \equiv 0 \pmod{3}$ , então  $n^2 \equiv 0 \pmod{3} \times 0 \pmod{3} \equiv 0 \pmod{3}$

Se  $n \equiv 1 \pmod{3}$ , então  $n^2 \equiv 1 \pmod{3} \times 1 \pmod{3} \equiv 1 \pmod{3}$

Se  $n \equiv 2 \pmod{3}$ , então  $n^2 \equiv 2 \pmod{3} \times 2 \pmod{3} \equiv 1 \pmod{3}$

Então, todo inteiro elevado a 2 é 0 ou é 1, tudo isso (mod 3).

Se algum de  $x$ ,  $y$  ou  $z$  é igual a 0 (mod 3), acabamos prova, porque então eles serão divisíveis por 3.

Suponha que nenhum de  $x$ ,  $y$  ou  $z$  é igual a 0 (mod 3). Sabemos que

$$x^2 + y^2 = z^2$$

e, desde que  $x$  e  $y$  são iguais a 1 (mod 3) ou 2 (mod 3),

$$z^2 \equiv 1 \pmod{3} + 1 \pmod{3} \equiv 2 \pmod{3}$$

Mas isso contradiz com o que foi provado e sublinhado, pouco acima ("todo inteiro elevado a 2 é 0 ou é 1, tudo isso (mod 3)").

Portanto, um dos três ( $x$  ou  $y$  ou  $z$ ) tem que ser divisível por 3.

3) Provemos que um número ( $x$  ou  $y$  ou  $z$ ) é um múltiplo de 5

Mais uma vez o mesmo tipo de argumento se mantém. Considere o que acontece quando elevamos inteiros ao quadrado, em mod 5. Digamos que  $m = q \pmod{5}$ . Então

Se  $q = 0$ , então  $m^2 = 0 \pmod{5}$

Se  $q = 1$ , então  $m^2 = 1 \pmod{5}$

Se  $q = 2$ , então  $m^2 = 4 \pmod{5}$

Se  $q = 3$ , então  $m^2 = 4 \pmod{5}$

Se  $q = 4$ , então  $m^2 = 1 \pmod{5}$

Assim, todo inteiro elevado a 2 é 0 ou é 1 ou é 4, tudo isso (mod 5).

Novamente, considere os nossos números  $x$ ,  $y$ , e  $z$ .

Se algum deles é divisível por 5, então terminamos a prova.

Suponha que nenhum deles é divisível por 5. A equação  $x^2 + y^2 = z^2$  nos diz que  $z^2$  é uma de três coisas: 0 (isto é, 1 + 4), ou 2 (isto é, 1 + 1), ou 3 (isto é, 4 + 4), tudo isso (mod 5). Uma vez que um número inteiro elevado ao quadrado nunca pode ser 2 ou 3 (mod 5), então  $z^2$  deve ser 0 (mod 5), o que significa que  $z$  é divisível por 5. Isto contradiz a nossa suposição original.

Por isso, um dos três números tem que ser divisível por 5.

EXEMPLO 8: À luz do teorema acima (Exemplo 7 "um dos números é divisível por 3, outro dos números é divisível por 4, e um outro dos números é divisível por 5."), como você explica que  $a = 15$ ;  $b = 8$ ;  $c = 17$  formam uma T.P. (pois  $a^2 + b^2 = 15^2 + 8^2 = 225 + 64 = 289 = 17^2$ ), mas 17 não é divisível por 3, nem por 4, nem por 5?

RESPOSTA: A citação do teorema está errada. O correto somente diz "um dos números é divisível por 3, um dos números é divisível por 4, e um dos números é divisível por 5." Não diz que esses números são distintos. 15 é divisível por 3, 8 é divisível por 4, e 15 é divisível por 5.

## Recapitulando a unidade

Parabéns! Você concluiu a unidade VII e, se foi disciplinado e realmente "suou" estudando 4 a 8 h cada semana, deve ter aprendido muitas coisas da parte básica da "Teoria dos Números" que lhe serão indispensáveis ou muito úteis em todo o resto do curso e sua vida profissional: Conceitos e propriedades dos primos, como testar a primalidade de um natural exatamente (se for pequeno) e com altíssima probabilidade e eficiência (se for enorme); divisibilidade e como achar mdc e mmc eficientemente; aritmética modular e sua aplicação à rápida exponenciação modular, vital para muita coisa da criptografia; congruências; triplas pitagóricas; as mais simples equações diofantinas e seus sistemas de equações.

Agora, um esforço final: invista pesado na próxima semana, revisando todas as 7 unidades, particularmente todos os exercícios que você já fez para nota e todos os exercícios de autoavaliação (sem nota) preparatórios para o exame final, depois confiantemente se submeta à prova final. Você pode ter pleno sucesso, só depende de você fazer este esforço final.

Desejamos-lhe todo sucesso nas provas finais desta disciplina, e na continuação do curso, e em toda sua vida profissional!



