

# Estrutura de Dados, Análise de Algoritmos e Complexidade Estrutural

4 de dezembro de 2007

# Sumário

<b>1</b>	<b>Introdução</b>	<b>2</b>
1.1	Alguns Conceitos Básicos . . . . .	3
1.2	Bibliografia do Curso . . . . .	3
1.3	Recursividade . . . . .	4
1.4	Teoria dos Números . . . . .	5
1.4.1	Indução Finita . . . . .	5
1.4.2	Chão e Teto . . . . .	6
1.4.3	Contagem de $n$ objetos . . . . .	6
1.4.4	Divisores e Múltiplos . . . . .	9
1.4.5	Números primos . . . . .	10
1.4.6	Crivo de Eratóstenes . . . . .	11
1.4.7	Máximo Divisor Comum . . . . .	11
1.4.8	Triângulo de Pascal . . . . .	12
1.4.9	Teorema Fundamental da Aritmética . . . . .	14
1.4.10	Aritmética Modular . . . . .	15
1.4.11	Teorema de Fermat . . . . .	18
1.4.12	Função Totiente de Euler (Função $\phi$ ) . . . . .	18
1.4.13	Quantidade de divisores (Função $\tau$ ) . . . . .	20
1.4.14	Soma dos divisores (Função $\sigma$ ) . . . . .	21
1.4.15	Congruência Linear . . . . .	22
1.4.16	Algoritmo de Euclides Estendido . . . . .	23
1.4.17	Quantidade de números primos menores que $x$ (Função $\pi$ ) . . . . .	24
1.5	Identidade Polinomial . . . . .	25

## Capítulo 1

# Introdução

## 1.1 Alguns Conceitos Básicos

Informalmente, um **algoritmo** é qualquer procedimento computacional bem definido que toma algum valor ou conjunto de valores como entrada e produz algum valor ou conjunto de valores como saída<sup>1</sup>.

Neste curso, iremos analisar diversos aspectos relacionados a algoritmos tais como:

- Qual o consumo de recursos computacionais (tempo de processamento, memória etc) do algoritmo em função do tamanho da entrada?
- Quanto longe o algoritmo está da melhor solução possível?
- Que condições podem fazer com que o algoritmo não produza uma resposta correta?

Para ter uma idéia deste tipo de análise, considere a função<sup>2</sup>:

$$g(n) = \begin{cases} n - 10 & \text{se } n > 100 \\ g^{(91)}(n + 901) & \text{se } n \leq 100 \end{cases}$$

onde  $g^{(91)}(n)$  significa a composição da função  $g$  com ela mesma  $g(g(\dots g(n) \dots))$  91 vezes.

Estaríamos interessados em saber, por exemplo, qual o valor de  $g(0)$  ou o número de vezes que a função  $g$  é chamada para determinar o valor de  $g(0)$ .

Note que podemos responder a estes questionamentos sem efetivamente implementar a função  $g$  como um programa de computador!

## 1.2 Bibliografia do Curso

A bibliografia do curso compreende os seguintes livros:

- CORMEN, T. H., LEISERSON, C.E. and STEIN, C. *Introduction do Algorithms*. The MIT Press. 2001. ISBN 0262032937.
- GAREY, M. R. and JOHNSON, D. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman. 1979. ISBN 0716710455.
- GRAHAM, R. L., KNUTH, D. E. and PATASHNIK, O. *Concrete Mathematics*. Addison-Wesley Publishing Company. 1994. ISBN 0201558025.

---

<sup>1</sup>Cf. [?] Pág.5

<sup>2</sup>Cf. [?]

## 1.3 Recursividade

Uma função se diz recursiva quando, em sua definição, ocorre uma chamada a própria função que se deseja definir.

Um bom exemplo é a função que calcula o fatorial de um número:

---

**Algorithm 1** FATORIAL\_RECURSIVO

---

**Require:**  $n \geq 0$

```
1: if  $n = 0$  then  
2:   return 1  
3: else  
4:   return  $n * FATORIAL\_RECURSIVO(n - 1)$   
5: end if
```

---

A função possui um caso trivial, que ocorre quando  $n = 0$ , que funciona como um *critério de parada*. Para valores de  $n > 0$  a função chama a si mesma várias vezes, reduzindo o valor de  $n$  em cada chamada.

O fatorial também pode ser calculado por uma função não recursiva:

---

**Algorithm 2** FATORIAL\_ITERATIVO

---

**Require:**  $n \geq 0$

```
1:  $aux \leftarrow 1$ ;  
2: for  $i = 1$  to  $n$  do  
3:    $aux \leftarrow aux * i$ ;  
4: end for  
5: return  $aux$ 
```

---

Exemplos de outras funções recursivas:

Função 91 de McCarthy[?]:

$$g(n) = \begin{cases} n - 10 & \text{se } n > 100 \\ g(g(n + 101)) & \text{se } n \leq 100 \end{cases}$$

Função 91 generalizada de Knuth[?]:

$$g(n) = \begin{cases} n - 10 & \text{se } n > 100 \\ g^{(91)}(n + 901) & \text{se } n \leq 100 \end{cases}$$

## 1.4 Teoria dos Números

Muitos algoritmos são analisados a partir de definições e teoremas da Teoria dos Números, que é o ramo da Matemática que estuda as propriedades dos números inteiros.

### 1.4.1 Indução Finita

O Princípio da Indução Finita (PIF) é utilizado para provar que uma determinada propriedade matemática vale para um subconjunto dos números inteiros.

**Proposição 1.4.1** (Princípio da Indução Finita). *Seja  $P(n)$  uma certa propriedade matemática válida para números inteiros  $n$  tais que:*

- (i)  $P(n)$  é válida para um certo inteiro  $n = n_0$ .
- (ii) Para quaisquer  $k$  inteiros, com  $k \geq n_0$ , se  $P(k)$  é válida, então  $P(k+1)$  também vale.

Satisfeitas estas condições,  $P(n)$  é válida para todo inteiro  $n \geq n_0$ .

Particularmente, quando  $n_0 = 0$  a propriedade  $P(n)$  vale para todos os números naturais.

Podemos usar o PIF para provar algumas proposições sobre os números inteiros.

**Proposição 1.4.2.** *Para qualquer  $n$  inteiro,  $\sum_{k=1}^n k = n(n+1)/2$ .*

*Demonstração.* Por indução em  $n$ .

Se  $n = 1$  então  $\sum_{k=1}^n k = \sum_{k=1}^1 k = 1$  e  $n(n+1)/2 = 1(1+1)/2 = 1$ . Portanto, a proposição vale para  $n = 1$ .

Agora, supondo que a proposição vale para  $n$ , vamos provar que vale para  $n+1$ .

$$\sum_{k=1}^{n+1} k = (n+1) + \sum_{k=1}^n k \quad (1.1)$$

Usando, na equação acima a **hipótese indutiva**  $\sum_{k=1}^n k = n(n+1)/2$  temos:

$$\sum_{k=1}^{n+1} k = (n+1) + \frac{n(n+1)}{2} = \frac{2n+2+n^2+n}{2} = \frac{n^2+3n+2}{2} \quad (1.2)$$

Portanto:

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+1+1)}{2} \quad (1.3)$$

Ou seja,  $\sum_{k=1}^n k = n(n+1)/2$  vale para qualquer valor de  $n \geq 1$ . □

**Proposição 1.4.3.** *A soma de  $n$  números ímpares é um quadrado perfeito.*

*Demonstração.* Por indução em  $n$ .

Pretendemos provar que, para qualquer  $n$  inteiro,  $\sum_{k=1}^n (2k-1) = n^2$ .

Se  $n = 1$  então  $\sum_{k=1}^n (2k-1) = \sum_{k=1}^1 (2k-1) = 2 \cdot 1 - 1 = 1$  e  $n^2 = 1^2 = 1$ . Portanto, a proposição vale para  $n = 1$ .

Supondo que é válido para  $n$ , vamos provar que é válido para  $n + 1$ :

$$\sum_{k=1}^{n+1} (2k - 1) = 2(n + 1) - 1 + \sum_{k=1}^n (2k - 1) \quad (1.4)$$

Usando a Hipótese Indutiva temos:

$$\sum_{k=1}^{n+1} (2k - 1) = 2(n + 1) - 1 + n^2 = 2n + 2 - 1 + n^2 = n^2 + 2n + 1 = (n + 1)^2 \quad (1.5)$$

□

**Proposição 1.4.4.** Para qualquer  $n$  inteiro,  $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$ .

### 1.4.2 Chão e Teto

**Definição 1.4.1** (Teto). Se  $x$  é um número real então  $\lceil x \rceil$  (“teto” ou “ceiling” de  $x$ ) é o menor inteiro maior ou igual a  $x$ .

**Definição 1.4.2** (Chão). Se  $x$  é um número real então  $\lfloor x \rfloor$  (“chão” ou “floor” de  $x$ ) é o maior inteiro menor ou igual a  $x$ .

Exemplos:

(i)  $\lfloor 3.1 \rfloor = 3$  e  $\lceil 3.1 \rceil = 4$ .

