

### *CAPÍTULO III*

## **METAMATEMÁTICA**

## SECÇÃO 1

### FUNÇÕES E RELAÇÕES ARITMÉTICAS

#### **Definição 1.**      [ *Relação Aritmética* ]

*Uma relação  $R$  cujos argumentos são números naturais diz-se que é uma relação aritmética.*

#### **Definição 2.**      [ *Função Aritmética* ]

*Diz-se que uma função  $f$  cujos argumentos são números naturais e cujos valores são números naturais é uma função aritmética.*

#### **Exemplo 1.:**

A função

$$x \mid y$$

é uma função aritmética, pela Def. 2.

#### **Exemplo 2.:**

A fórmula

$$(x + y) < z$$

determina uma relação ternária entre os argumentos  $x$ ,  $y$  e  $z$ .

Se  $x$ ,  $y$  e  $z$  são números naturais, então a fórmula

$$R(x, y, z)$$

denota uma relação aritmética, pela Def. 1.

Estas funções e relações introduzidas pelas Definições 1 e 2 não são objectos de uma teoria formal particular. Mas uma Teoria Formal para a Aritmética sem estas funções e relações seria inútil. Assim é-se colocado perante o problema de saber como transportar estes objectos para uma Teoria Formal, em particular para  $Z$ .

Neste capítulo estudamos este problema sob o ponto de vista do conceito da sua formulação na sintaxe de  $Z$ .

## SECÇÃO 2

### A EXPRESSÃO DE RELAÇÕES ARITMÉTICAS

Nesta secção estudaremos relações simples e relações compostas por meio de conectivas proposicionais.

Aos termos

$$0, f_1^1(0), \dots$$

que representam na interpretação  $\mathbb{N}$  os números naturais chamámos numerais e têm a abreviatura já introduzida

$$0, \bar{1}, \dots$$

Vamos agora fazer uso dessa notação para variáveis, de modo a que  $\bar{x}$  designe o numeral correspondente, *i.e.*, 0 com  $x$  ocorrências de  $f_1^1$ .

Em particular

$$\bar{x} - 1$$

$\bar{x}$  designa o numeral com  $x - 1$  ocorrências de  $f_1^1$ .

**Definição 1.** [ *Relação Numeralmente Expressível em Z* ]

*Uma relação aritmética*

$$R(x_1, \dots, x_n)$$

*é numeralmente exprimível em  $Z$  se e somente se existe  
uma fórmula bem formada de  $Z$*

$$\alpha (x_1, \dots, x_n)$$

*com  $n$  variáveis livres e tal que  
para qualquer  $n$ -tuplo de números naturais*

$$x_1, \dots, x_n$$

*as duas seguintes condições são satisfeitas:*

1) *Se*

$$R (x_1, \dots, x_n)$$

*é verdadeira, então*

$$\vdash \alpha (\overline{x_1}, \dots, \overline{x_n}).$$

2) *Se*

$$R (x_1, \dots, x_n)$$

*é falsa, então*

$$\vdash \neg \alpha (\overline{x_1}, \dots, \overline{x_n}).$$

O uso legítimo deste conceito depende da existência de um processo de decisão para a relação

$$R (x_1, \dots, x_n),$$

de modo a que para qualquer  $n$ -tuplo  $x_1, \dots, x_n$

$$R (x_1, \dots, x_n) \vee \neg R (x_1, \dots, x_n)$$

e por isso em  $Z$

$$\vdash \alpha (\overline{x_1}, \dots, \overline{x_n}) \text{ ou } \vdash \neg \alpha (\overline{x_1}, \dots, \overline{x_n}).$$

Diz-se então que

$$\alpha (\overline{x_1}, \dots, \overline{x_n})$$

é decidível ou numeralmente decidível para qualquer  $n$ -tuplo

$$x_1, \dots, x_n .$$

A fórmula

$$\neg \alpha (\overline{x_1}, \dots, \overline{x_n})$$

exprime numeralmente a relação

$$\neg R (x_1, \dots, x_n) .$$

**Exemplo 1.:**      [ *A relação de Igualdade é Numeralmente Exprimível em Z* ]

Seja

$$R (x_1, x_2)$$

a relação binária que exprime a igualdade entre os argumentos  $x_1$  e  $x_2$ .

A fórmula

$$\alpha (x, y)$$

de Z é agora a fórmula

$$x = y ,$$

a qual é uma fórmula bem formada de Z.

Resta-nos determinar se a fórmula

$$\alpha (x, y)$$

satisfaz as condições 1) e 2) .

[Caso 1.]

Se

$$x_1 = x_2$$

então  $\overline{x_1}$  é o mesmo termo que  $\overline{x_2}$ .

Mas usando o Teorema de Z

$$\vdash a = a$$

tem-se imediatamente

$$\vdash \overline{x_1} = \overline{x_2}.$$

[Caso 2.]