(ii)  $\lfloor 3 \rfloor = \lceil 3 \rceil = 3$ .

(iii)  $\lfloor -3.1 \rfloor = -4$  e  $\lceil -3.1 \rceil = -3$ .

Note que, se  $n \in \mathbb{N}$  e  $x \in \mathbb{R}$ , então:

(i)  $n = \lfloor x \rfloor \Rightarrow n \leq x < n + 1$ .

(ii)  $\lfloor x \rfloor \leq x$ .

(iii)  $\lfloor x \rfloor = x \Rightarrow x \in \mathbb{Z}$ .

(iv)  $x - 1 < \lfloor x \rfloor \leq x$ .

Propriedades análogas podem ser demonstradas para  $\lceil x \rceil$ .

### 1.4.3 Contagem de $n$ objetos

#### Princípio Fundamental da Contagem

**Teorema 1.4.1** (Princípio Fundamental da Contagem). Se determinado evento ocorre em  $n$  etapas diferentes, e se a primeira etapa pode ocorrer de  $k_1$  maneiras diferentes, a segunda de  $k_2$  maneiras diferentes, e assim sucessivamente, então o número total  $T$  de maneiras de ocorrer o evento é dado por:

$$T = k_1 \cdot k_2 \cdot k_3 \cdot \dots \cdot k_n \quad (1.6)$$

**Definição 1.4.3.** O símbolo  $[n]$  denota o conjunto  $\{1, 2, \dots, n\}$  com  $n \in \mathbb{N}^*$ .

Exemplo:  $[2] = \{1, 2\}$ . Existem 4 subconjuntos de  $[2]$ :  $\{\}, \{1\}, \{2\}$  e  $\{1, 2\}$ .

**Teorema 1.4.2.**  $[n]$  possui  $2^n$  subconjuntos.

*Demonstração.* Para obter os subconjuntos de  $[n]$ , escolha (ou não escolha) o elemento ‘1’. Em seguida, escolha (ou não) o elemento ‘2’ e prossiga assim até o elemento ‘n’. Para cada um dos  $n$  elementos há 2 escolhas. Portanto, pelo Princípio Fundamental da Contagem, há  $2^n$  formas de se criar subconjuntos para  $[n]$ .  $\square$

### Cardinalidade

**Definição 1.4.4** (Cardinalidade). *O número de elementos em um conjunto é denominado cardinalidade.*

**Definição 1.4.5.** *A cardinalidade de um conjunto  $S$  é denotada por  $|S|$ .*

Exemplos:

(i)  $||[2]|| = 2$ .

(ii)  $|\{1, 3, 6\}| = 3$ .

**Definição 1.4.6.** *Um conjunto cuja cardinalidade é  $k$  é chamado de  $k$ -conjunto.*

### Fatorial

**Definição 1.4.7** (Fatorial). *O símbolo  $n!$ , que se lê “ $n$  fatorial”, indica o produto  $1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$  com  $n \in \mathbb{N}^*$ . Por convenção:  $0! = 1$ .*

**Teorema 1.4.3** (Aproximação de Stirling). *O valor de  $n!$  pode ser aproximado por:*

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2n\pi} \quad (1.7)$$

### Permutação

**Definição 1.4.8** (Permutação). *Denomina-se permutação a cada agrupamento de  $n$  elementos distintos, de forma que cada agrupamento se distingue dos demais apenas pela ordem de seus elementos.*

Exemplo: ‘abc’ e ‘cba’ são duas permutações distintas de ‘abc’.

**Teorema 1.4.4.**  *$n$  objetos distintos podem ser permutados de  $P(n) = n!$  maneiras.*

*Demonstração.* Para obter o primeiro elemento da permutação, podemos escolher  $n$  elementos. Uma vez escolhido o primeiro elemento, há  $(n-1)$  opções para escolher o segundo elemento,  $(n-2)$  opções para escolher o terceiro e assim sucessivamente até o último elemento. Pelo Princípio Fundamental da Contagem, o número total de permutações é dado por  $n(n-1)(n-2) \dots 2 \cdot 1$ . Por definição, este produto é igual a  $n!$ .  $\square$

Exemplo: Existem  $P(3) = 3! = 6$  anagramas<sup>3</sup> da palavra ‘mar’: arm, amr, ram, rma, mar e mra.

---

<sup>3</sup>Anagrama é qualquer palavra, com significado ou não, que pode ser formada com as letras da palavra dada.



**Definição 1.4.9** (Ordem Lexicográfica). *Diz-se que as permutações estão em ordem lexicográfica quando são mostradas na forma como apareceriam em um léxico (dicionário). Ou seja, quando estão ordenadas alfabeticamente tal como mostrado no exemplo acima.*

**Teorema 1.4.5** (Permutação com Repetição). *O número total de permutações de  $n$  objetos, onde o objeto 1 se repete  $n_1$  vezes, o objeto 2 se repete  $n_2$  vezes, e assim assim sucessivamente até o objeto  $k$  que se repete  $n_k$  vezes, é dado por:*

$$P(n, n_1, \dots, n_k) = \frac{n!}{n_1! n_2! \dots n_k!} \quad (1.8)$$

Exemplo: Existem  $P(4, 2) = \frac{4!}{2!} = 12$  anagramas da palavra ‘PATA’: AAPT, AATP, APAT, APTA, ATAP, ATPA, PAAT, PATA, PTAA, TAAP, TAPA e TPAA.

### Arranjo

**Definição 1.4.10** (Arranjo). *Definimos como “arranjo de  $n$  elementos, escolhidos  $k$  a  $k$ ” como:*

$$A(n, k) = \frac{n!}{(n-k)!} = n(n-1)(n-2) \dots (n-k+1) \quad (1.9)$$

Exemplo:  $S = \{X, Y, Z\}$

Existem  $A(3, 1) = \frac{3!}{(3-1)!} = 3$  arranjos dos 3 elementos  $S$  agrupados 1 a 1:  $\{X\}$ ,  $\{Y\}$  e  $\{Z\}$ .

Existem  $A(3, 2) = \frac{3!}{(3-2)!} = 6$  arranjos dos 3 elementos  $S$  agrupados 2 a 2:  $\{XY\}$ ,  $\{XZ\}$ ,  $\{YX\}$ ,  $\{YZ\}$ ,  $\{ZX\}$  e  $\{ZY\}$ .

Existem  $A(3, 3) = \frac{3!}{(3-3)!} = 6$  arranjos dos 3 elementos  $S$  agrupados 3 a 3:  $\{XYZ\}$ ,  $\{XZY\}$ ,  $\{YXZ\}$ ,  $\{YZX\}$ ,  $\{ZXY\}$  e  $\{ZYX\}$ .

**Teorema 1.4.6.** *Há  $A(n, k)$  modos de obtermos um  $k$ -subconjunto de  $[n]$ .*

**Definição 1.4.11** (Arranjo com Repetição). *Definimos como “arranjo de  $n$  elementos, escolhidos  $k$  a  $k$ , com repetição” como:*

$$A^k_n = n^k \quad (1.10)$$

Exemplo:  $S = \{X, Y, Z\}$

Existem  $A^2_3 = 3^2 = 9$  arranjos dos 3 elementos  $S$  agrupados 2 a 2, com repetição:  $\{XX\}$ ,  $\{XY\}$ ,  $\{XZ\}$ ,  $\{YX\}$ ,  $\{YY\}$ ,  $\{YZ\}$ ,  $\{ZX\}$ ,  $\{ZY\}$  e  $\{ZZ\}$ .

### Combinação

**Definição 1.4.12** (Combinação). *Definimos como “combinação de  $n$  elementos, escolhidos  $k$  a  $k$ ” como:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (1.11)$$

com  $n, k \in \mathbb{N}$  e  $0 \leq k \leq n$ .

Por convenção,  $\binom{n}{k} = 0$  para  $k < 0$  e para  $k > n$ .  
Alguns valores notáveis para qualquer  $n \in \mathbb{N}$ :

- (i)  $\binom{n}{0} = 1$ .
- (ii)  $\binom{n}{1} = n$ .
- (iii)  $\binom{n}{n} = 1$ .
- (iv)  $\binom{n}{2} = \frac{n(n-1)}{2}$ .

**Teorema 1.4.7.** Para  $n, k \in \mathbb{N}$  e  $0 \leq k \leq n$ , temos: um conjunto com  $n$  elementos tem  $2^n$  subconjuntos dos quais  $\binom{n}{k}$  têm cardinalidade  $k$ :

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad (1.12)$$

### Binômio de Newton

**Teorema 1.4.8** (Binômio de Newton). Para  $n \in \mathbb{N}$  e  $x, y \in \mathbb{R}$  temos:

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \quad (1.13)$$

Em especial, quando  $y = 1$  temos:

$$(1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k \quad (1.14)$$

O termo  $\binom{n}{k}$  que define a combinação de  $n$  elementos tomados  $k$  a  $k$  é também conhecido como “coeficiente binomial”.

### 1.4.4 Divisores e Múltiplos

**Definição 1.4.13** (Divisão Inteira). Sejam  $a \in \mathbb{Z}$  e  $b \in \mathbb{Z}^*$ . Dividir  $a$  por  $b$  é encontrar um inteiro  $q$ , denominado quociente, e um inteiro  $r$ , denominado resto, tal que  $0 \leq r < |b|$  e  $a = qb + r$ .

A Divisão Inteira também é conhecida como Divisão Euclidiana.

Notação:

- (i) O operador **mod** retorna o resto da divisão de  $a$  por  $b$ . Portanto,  $r = a \bmod b$
- (ii) O operador **div** retorna o quociente da divisão inteira de  $a$  por  $b$ . Portanto,  $q = a \operatorname{div} b$

Exemplo:  $23 = 3 \cdot 7 + 2$ . Portanto, na divisão inteira de 27 por 3, o quociente é  $3 = 27 \operatorname{div} 7$  e o resto é  $2 = 27 \bmod 7$ .

**Definição 1.4.14** (Divisor). Sejam  $a \in \mathbb{Z}$  e  $b, c \in \mathbb{Z}^*$ . Diz-se que  $b$  é divisor de  $a$  se existe  $c$  tal que  $a = bc$ . Por convenção, diz-se que 0 é divisor de 0.

Exemplo: 3 é divisor de 6 pois  $6 = 2 \cdot 3$ .

Formalmente os divisores de um número são números inteiros que podem ser positivos ou negativos. Os divisores de 6 são  $\{-6, -3, -2, -1, 1, 2, 3, 6\}$ .

É muito comum, porém, referir-se em teoremas apenas aos divisores positivos quando se fala em “divisores de um número”.

Notação:

(i)  $a|b$  significa ‘ $a$  é divisor de  $b$ ’. Portanto,  $a|b \Leftrightarrow a \bmod b = 0$

(ii)  $a \nmid b$  significa ‘ $a$  não é divisor de  $b$ ’. Portanto,  $a \nmid b \Leftrightarrow a \bmod b \neq 0$

**Definição 1.4.15** (Múltiplo). Se  $a|b$  então  $b$  é múltiplo de  $a$ .

Portanto,  $a|b$  é equivalente a:

(i)  $a$  divide  $b$ .

(ii)  $a$  é um divisor de  $b$ .

(iii)  $a$  é um fator  $b$ .

(iv)  $b$  é múltiplo de  $a$ .

**Teorema 1.4.9** (Propriedades da Divisão Inteira). De modo geral, se  $a, b, c \in \mathbb{Z}^*$  então:

(i) Se  $a|b$  e  $b|c$  então  $a|c$  (propriedade transitiva).

(ii) Se  $a|b$  e  $a|c$  então  $a|(mb + nc)$  para quaisquer  $m, n$  inteiros (linearidade).

(iii) Se  $a|b$  então  $ma|mb$  para qualquer  $m$  inteiro (propriedade multiplicativa).

(iv) Se  $ma|mb$  e  $b \neq 0$  então  $a|b$  (propriedade do cancelamento).

(v)  $1|a$ , ou seja, 1 é divisor de qualquer inteiro.

(vi)  $a|0$ , ou seja, qualquer inteiro é divisor de 0.

(vii)  $0|a \Rightarrow a = 0$ , ou seja, apenas zero é divisor de zero.

(viii) Se  $a|b$ ,  $a > 0$  e  $b > 0$  então  $a \leq b$  (propriedade da comparação).

(ix) Se  $a|b$  e  $a|c$  então  $a|(b - c)$ .

### 1.4.5 Números primos

**Definição 1.4.16** (Número Primo). Diz-se que um inteiro  $p > 1$  é primo se seus únicos divisores positivos são  $p$  e 1.

**Definição 1.4.17** (Número Composto). Diz-se que um inteiro  $p > 1$  é um número composto se ele não é primo.

O número 1 não é considerado nem primo e nem composto. Ele é a identidade multiplicativa e constitui uma classe em si mesmo.

**Definição 1.4.18** (Fatoração). O processo de encontrar os fatores primos de um número inteiro é denominado ‘fatoração’.

**Definição 1.4.19** (Fatoração Canônica). Diz-se que um inteiro  $n > 1$  está ‘fatorado em sua forma canônica’ quando  $n$  é expresso na forma:

$$n = \prod_{k=1}^m p_k^{\alpha_k} \quad (1.15)$$

com todos os  $p_k$  primos,  $p_k < p_{k+1} \forall k : 1 \leq k \leq m$  e  $\alpha_k \in \mathbb{N}$ .

**Lema 1.4.1.** Se  $n > 1$  é composto, então pelo menos um de seus fatores é menor que  $\sqrt{n}$ .

*Demonstração.* Por contradição.

Se  $n$  é composto então podemos escrevê-lo na forma  $n = ab$  com  $a, b \in \mathbb{N}$  com  $1 < a < n$  e  $1 < b < n$ .

Afirmamos que  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$ .

Se esta afirmativa for falsa, então  $a > \sqrt{n}$  e  $b > \sqrt{n}$  e, portanto,  $ab > \sqrt{n}\sqrt{n} = n$ , o que é uma contradição pois sabemos que  $ab = n$ .

Logo, a afirmativa é verdadeira.  $\square$

**Teorema 1.4.10.** Se  $n > 1$  é composto, então existe um primo  $p \leq \sqrt{n}$  tal que  $p|n$ .

*Demonstração.* Se  $n$  é composto então podemos escrevê-lo na forma  $n = ab$  com  $a, b \in \mathbb{N}$  com  $1 < a < n$  e  $1 < b < n$ .

Pelo lema 1.4.1 sabemos que  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$ . Sem perda de generalidade, vamos supor que  $a \leq \sqrt{n}$ .

Sabemos que existe um primo  $p$  que é divisor de  $a$  pois todo inteiro  $a > 1$  pode ser fatorado canonicamente de acordo com a equação 1.4.19. Portanto, basta tomarmos  $p$  igual a um dos  $p_i$  da fatoração canônica.

Se  $p|a$  então  $p \leq a$  pois  $p$  é um dos fatores de  $a$ . Mas  $a \leq \sqrt{n}$  portanto:  $p \leq a \leq \sqrt{n}$ .  $\square$

### 1.4.6 Crivo de Eratóstenes

De acordo com o teorema 1.4.10, para saber se um número  $n$  é primo, bastar dividir  $n$  por todos os números primos  $p \leq \sqrt{n}$ . Se nenhum divisor de  $n$  for encontrado neste intervalo, então  $n$  é primo.

Este é o algoritmo *Crivo de Eratóstenes* atribuído ao matemático, geógrafo e astrônomo grego Eratóstenes, nascido em Cirene, Grécia em 276 aC.

### 1.4.7 Máximo Divisor Comum

Considere os inteiros  $8 = 2^3$  e  $12 = 2^2 \cdot 3$ .

Os divisores positivos de 8 são  $\{1, 2, 4, 8\}$  e os divisores positivos de 12 são  $\{1, 2, 3, 4, 6, 12\}$ . Os divisores comuns de 8 e 12 são  $\{1, 2, 4\}$ . Portanto, o maior divisor comum é 4.

**Definição 1.4.20** (Máximo Divisor Comum(MDC)). Se  $a$  e  $b$  são dois inteiros não negativos, definimos  $MDC(a, b)$  como o número inteiro  $m$  que:

- (i) É divisor comum de  $a$  e de  $b$  (isto é, é divisor tanto de  $a$  quanto de  $b$ ) e
- (ii) É divisível por qualquer outro divisor comum de  $a$  e  $b$ .

Por convenção,  $MDC(0, 0) = 0$ .

**Definição 1.4.21** (Números relativamente primos). *Diz-se que  $a$  e  $b$  são números relativamente primos, co-primos, ou primos entre si quando  $MDC(a, b) = 1$ .*

Note que dois números podem ser co-primos sem que nenhum deles seja primo. Exemplo:  $4 = 2^2$  e  $15 = 3 \cdot 5$  são relativamente primos (apesar de nenhum dos dois números ser primo) pois  $MDC(4, 15) = 1$ .

**Teorema 1.4.11.** *Dois inteiros consecutivos são sempre co-primos. Formalmente:  $MDC(a, a + 1) = 1 \quad \forall a \in \mathbb{Z}$ .*

**Lema 1.4.2** (Lema de Euclides). *Se  $p$  é primo e  $p|ab$  então  $p|a$  ou  $p|b$ .*

*Demonstração.* Se  $p|a$  então o lema está provado.

Se  $p \nmid a$  então seja  $d = MDC(p, a)$ . Portanto,  $d|p$  e  $d|a$ .

Mas, se  $p$  é primo, então  $d = 1$  ou  $d = p$ . Se  $d = p$  então  $d|a$  o que contradiz nossa hipótese de que  $p \nmid a$ . Portanto,  $d = 1$ .

Mas, se  $d = 1$ , então  $MDC(p, a) = 1$ .