Se

$$x_1 \neq x_2$$

então pela Proposição

$$(m \neq n) \rightarrow (\overline{m} \neq \overline{n})$$

tem-se imediatamente

$$\vdash \overline{x_1} \neq \overline{x_2}.$$

Mas pela Definição de “ $\neq$ ”, essa fórmula é equivalente a

$$\vdash \neg (\overline{x_1} = \overline{x_2}).$$

**Exemplo 2.:** [ *A relação  $<$  é Numeralmente Expressível em Z* ]

Seja

$$R(k_1, k_2)$$

a relação binária que exprime o facto de  $k_2$  ser maior do que  $k_1$ .

A fórmula

$$\alpha(x, y)$$

de  $Z$  é agora a fórmula

$$x < y$$

a qual é uma fórmula bem formada de  $Z$ .

Resta-nos determinar se a fórmula

$$\alpha(x, y)$$

satisfaz as condições 1) e 2).

[ **Caso 1.:**  $(k_1 < k_2)$  ]

1.  $(\exists n) (n \neq 0) (k_2 = k_1 + n)$
2.  $\vdash \overline{k_2} = \overline{k_1} + n$
3.  $n \neq 0 \rightarrow \overline{n} \neq 0$
4.  $(\exists x) (x \neq 0) (\overline{k_2} = \overline{k_1} + x)$
5.  $\vdash \overline{k_1} < \overline{k_2}$

[ **Caso 2.:**  $\neg(k_1 < k_2)$  ]

1.  $\neg(k_1 < k_2) \rightarrow [(k_2 < k_1) \vee (k_2 = k_1)]$
2.  $k_2 < k_1 \rightarrow \overline{k_2} < \overline{k_1}$
3.  $k_2 = k_1 \rightarrow \overline{k_2} = \overline{k_1}$
4.  $\overline{k_2} \leq \overline{k_1}$
5.  $\vdash \neg(\overline{k_1} < \overline{k_2})$

**Exemplo 3.:**

A relação

$$x + y = z$$

é exprimível em  $Z$ .

Seja

$$R(x_1, x_2, x_3)$$

a relação que exprime

$$x_1 + x_2 = x_3.$$

Se

$$x + y = z$$

então a fórmula

$$\alpha(\overline{x_1}, \overline{x_2}, \overline{x_3})$$

é verdadeira e

$$\vdash \alpha(\overline{x_1}, \overline{x_2}, \overline{x_3}).$$

Se

$$\neg(x + y = z)$$

então a fórmula

$$\alpha(\overline{x_1}, \overline{x_2}, \overline{x_3})$$

é falsa e

$$\vdash \neg \alpha(\overline{x_1}, \overline{x_2}, \overline{x_3}).$$

**Proposição 1.**      [ *Negação* ]

*Se  $R$  é numeralmente exprimível em  $Z$   
então a negação de  $R$  é numeralmente exprimível em  $Z$ .*

Dem.:

1.  $R$  é numeralmente exprimível em  $Z$  ou pela fórmula  $\alpha(\overline{k_1}, \dots, \overline{k_n})$  ou pela fórmula  $\neg \alpha(\overline{k_1}, \dots, \overline{k_n})$ .
1. Se  $\neg R$  é verdadeira então  $R$  é falsa e logo  
 $\vdash \neg \alpha(\overline{k_1}, \dots, \overline{k_n})$ .
3. Se  $\neg R$  é falsa então  $R$  é verdadeira e logo  
 $\vdash \alpha(\overline{k_1}, \dots, \overline{k_n})$ .

**Proposição 2.**      [ *Conjunção* ]

*Se  $R$  é numeralmente exprimível em  $Z$   
e  $S$  é numeralmente exprimível em  $Z$  então  
 $R \wedge S$   
é numeralmente exprimível em  $Z$ .*

Dem.:

1. Se  $R$  e  $S$  são numeralmente exprimíveis em  $Z$ , então tem-se os pares de fórmulas  
 $\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}), \vdash \neg \alpha(\overline{k_1}, \dots, \overline{k_n})$  para  $R$ ;  
e  $\vdash \beta(\overline{k_1}, \dots, \overline{k_n}), \vdash \neg \beta(\overline{k_1}, \dots, \overline{k_n})$  para  $S$ .
2. Se  $R \wedge S$  é verdadeira então tem-se a fórmula

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}) \wedge \beta(\overline{k_1}, \dots, \overline{k_n}).$$

3. Se  $R \wedge S$  é falsa então tem-se uma das fórmulas

$$\vdash \neg \alpha(\overline{k_1}, \dots, \overline{k_n}) \wedge \neg \beta(\overline{k_1}, \dots, \overline{k_n});$$

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}) \wedge \neg \beta(\overline{k_1}, \dots, \overline{k_n});$$

$$\vdash \neg \alpha(\overline{k_1}, \dots, \overline{k_n}) \wedge \beta(\overline{k_1}, \dots, \overline{k_n}).$$

**Proposição 3.**      [ *Disjunção* ]

*Se R é numeralmente exprimível em Z  
e S é numeralmente exprimível em Z então*

$$R \vee S$$

*é numeralmente exprimível em Z.*

Dem.:

1. Se  $R$  é numeralmente exprimível então  $\neg R$  é numeralmente exprimível e logo  $\neg S$  é numeralmente exprimível, pela Prop. 1.