Se  $MDC(p, a) = 1$  e  $p|ab$  então  $p|b$ . □

Note que se  $a|bc$  então nem sempre  $a|b$  ou  $a|c$ . Por exemplo,  $6|4 \cdot 9$  mas  $6 \nmid 4$  e  $6 \nmid 9$ . Isto ocorre porque  $MDC(6, 4) \neq 1$  e  $MDC(6, 9) \neq 1$ .

**Teorema 1.4.12.** *Se  $MDC(a, b) = c$  então  $MDC(a, a \pmod{b}) = c$ .*

A partir deste teorema é possível definir um algoritmo para calcular o MDC de dois inteiros.

#### Algoritmo Iterativo do Máximo Divisor Comum

```
int MDCIterativo(int m, int n){
    int resto;
    while (n>0){
        resto = m % n;
        m = n;
        n = resto;
    }
    return m;
}
```

#### Algoritmo Recursivo do Máximo Divisor Comum

```
int MDCRecursivo(int m, int n){
    if (n==m) return m;
    return MDCRecursivo(n, m%n);
}
```

### 1.4.8 Triângulo de Pascal

**Definição 1.4.22** (Triângulo de Pascal). *Chama-se de “Triângulo de Pascal” ao agrupamento triangular infinito que se obtém organizando os coeficientes  $\binom{n}{k}$  com  $n, k \in \mathbb{N}^*$  de modo que  $n$  representa a linha e  $k \leq n$  a coluna do coeficiente:*

1  
 1 1  
 1 2 1  
 1 3 3 1  
 1 4 6 4 1  
 1 5 10 10 5 1  
 1 6 15 20 15 6 1  
 1 7 21 35 35 21 7 1  
 ...

**Teorema 1.4.13.** *Quando o segundo termo do triângulo é primo então todos os termos (exceto os extremos) são múltiplos deste primo.*

*Demonstração.*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\dots(n-k+1)(n-k)!}{k!(n-k)!} \quad (1.16)$$

Portanto:

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)(k-2)\dots 2 \cdot 1} \quad (1.17)$$

O maior fator do denominador, ou seja  $k$ , é menor ou igual a  $n$ .

Se  $n$  for um número primo, então  $n$  não poderá ser simplificado com nenhum outro fator do denominador (afinal, o único divisor de  $n$  primo que é menor que  $n$  é 1) e  $n | \binom{n}{k}$ . Portanto, todos os termos (exceto os extremos) são múltiplos de  $n$ .  $\square$

**Teorema 1.4.14** (Relação de Stiffel). *Cada elemento no triângulo de Pascal é igual à soma do elemento imediatamente acima e seu antecessor:*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad (1.18)$$

**Teorema 1.4.15.** *A soma dos elementos de uma linha do Triângulo de Pascal é igual  $2^n$ :*

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad (1.19)$$

**Teorema 1.4.16.** *A soma dos elementos de uma coluna do Triângulo de Pascal é calculada por:*

$$\sum_{k=0}^m \binom{n+k}{n} = \binom{n+m+1}{n+1} \quad (1.20)$$

**Teorema 1.4.17.** *O Triângulo de Pascal é simétrico em relação à altura:*

$$\binom{n}{k} = \binom{n}{n-k} \quad (1.21)$$

**Teorema 1.4.18.** *O termo central é o maior termo do Triângulo de Pascal.*

*Demonstração.* Se  $n$  é ímpar, os coeficientes de maior ordem são  $\binom{n}{(n-1)/2} = \binom{n}{(n+1)/2}$ . Se  $n$  for par, o coeficiente central é  $\binom{n}{n/2}$ . Para um certo valor  $k$  temos que a razão entre os termos consecutivos  $\binom{n}{k+1}$  e  $\binom{n}{k}$  é dada por:

$$R_n(k) = \frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{n!/\{(k+1)!(n-k-1)!\}}{n!/\{k!(n-k)!\}} \quad (1.22)$$

Portanto:

$$R_n(k) = \frac{k!(n-k)!}{(k+1)!(n-k-1)!} = \frac{n-k}{k+1} \quad (1.23)$$

Tomando  $n$  fixo e variando  $k$ , vemos que  $R_n(k) > 1$  para  $k < (n-1)/2$  e  $R_n(k) < 1$  para  $k > (n-1)/2$ .  $\square$

O valor do termo central do Triângulo de Pascal é dado por:

$$\binom{n}{n/2} = \frac{n!}{(\frac{n}{2})!(n-\frac{n}{2})!} = \frac{n!}{(\frac{n}{2})!^2} \quad (1.24)$$

Usando a aproximação de Stirling temos:

$$\binom{n}{n/2} = \frac{\left(\frac{n}{e}\right)^n \sqrt{2n\pi}}{\left\{\left(\frac{n/2}{e}\right)^{n/2} \sqrt{n/2\pi}\right\}^2} \quad (1.25)$$

Portanto:

$$\binom{n}{n/2} = \sqrt{\frac{2}{n\pi}} 2^n \quad (1.26)$$

Notamos que o termo central, igual a  $\sqrt{\frac{2}{n\pi}} 2^n$ , é responsável por grande parte da soma de todos os termos, que é igual a  $2^n$ .

#### 1.4.9 Teorema Fundamental da Aritmética

**Teorema 1.4.19** (Teorema Fundamental da Aritmética). *Todo inteiro  $n > 1$  pode ser univocamente expresso na forma canônica. Em outras palavras, todo inteiro  $n > 1$  pode ser expresso na forma de um produto de números primos e esta decomposição é única, a menos da ordem dos fatores.*

*Demonstração.* Por indução em  $n$ .

Se  $n = 2$  então  $2 = 2^1$ .

Se  $n > 2$  é primo então  $n = n^1$ .

Se  $n$  é composto, então  $n = ab$  para  $a, b \in \mathbb{N}^*$ ,  $a < n$  e  $b < n$ . Pela hipótese indutiva,  $a$  e  $b$  se decompõem como produto de primos. Portanto  $n$ , sendo o produto de  $a$  por  $b$ , também se decompõe como produto de primos.

Vamos agora mostrar a unicidade, também por indução: Suponha que  $n$  admita duas fatorações  $n = p_1 p_2 \dots p_m$  e  $n = q_1 q_2 \dots q_s$  com  $p_k$  e  $q_k$  primos.

Se  $p_1$  é um dos fatores de  $n$  então, pelo lema 1.4.2  $p_1 | n$ . Logo,  $p_1 | q_1 q_2 \dots q_s$ . Portanto  $p_1$  divide algum dos  $q_k$  para  $1 \leq k \leq s$ . Neste caso,  $p_1 = q_k$  pois  $p_1$  é primo e seu único divisor maior que 1 é o próprio  $p_1$ .

Pela hipótese de indução  $\frac{n}{p_1} = \frac{n}{q_k} < n$  admite uma única fatoração prima. Portanto, concluímos que a fatoração é única.  $\square$

### 1.4.10 Aritmética Modular

Muitos problemas do dia-a-dia podem ser simplificados pela aritmética modular. A ideia básica consiste na escolha de um inteiro  $n$ , denominado “módulo”, e na substituição dos inteiros envolvidos pelo resto da sua divisão por  $n$ .

Exemplo: Sendo hoje terça-feira, que dia da semana será daqui a 1000 dias? Sabemos que os dias da semana se repetem a cada 7 dias. Portanto, podemos agrupar os 1000 dias em conjuntos de 7.

Portanto:  $142 = 1000 \bmod 7$  e  $6 = 1000 \operatorname{div} 7$ . Ou seja:  $1000 = 142 \cdot 7 + 6$ . Portanto, daqui a 1000 dias teremos o mesmo dia da semana que daqui a 6 dias: segunda-feira!

**Definição 1.4.23** (Equivalência Modular). *Se  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  com  $n > 1$ , dizemos que  $a$  e  $b$  são módulo  $n$  equivalentes e denotamos  $a \equiv b \pmod{n}$  quando  $n|(a - b)$ .*

Exemplo:  $23 \equiv -19 \pmod{7}$  pois  $7|(23 - (-19))$  ou seja  $7|42$ . De fato,  $42 = 6 \cdot 7 + 0$ .

A expressão  $a \equiv b \pmod{n}$  pode ser lida como:

- (i)  $a$  é equivalente a  $b$  módulo  $n$ .
- (ii)  $a$  é congruente a  $b$  módulo  $n$ .
- (iii)  $a$  e  $b$  são módulo  $n$  equivalentes.

Atenção:

- (i)  $38 \equiv 14 \pmod{12}$  pois  $12|(38 - 14)$ . Afinal,  $38 - 14 = 24 = 2 \cdot 12 + 0$ .
- (ii)  $38 = 14 \bmod 12$  tem notação parecida mas é uma afirmação falsa, pois  $14 \bmod 12$  é o resto da divisão de 14 por 12. Logo:  $14 \bmod 12 = 2 \neq 38$ .

**Teorema 1.4.20.** *Se  $a \equiv b \pmod{n}$  então  $\exists q \in \mathbb{Z} : a = qn + b$ .*

*Demonstração.* Da definição de equivalência modular temos que: se  $a \equiv b \pmod{n}$  então  $n|(a - b)$ .

Da definição de divisibilidade inteira, temos que: se  $n|(a - b)$  então  $\exists q \in \mathbb{Z} : (a - b) = qn + 0$ . Ou seja, se  $n$  divide  $(a - b)$ , então a divisão inteira de  $(a - b)$  por  $n$  resulta num quociente  $q$  inteiro e resto 0.

Se  $(a - b) = qn + 0$  então  $a = qn + b$ . □

**Teorema 1.4.21** (Propriedade Reflexiva da Congruência). *Se  $a \in \mathbb{Z}$  e  $n \in \mathbb{N}$  então  $a \equiv a \pmod{n}$ .*

*Demonstração.*  $a \equiv a \pmod{n} \Leftrightarrow n|(a - a) \Leftrightarrow n|0$ . Como todo inteiro é divisor de zero, a propriedade está provada. □

**Teorema 1.4.22** (Simetria da Congruência). *Se  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$  tal que  $a \equiv b \pmod{n}$  então  $b \equiv a \pmod{n}$ .*

*Demonstração.* Se  $a \equiv b \pmod{n}$ , então, por definição,  $n|(a - b)$ .

Se  $n|(a - b)$  então  $\exists q \in \mathbb{Z} : (a - b) = qn + 0$ .

Multiplicando a igualdade por  $(-1)$  temos:  $-(a - b) = (b - a) = -qn$ . Logo,  $n|(b - a)$ .

Portanto, por definição,  $b \equiv a \pmod{n}$ . □



**Teorema 1.4.23** (Transitividade da Congruência). *Se  $a, b, c \in \mathbb{Z}$  e  $n \in \mathbb{N}$  tal que  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n}$  então  $a \equiv c \pmod{n}$ .*

*Demonstração.* Se  $a \equiv b \pmod{n}$ , então, por definição,  $n|(a-b)$ . Analogamente, se  $b \equiv c \pmod{n}$ , então  $n|(c-b)$ .

Se  $n|(a-b)$  então  $\exists q_1 \in \mathbb{Z} : (a-b) = q_1n + 0$ . Analogamente,  $n|(b-c)$  então  $\exists q_2 \in \mathbb{Z} : (b-c) = q_2n + 0$ .

Mas  $a-c = (a-b) + (b-c) = q_1n + q_2n = (q_1 + q_2)n + 0$ . Portanto,  $n|(a-c)$ . Logo,  $a \equiv c \pmod{n}$   $\square$

**Teorema 1.4.24** (Igualdade do Resto na Equivalência Modular). *Se  $a, b \in \mathbb{N}$ ,  $n > 0$  e  $a \equiv b \pmod{n}$  então:*

$$a \bmod n = b \bmod n \quad (1.27)$$

Exemplo:  $23 \equiv -19 \pmod{7}$  pois  $7|(23-(-19))$  afinal  $23-(-19) = 42 = 6 \cdot 7 + 0$ . O resto da divisão de 23 por 7 é igual ao resto da divisão de -19 por 7. Ambos os restos são iguais a 2 pois  $23 = 3 \cdot 7 + 2$  e  $-19 = -3 \cdot 7 + 2$ .

**Teorema 1.4.25** (Soma na Congruência). *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $a \equiv b \pmod{n}$  então:*

$$a + c \equiv b + c \pmod{n} \quad (1.28)$$

*Demonstração.* Se  $a \equiv b \pmod{n}$ , então, por definição,  $n|(a-b)$ .

Mas  $a-b = (a+c) - (b+c)$  então  $n|(a+c) - (b+c)$ . Logo, por definição,  $a+c \equiv b+c \pmod{n}$   $\square$

Considere, por exemplo,  $a = 19, b = 3, c = 7$  e  $n = 8$ :

- (i)  $19 \equiv 3 \pmod{8}$  pois  $8|(19-3)$ . Afinal,  $19-3 = 16 = 2 \cdot 8 + 0$ .
- (ii)  $19+7 \equiv 3+7 \pmod{8}$ . Ou seja  $26 \equiv 10 \pmod{8}$  pois  $8|(26-10)$ . Afinal,  $26-10 = 16 = 2 \cdot 8 + 0$ .

**Teorema 1.4.26** (Subtração na Congruência). *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $a \equiv b \pmod{n}$  então:*

$$a - c \equiv b - c \pmod{n} \quad (1.29)$$

*Demonstração.* Se  $a \equiv b \pmod{n}$ , então, por definição,  $n|(a-b)$ .

$a-b = (a-c) - (b-c)$  e, portanto,  $n|(a-c) - (b-c)$ . Logo, por definição,  $a-c \equiv b-c \pmod{n}$   $\square$

Considere, por exemplo,  $a = 19, b = 3, c = 4$  e  $n = 8$ :

- (i)  $19 \equiv 3 \pmod{8}$  pois  $8|(19-3)$ . Afinal,  $19-3 = 16 = 2 \cdot 8 + 0$ .
- (ii)  $19-4 \equiv 3-4 \pmod{8}$ . Ou seja  $15 \equiv -1 \pmod{8}$  pois  $8|(15-(-1))$ . Afinal,  $15-(-1) = 16 = 2 \cdot 8 + 0$ .

**Teorema 1.4.27** (Multiplicação na Congruência). *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $a \equiv b \pmod{n}$  então:*

$$ac \equiv bc \pmod{n} \quad (1.30)$$

*Demonstração.* Se  $a \equiv b \pmod{n}$ , então, por definição,  $n|(a-b)$ .

Mas  $ac-bc = c(a-b)$  e, se  $n|(a-b)$  então  $n|c(a-b)$ . Logo, por definição,  $ac \equiv bc \pmod{n}$   $\square$

Considere, por exemplo,  $a = 19, b = 3, c = 2en = 8$ :

(i)  $19 \equiv 3 \pmod{8}$  pois  $8|(19 - 3)$ . Afinal,  $19 - 3 = 16 = 2 \cdot 8 + 0$ .

(ii)  $19 \cdot 2 \equiv 3 \cdot 2 \pmod{8}$ . Ou seja  $38 \equiv 6 \pmod{8}$  pois  $8|(38 - 6)$ . Afinal,  $38 - 6 = 32 = 4 \cdot 8 + 0$ .

**Teorema 1.4.28** (Exponenciação na Congruência). *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $a \equiv b \pmod{n}$  então:*

$$a^c \equiv b^c \pmod{n} \quad (1.31)$$

**Teorema 1.4.29.** *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ ,  $c|n$  e  $a \equiv b \pmod{n}$  então:*

$$a^c \equiv b^c \pmod{c} \quad (1.32)$$

**Teorema 1.4.30** (Divisão na Congruência). *Se  $a, b, c \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $MDC(n, c) = 1$  então:*

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{n} \quad (1.33)$$

*Demonstração.* Se  $ac \equiv bc \pmod{n}$  então  $n|(ac - bc)$ . Portanto  $n|c(a - b)$ .

Se  $n|c(a - b)$  então  $\exists q \in \mathbb{Z}$  tal que  $c(a - b) = qn + 0$ .

Se  $c(a - b) = qn$  e  $MDC(n, c) = 1$ , então  $n|(a - b)$ . Logo, por definição,  $a \equiv b \pmod{n}$ .  $\square$

Considere, por exemplo,  $a = 19, b = 3, c = 5en = 8$ :

(i)  $19 \equiv 3 \pmod{8}$  pois  $8|(19 - 3)$ . Afinal,  $19 - 3 = 16 = 2 \cdot 8 + 0$ .

(ii)  $MDC(8, 5) = 1$ .

(iii)  $19 \cdot 5 \equiv 3 \cdot 5 \pmod{8}$ . Ou seja  $95 \equiv 15 \pmod{8}$  pois  $8|(95 - 15)$ . Afinal,  $95 - 15 = 80 = 10 \cdot 8 + 0$ .

Note o que acontece quando  $MDC(n, c) \neq 1$ :

(i)  $14 \equiv 8 \pmod{6}$  pois  $6|(14 - 8)$ . Afinal,  $14 - 8 = 6 = 1 \cdot 6 + 0$ .

(ii) Portanto:  $7 \cdot 2 \equiv 4 \cdot 2 \pmod{6}$ . Porém eu não posso cancelar o fator comum pois  $MDC(6, 4) = 2 \neq 1$ .

(iii)  $7 \not\equiv 4 \pmod{6}$  pois  $6 \nmid (7 - 4)$ . Afinal, não existe  $q$  inteiro tal que  $7 - 4 = 3 = q \cdot 6 + 0$  pois  $q = \frac{6}{3} = 0.5$ .

**Teorema 1.4.31.** *Se  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  e  $a \equiv b \pmod{n}$  então:*

$$MDC(a, n) = MDC(b, n) \quad (1.34)$$

Suponha que vc tenha dois inteiros de 32 bits  $a$  e  $b$  e queira obter  $ab \pmod{n}$  com  $n \ll a$  e  $n \ll b$ .

Fazer a conta diretamente irá causar um overflow pois  $ab$  pode ter até 64 bits de comprimento. Porém, podemos usar esta equação para resolver o problema:

$$ab \pmod{n} = [(a \pmod{n})(b \pmod{n})] \pmod{n} \quad (1.35)$$

Por exemplo, se  $a = 2^{30}$ ,  $b = 2^{31}$  e  $n = 12$  temos:

$$2^{30}2^{31} \pmod{12} = [(2^{30} \pmod{12})(2^{31} \pmod{12})] \pmod{12} \quad (1.36)$$

Logo:

$$2^{30}2^{31} \pmod{12} = [(2^{30} \pmod{12})(2^{31} \pmod{12})] \pmod{12} \quad (1.37)$$

Portanto:

$$2^{30}2^{31} \pmod{12} = (4 \cdot 8) \pmod{12} = 8 \quad (1.38)$$

### 1.4.11 Teorema de Fermat

**Teorema 1.4.32.** *Se  $a, b \in \mathbb{Z}$  e  $p$  é primo então:*

$$(a + b)^p = a^p + b^p \pmod{p} \quad (1.39)$$

*Demonstração.* Pela expansão do Binômio de Newton, temos:

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^{n-k} b^k \quad (1.40)$$

Notamos que  $\forall 0 < k < p$  temos:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \pmod{p} \quad (1.41)$$

pois há pelo menos um fator  $p$  no numerador que não pode ser cancelado com nada que apareça no denominador.

Ou seja, todos os termos  $\binom{p}{k} a^{n-k} b^k$  cancelam na operação MOD exceto o primeiro ( $a^p$ ) e o último ( $b^p$ ).  $\square$

**Teorema 1.4.33.** *Se  $a \in \mathbb{Z}$  e  $p$  é primo então:*

$$a^p \equiv a \pmod{p} \quad (1.42)$$

*Demonstração.* Por indução em  $p$ .

Se  $p = 2$  então  $a^2 \equiv a \pmod{2}$  o que equivale a  $2|(a^2 - a)$ . De fato, 2 divide  $a(a - 1)$  pois  $a - 1$  e  $a$  são inteiros consecutivos e, portanto, um deles é par.

Supondo que  $a^p \equiv a \pmod{p}$  para todos os primos até  $n$ . De acordo com o teorema 1.39 temos:  $(a + 1)^p = a^p + 1^p \pmod{p}$ .

Logo:  $(a + 1)^p = a^p + 1 \pmod{p}$ .

Pela hipótese indutiva,  $a^p \equiv a \pmod{p}$  temos:  $(a + 1)^p = a + 1 \pmod{p}$ .  $\square$

**Teorema 1.4.34** (Teorema de Fermat). *Se  $n \in \mathbb{N}^*$ ,  $p$  é primo e  $MDC(n, p) = 1$  então:*

$$n^{p-1} \equiv 1 \pmod{p} \quad (1.43)$$

**Teorema 1.4.35.** *Se  $p$  é primo e  $a \in \mathbb{Z}$  então:*

$$p|(a^p - a) \quad (1.44)$$

*Demonstração.* Pelo Teorema de Fermat,  $a^{p-1} \equiv 1 \pmod{p}$  que equivale a  $p|(a^{p-1} - 1)$ .

Mas se  $p|(a^{p-1} - 1)$  então  $p|a(a^{p-1} - 1)$  que equivale a  $p|(a^p - a)$ .  $\square$

### 1.4.12 Função Totiente de Euler (Função $\phi$ )

**Definição 1.4.24** (Função  $\phi$ ). *A função Totiente de Euler, denotada  $\phi(n)$ , é igual à quantidade de números naturais  $a \in \mathbb{N}^*$  tal que  $a < n$  e  $MDC(a, n) = 1$ .*

Exemplo: os naturais menores que 6 são  $\{1, 2, 3, 4, 5\}$ . Destes, apenas 1 e 5 são relativamente primos a 6 (isto é,  $MDC(6, 1) = 1$  e  $MDC(6, 5) = 1$ ). Portanto,  $\phi(6) = 1 + 5 = 6$ . Analogamente,  $\phi(0) = 0$ ,  $\phi(2) = 1$ ,  $\phi(5) = \phi(8) = 4$  e  $\phi(7) = \phi(9) = 6$ .

**Teorema 1.4.36.** *Se  $p$  é primo então:*

$$\phi(p) = p - 1 \quad (1.45)$$

*Demonstração.* Seja  $S = \{1, 2, \dots, p-2, p-1\}$  o conjunto dos naturais menores que  $p$ .

Dado  $a \in S$  temos que  $p \nmid a$  pois  $a < p$ .

Portanto, para todo  $a \in S$ , temos  $MDC(a, p) = 1$ . Portanto, pela definição de  $\phi$ , temos que contar todos os elementos de  $S$ .

Como  $|S| = p - 1$ , ou seja,  $S$  tem  $p - 1$  elementos, concluímos que  $\phi(p) = (p - 1)$ .  $\square$

**Teorema 1.4.37.** *Se  $p$  é primo,  $\alpha \in \mathbb{N}$  e  $n = p^\alpha$  então:*

$$\phi(p) = p^\alpha(1 - \frac{1}{p}) \quad (1.46)$$

*Demonstração.* Se  $n = p^\alpha$  então existem  $p^\alpha$  números naturais menores que  $n$ .

E o conjunto  $S$ , dos números menores que  $n$  e que têm divisores comuns com  $n$  é  $S = \{p, 2p, 3p, \dots, p^{\alpha-1}p\}$ . Este conjunto tem  $p^{\alpha-1}$  elementos.

Portanto, a quantidade de números naturais menores que  $n$  e que não têm divisores comuns com  $p^\alpha$  é dada por:

$$\phi(n) = \phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p}) \quad (1.47)$$

$\square$

**Teorema 1.4.38.** *Se  $n$  está fatorado em sua forma canônica<sup>4</sup>, então:*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m}) \quad (1.48)$$

*Demonstração.* A idéia é contar, de forma análoga ao que fizemos nas provas dos dois últimos teoremas, a quantidade de números  $a \in \mathbb{N}$  tais que:

(i)  $a < n$

(ii)  $MDC(a, n) = 1$

$p_1$  é um dos divisores de  $n$ . Então o conjunto dos naturais menores que  $n$  que têm divisores comuns com  $p_1$  é  $S_{p_1} = \{p_1, 2p_1, 3p_1, \dots, \frac{n}{p_1}p_1\}$  e  $|S_{p_1}| = \frac{n}{p_1}$ .

Portanto, o número de naturais menores que  $p_1$  que não têm divisor comum com  $p_1$  é dado por:

$$\phi_{p_1}(n) =$$

$$n - \frac{n}{p_1} = n(1 - \frac{1}{p_1}) \quad (1.49)$$

Usando raciocínio análogo para  $p_2$  temos:  $S_{p_2} = \{p_2, 2p_2, 3p_2, \dots, \frac{n}{p_2}p_2\}$  e  $|S_{p_2}| = \frac{n}{p_2}$ .

Portanto, o número de naturais menores que  $p_2$  que não têm divisor comum com  $p_2$  é dado por:

$$\phi_{p_2}(n) =$$

$$n - \frac{n}{p_2} = n(1 - \frac{1}{p_2}) \quad (1.50)$$

---

<sup>4</sup>Ver equação 1.4.19 na página 14.

Para encontrar a quantidade de números menores que  $n$  e que não sejam divisíveis nem por  $p_1$  nem por  $p_2$  não é suficiente somar  $\phi_{p_1}(n) + \phi_{p_2}(n)$  pois os múltiplos de  $p_1 p_2$  pertencem a  $S_{p_1}$  e  $S_{p_2}$  e, portanto, foram contados duas vezes. O conjunto dos inteiros que têm divisores comuns com  $p_1 p_2$  é  $S_{p_1 p_2} = \{p_1 p_2, 2p_1 p_2, 3p_1 p_2, \dots, \frac{n}{p_1 p_2} p_1 p_2\}$  e  $|S_{p_1 p_2}| = \frac{n}{p_1 p_2}$ . Portanto, o número de naturais menores que  $p_1 p_2$  que não têm divisor comum com  $p_1 p_2$  é dado por:

$$\phi_{p_1 p_2}(n) =$$

$$n - \frac{n}{p_1 p_2} = n(1 - \frac{1}{p_1 p_2}) \quad (1.51)$$

Portanto, o total de naturais menores que  $n$  que não têm divisores comuns com  $p_1, p_2$  e  $p_1 p_2$  é dado por  $n - n/p_1 + n/p_2 - n/(p_1 p_2)$ .

Mas  $n - n/p_1 = n(1 - \frac{1}{p_1})$  e  $n/p_2 - n/(p_1 p_2) = \frac{n}{p_2}(1 - \frac{1}{p_1 p_2})$ .

Portanto:  $n - n/p_1 + n/p_2 - n/(p_1 p_2) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$

Repetindo o raciocínio para todos os  $p_k$  com  $k$  de 1 a  $m$  iremos obter  $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_m})$ .  $\square$

Portanto, para calcular  $\phi(120)$  basta obter a fatoração canônica de 120:

$$120 = 2^3 \cdot 3 \cdot 5 \quad (1.52)$$

Logo:

$$\phi(120) = 120(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 32 \quad (1.53)$$

Logo, existem 32 co-primos menores que 120.

**Teorema 1.4.39.** Se  $a, b \in \mathbb{Z}$  e  $MDC(a, b) = 1$  então:

$$\phi(ab) = \phi(a)\phi(b) \quad (1.54)$$

**Proposição 1.4.5.** Se  $a \in \mathbb{Z}$  e  $a > 5$  então:

$$\phi(a) > \frac{a}{6 \ln \ln(a)} \quad (1.55)$$

### Teorema de Euler

**Teorema 1.4.40** (Teorema de Euler). Se  $m, n \in \mathbb{N}^*$  e  $MDC(m, n) = 1$  então:

$$m^{\phi(n)} \equiv 1 \pmod{n} \quad (1.56)$$

### 1.4.13 Quantidade de divisores (Função $\tau$ )

**Definição 1.4.25** (Função  $\tau$ ).  $\tau(n)$  é igual a quantidade divisores positivos de um inteiro  $n \geq 0$ .

Por exemplo: os divisores de 6 são  $\{-6, -3, -2, -1, 1, 2, 3, 6\}$ . Portanto, os divisores positivos de 6 são  $\{1, 2, 3, 6\}$  e  $\tau(6) = 4$ .

Considere, por exemplo,  $120 = 2^3 \cdot 3 \cdot 5$ . Portanto, um divisor de 120 é da forma  $m = 2^a 3^b 5^c$  com  $a \in A = \{0, 1, 2, 3\}$ ,  $b \in B = \{0, 1\}$  e  $c \in C = \{0, 1\}$ . Portanto, existem 16 divisores de 120 e  $\tau(120) = |A| \cdot |B| \cdot |C| = 4 \cdot 2 \cdot 2 = 16$ .

De modo geral, se um número  $n$  é fatorado canonicamente (veja a equação 1.4.19 na pág. 14) então:

$$\tau(n) = \prod_{k=1}^m (1 + \alpha_k) \quad (1.57)$$

#### 1.4.14 Soma dos divisores (Função $\sigma$ )

Definimos  $\sigma(n)$  a soma de todos os divisores positivos de um inteiro  $n \geq 0$ . Por exemplo: os divisores positivos de 6 são  $\{1, 2, 3, 6\}$  e  $\sigma(6) = 1 + 2 + 3 + 6 = 12$ .

**Lema 1.4.3.** Se  $n = ab$  com  $n, a, b \in \mathbb{N}^+$  e  $MDC(a, b) = 1$  então  $\sigma(n) = \sigma(a)\sigma(b)$

*Demonstração.* Sejam  $a_1, a_2, \dots, a_n$  os divisores de  $a$  e  $b_1, b_2, \dots, b_m$  os divisores de  $b$ . Portanto  $a = \prod_{k=1}^n a_k$  e  $b = \prod_{k=1}^m b_k$ .

Se  $n = ab$  então  $n = \prod_{k=1}^n a_k b \prod_{k=1}^m b_k$ .

Portanto, podemos listar os divisores de  $n$  da seguinte forma:

$$\begin{array}{ll} 1 & , \quad b_1, b_2, \dots, b_m \\ a_1 & , \quad a_1 b_1, a_1 b_2, \dots, a_1 b_m \\ \dots & \\ a_n & , \quad a_n b_1, a_n b_2, \dots, a_n b_m \end{array} \quad (1.58)$$

Se  $MDC(a, b) = 1$  então 1 é o único fator comum de  $a$  e  $b$ . Portanto, na lista de divisores acima, quando  $a_i b_j = a_k b_l$  temos  $a_i = a_k$  e  $b_j = b_l$ .

Se somarmos os divisores em cada linha, vamos obter:

$$\begin{array}{ll} 1\sigma(b) & = 1 + b_1 + b_2 + \dots + b_m \\ a_1\sigma(b) & = a_1 + a_1 b_1 + a_1 b_2 + \dots + a_1 b_m \\ \dots & \\ a_n\sigma(b) & = a_n + a_n b_1 + a_n b_2 + \dots + a_n b_m \end{array} \quad (1.59)$$

Somando todas as linhas, temos:

$$(1 + a_1 + \dots + a_n)\sigma(b) = \sigma(n) \quad (1.60)$$

Portanto:

$$\sigma(a)\sigma(b) = \sigma(n) \quad (1.61)$$

□

**Lema 1.4.4.** Se  $p$  é primo e  $n \in \mathbb{N}^+$  então  $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$

*Demonstração.* Se  $p$  é primo, então os divisores de  $p^n$  são  $1, p, p^2, \dots, p^n$ .

Portanto,  $\sigma(p^n) = 1 + p + p^2 + \dots + p^n$ .

Concluindo a soma da P.G., temos:  $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$

□

**Teorema 1.4.41.** Se  $n \in \mathbb{N}$  está fatorado na forma canônica (ver equação 1.4.19 na página 14) então

$$\sigma(n) = \left( \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left( \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \dots \left( \frac{p_n^{\alpha_n+1} - 1}{p_n - 1} \right) \quad (1.62)$$

*Demonstração.* Seja  $n = \prod_{k=1}^m p_i^{\alpha_i}$ .

Prova por indução em  $m$ .

Se  $m = 1$  então  $n = p_1^{\alpha_1}$ . De acordo com o lema 1.4.4, temos:

$$\sigma(p_1^{\alpha_1}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \quad (1.63)$$

Portanto, a eq. 1.62 vale para  $m = 1$ .

Supondo a eq. 1.62 válida para  $1 \leq m \leq k$ , vamos considerar o caso para  $m = k + 1$ , ou seja,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k+1}^{\alpha_{k+1}}$ .

Fazemos  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  e  $b = p_{k+1}^{\alpha_{k+1}}$ .

Pela Hipótese Indutiva, temos:

$$\sigma(a) = \left( \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left( \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left( \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right) \quad (1.64)$$

Pelo Lema 1.4.4 temos:

$$\sigma(b) = \left( \frac{p_{k+1}^{\alpha_{k+1}+1} - 1}{p_{k+1} - 1} \right) \quad (1.65)$$

Como os  $p_i$  são distintos para  $1 \leq i \leq k+1$  temos que  $MDC(a, b) = 1$ . Portanto, podemos usar o Lema 1.4.3 ( $\sigma(n) = \sigma(a)\sigma(b)$ ) para mostrar que:

$$\sigma(n) = \left( \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left( \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left( \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right) \left( \frac{p_{k+1}^{\alpha_{k+1}+1} - 1}{p_{k+1} - 1} \right) \quad (1.66)$$

Portanto, supondo válida para  $1 \leq m \leq k$ , mostramos que a eq. 1.62 vale para  $m = k + 1$ .

Logo, pelo Princípio da Indução Finita, a eq. 1.62 vale para quaisquer  $m > 1$ .  $\square$

### 1.4.15 Congruência Linear

Suponha um relógio de ponteiros marcando exatamente meio-dia. O mecanismo do relógio tem um defeito de modo que o ponteiro de horas só avança de 5 em 5 horas. Quantos movimentos tenho que fazer para que o ponteiro mostre 1h?

Um modo de resolver o problema é acompanhar a posição do ponteiro a cada movimento: 12h, 5h, 10h, 3h, 8h e 1h. Portanto, bastam 5 movimentos.

Outro modo é resolver esta equação:

$$ax \equiv b \pmod{n} \quad (1.67)$$

considerando  $a = 5, b = 1$  e  $n = 12$  e  $x \in \mathbb{Z}$ .

A equação 1.67 nem sempre tem solução. Por exemplo, se  $a = 2, b = 1$  e  $n = 4$ . Em particular, quando  $b = 1$ , a solução da equação é denominado *inverso multiplicativo* de  $a$  pois:

$$aa^{-1} \equiv 1 \pmod{n} \quad (1.68)$$

**Teorema 1.4.42.** Se  $n > 1$  e  $MDC(a, n) = 1$  então  $ax \equiv b \pmod{n}$  tem solução única ou não tem solução.

*Demonstração.* Seja a equação linear  $sa + tn = 1$  para  $s, a \in \mathbb{Z}$

Multiplicando todos os termos por  $b$ , temos:  $sba + tbn = b$  que é equivalente a:

$$sba = b \pmod{n} \quad (1.69)$$

cuja solução é  $x = sb$ .

Sejam  $x_1$  e  $x_2$  possíveis soluções. Então:  $ax_1 = b \pmod{n}$  e  $ax_2 = b \pmod{n}$ .

Portanto  $ax_1 = ax_2 \pmod{n}$ .

Se  $MDC(a, n) = 1$  temos  $x_1 = x_2 \pmod{n}$  e, portanto, a solução é única.  $\square$

**Teorema 1.4.43.** Se  $ax \equiv b \pmod{n}$ , então  $\exists q \in \mathbb{Z}$  tal que  $ax = qn + b$ . Portanto, um divisor comum de  $a$  e  $n$  é também divisor de  $b$ .

**Teorema 1.4.44.** Se  $n > 1$ ,  $\mathcal{L} \in \mathbb{N}, x, y \in \mathbb{Z}$  e  $MDC(a, n) = 1$  então:

$$ax \equiv \mathcal{L} \pmod{n} \Leftrightarrow ax - by = \mathcal{L} \quad (1.70)$$

**Teorema 1.4.45.** Se  $n > 1$ ,  $\mathcal{L} \in \mathbb{N}, x, y \in \mathbb{Z}$ ,  $MDC(a, n) = d > 1$  e  $d \nmid \mathcal{L}$  então não há soluções inteiras para:

$$ax \equiv \mathcal{L} \pmod{n} \quad (1.71)$$

### 1.4.16 Algoritmo de Euclides Estendido

Para encontrar o de dois números inteiros, usando o Algoritmo de Euclides:

- (i) Divide-se o maior número pelo menor.
- (ii) Se o resto é zero, o MDC é igual ao divisor.
- (iii) Se o resto é diferente de zero, substituímos o maior número pelo resto e voltamos ao passo (i).

Vamos acompanhar estes cálculos para o MDC de 120 e 23:

$$(i) \quad 120 = 23 \cdot 5 + 5$$

$$(ii) \quad 23 = 5 \cdot 4 + 3$$

$$(iii) \quad 5 = 3 \cdot 1 + 2$$

$$(iv) \quad 3 = 2 \cdot 1 + 1$$

$$(v) \quad 2 = 2 \cdot 1 + 0$$

O Algoritmo de Euclides Estendido trabalha de forma semelhante, utilizando os restos obtidos no Algoritmo de Euclides para definir as soluções inteiras da equação  $120m + 23n = MDC(120, 23) = 1$  para  $m, n, k \in \mathbb{Z}$ .

Considerando o resto 5 (ver item (i) acima):

$$5 = 1 \cdot 120 - 5 \cdot 23 \quad (1.72)$$

Considerando o resto 3 (ver item (ii) acima):

$$3 = 1 \cdot 23 - 4 \cdot 5 = \quad (1.73)$$

Substituindo  $5 = 1 \cdot 120 - 5 \cdot 23$ , obtemos:

$$3 = 1 \cdot 23 - 4 \cdot (1 \cdot 120 - 5 \cdot 23) = -4 \cdot 120 + 21 \cdot 23 \quad (1.74)$$

Considerando o resto 2 (ver item (iii) acima):

$$2 = 1 \cdot 5 - 1 \cdot 3 \quad (1.75)$$

Substituindo  $5 = 1 \cdot 120 - 5 \cdot 23$  e  $3 = -4 \cdot 120 + 21 \cdot 23$ , obtemos:

$$2 = 1 \cdot (1 \cdot 120 - 5 \cdot 23) - 1 \cdot (-4 \cdot 120 + 21 \cdot 23) = -5 \cdot 120 + 26 \cdot 23 \quad (1.76)$$



Considerando o resto 1 (ver item (iv) acima):

$$1 = 1 \cdot 3 - 1 \cdot 2 \quad (1.77)$$

Substituindo  $3 = -4 \cdot 120 + 21 \cdot 23$  e  $2 = -5 \cdot 120 - 26 \cdot 23$ , obtemos:

$$1 = 1 \cdot (-4 \cdot 120 + 21 \cdot 23) - 1 \cdot (-5 \cdot 120 - 26 \cdot 23) = -9 \cdot 120 + 47 \cdot 23 \quad (1.78)$$

Portanto, o algoritmo encontra  $m = -9$  e  $n = 47$ .

#### 1.4.17 Quantidade de números primos menores que $x$ (Função $\pi$ )

**Definição 1.4.26** (Função  $\pi$ ). *Se  $x \in \mathbb{R}^+$  então  $\pi(x)$  denota a quantidade de números primos  $p$  menores ou iguais a  $x$ .*

Exemplo:  $\pi(10) = 4$  pois há apenas 4 primos (2, 3, 5 e 7) menores que 10.

Note que a função  $\pi(x)$  tem valor constante quando  $x$  varia entre dois primos consecutivos.  $\pi(3) = 2, \pi(3.5) = 2, \pi(\pi) = 2, \pi(4) = 2, \pi(5) = 3$ .

## 1.5 Identidade Polinomial

Considere dois polinômios:

$$P(x) = (x-3)(x-5)(x+1)(x-1)(x+3) \quad (1.79)$$

$$Q(x) = x^5 - 5x^4 - 9x^3 + 45x^2 + 9x - 45 \quad (1.80)$$

O polinômio  $P(x)$  é formado pelo produto de vários monômios e o polinômio  $Q(x)$  está em sua forma “canônica”, isto é,  $Q(x) = \sum_{k=0}^n a_k x^k$  com  $a_n \neq 0$ .

Uma forma de saber se os polinômios são idênticos (isto é, se retornam o mesmo resultado para qualquer valor de  $x$ ) é converter ambos os polinômios em sua forma canônica e depois comparar os termos  $a_k$  obtidos.

Se  $P(x) = \prod_{k=1}^n (x - a_k)$  e  $Q(x) = \sum_{k=0}^n a_k x^k$ , então podemos multiplicar os monômios de  $P$  em  $\Theta(n^2)$  e comparar seus coeficientes com os de  $Q(x)$  em  $\Theta(n)$ . Portanto, o tempo total é  $\Theta(n^2)$ .

Podemos usar um algoritmo probabilístico e comparar os polinômios em tempo  $\Theta(n)$ , obtendo uma certa probabilidade do algoritmo dar um “falso positivo” (isto é, o algoritmo diz que os polinômios são equivalente quando na verdade não o são).

Seja  $n$  o maior expoente de  $x$  nos polinômios  $P(x)$  e  $Q(x)$ . Portanto, se definirmos  $H(x) = P(x) - Q(x)$  sabemos que  $H(x)$  tem grau menor ou igual a  $n$ . Portanto  $H(x)$  tem no máximo  $n$  raízes reais.

Se  $P(x) \equiv Q(x)$  então  $H(x) = 0$  para todo  $x$ . Se  $P(x) \not\equiv Q(x)$  então  $H(x) = 0$  para no máximo  $n$  valores de  $x$  (estes valores são as  $n$  raízes reais de  $H$ ).

Seja  $r$  um número inteiro aleatoriamente escolhido no intervalo real  $[1 \dots 100n]$ . É possível calcular  $H(r)$  em tempo  $\Theta(n)$ . Se  $H(r) \neq 0$  podemos afirmar com certeza que  $P(x) \not\equiv Q(x)$ . Porém, se  $H(r) = 0$  e afirmarmos que  $P(x) \equiv Q(x)$ , qual a probabilidade desta afirmação ser falsa?

Se a afirmação for falsa, isto significa que, apesar de termos  $H(x) \neq 0$  para uma infinidade de valores de  $x$ , o valor sorteado para  $r$  foi igual a uma das  $n$  raízes de  $H(x)$ . Qual a probabilidade disso ocorrer?

No intervalo  $[1 \dots 100n]$  temos  $100n$  números inteiros e  $n$  possíveis raízes de  $H(x)$ . Portanto, a probabilidade de termos escolhido o valor  $r$  como sendo uma das  $n$  raízes de  $H(x)$  é dada por  $q \leq \frac{n}{100n} = \frac{1}{100}$ .

A probabilidade é dada por  $q \leq \frac{1}{100}$  e não  $q = \frac{1}{100}$  porque temos “no máximo”  $n$  raízes reais distintas.

Podemos reduzir a probabilidade de erro realizando vários sorteios. A probabilidade de  $r$  ser sorteado como raiz de  $H(x)$  em  $k$  sorteios é  $q^k = \left(\frac{1}{100}\right)^k$ .

Vale a pena realizar vários sorteios pois cada sorteio ocorre em tempo  $\Theta(1)$  e o cálculo de  $H(x)$  em  $\Theta(n)$  enquanto que a avaliação completa de  $H(x)$  ocorre em  $\Theta(n^2)$ .

Outra forma de reduzir a probabilidade de erro é ampliar o intervalo no qual o sorteio é realizado. Por exemplo, se sortearmos  $r$  no intervalo  $[1 \dots 1000d]$  a probabilidade de que  $r$  seja uma raiz de  $H(x)$  é  $q = \frac{1}{1000}$ .

# Referências Bibliográficas

- [1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. The MIT Press, Cambridge, Massachusetts, 2001.
- [2] Donald E. Knuth. *Textbook examples of recursion*, pages 207–229. Artificial Intelligence and Mathematical Theory of Computation: Papers in Honor of John McCarthy. Academic Press, New York, v. lifschitz edition, 1991. ISBN=0124500102.
- [3] Zohar Manna and John McCarthy. Properties of programs and partial function logic. *Machine Intelligence*, 5:27–37, 1970.