2. Então a conjunção

$$\neg R \wedge S$$

é numeralmente exprimível pela Prop. 2.

3. Mas  $\neg R \wedge S \leftrightarrow R \vee S$ .

### SECÇÃO 3

#### A REPRESENTAÇÃO DE FUNÇÕES ARITMÉTICAS

Seja  $f(x_1, \dots, x_n)$  uma função aritmética e seja

$$F(x_1, \dots, x_n, x_{n+1})$$

o predicado

$$f(x_1, \dots, x_n) = x_{n+1}.$$

Diz-se então que

$$F(x_1, \dots, x_n, x_{n+1})$$

é o predicado representativo da função

$$f(x_1, \dots, x_n).$$

A condição necessária e suficiente para  $F(x_1, \dots, x_n, x_{n+1})$  ser o predicado representativo da função  $f(x_1, \dots, x_n)$  é a de que para qualquer  $n$ -tuplo

$$x_1, \dots, x_n$$

exista um único  $x_{n+1}$  tal que  $F(x_1, \dots, x_n, x_{n+1})$ .

Se essa univocidade é garantida então a função  $f(x_1, \dots, x_n)$  pode ser definida *descritivamente* a partir do predicado  $F(x_1, \dots, x_n, x_{n+1})$  como o  $x_{n+1}$  tal que  $F(x_1, \dots, x_n, x_{n+1})$ .

**Definição 1.**      [ *Função Numeralmente Representável* ]

Seja

$$f(x_1, \dots, x_n)$$

uma função aritmética.

Diz-se que  $f(x_1, \dots, x_n)$  é numeralmente representável em  $Z$

se e somente se

existe uma fórmula bem formada

$$\alpha(x_1, \dots, x_n, x_{n+1})$$

de  $Z$  com

$$x_1, \dots, x_n, x_{n+1}$$

variáveis livres tal que, para qualquer

$$\langle k_1, \dots, k_{n+1} \rangle$$

de números naturais, as duas condições seguintes são satisfeitas:

1) Se

$$f(k_1, \dots, k_n) = k_{n+1}$$

então

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}});$$

$$2) \vdash (\exists^1 x_{n+1}) \alpha(\overline{k_1}, \dots, \overline{k_n}, x_{n+1}).$$

Diz-se então que a fórmula

$$F(x_1, \dots, x_n, x_{n+1})$$

representa numeralmente a função

$$f(x_1, \dots, x_n).$$

Tal como foi observado a respeito da expressão numeral, o conceito de representação numeral de um função só tem sentido construtivista se existir um algoritmo para calcular  $f(x_1, \dots, x_n)$ , de modo a que  $x_{n+1}$  pode ser sempre determinado para qualquer  $x_1, \dots, x_n$ .

É óbvio que se  $f(x_1, \dots, x_n)$  é numeralmente representável por

$$F(x_1, \dots, x_n, x_{n+1})$$

essa fórmula representa numeralmente o predicado representativo de  $f$ ,  $F(x_1, \dots, x_n, x_{n+1})$ .

Assim, se

$$f(x_1, \dots, x_n) \neq x_{n+1} \rightarrow \neg F(\overline{x_1}, \dots, \overline{x_n}, \overline{x_{n+1}}).$$

## **Definição 2.** [ *Representação- $\Phi$* ]

*Seja*

$$f(x_1, \dots, x_n)$$

*uma função aritmética.*

*Diz-se que  $f(x_1, \dots, x_n)$  é  $\Phi$ -representável em  $Z$*

*se e somente se existe uma fórmula bem formada*

$$\alpha(x_1, \dots, x_n, x_{n+1})$$

*de  $Z$  com*

$$x_1, \dots, x_{n+1}$$

*variáveis livres tal que, para quaisquer*

$$\langle k_1, \dots, k_{n+1} \rangle$$

*números naturais, as duas condições seguintes são satisfeitas:*

1) *Se*

$$f(k_1, \dots, k_n) = k_{n+1}$$

*então*

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$$

2)  $\vdash (\exists^1 x_{n+1}) \alpha(x_1, \dots, x_n, x_{n+1})$ .

**Proposição 1.**      [ *Representação- $\varphi$  e Representação* ]

*Qualquer função aritmética  $\varphi$ -representável  
é também numeralmente representável.*

Dem.:

A cláusula 2) da Definição 2 implica a cláusula 2) da Definição 1 por Introdução e Eliminação de  $\forall$ .

**Definição 3.**      [ *Função Zero* ]

*A função aritmética Z, tal que para qualquer  
número natural x  
se tem  
 $Z(x) = 0$ ,  
chama-se função zero.*

**Proposição 2.**      [ *A Função Zero é  $\varphi$ -Representável em Z* ]

*A função zero é  $\Phi$ -representável em Z.*

Dem.:

Como fórmula bem formada de Z podemos adoptar a fórmula

$$(x = x) \wedge (y = 0) .$$

i) Para qualquer  $k_1$ ,

$$Z(k_1) = k_2$$

implica que

$$k_2 = 0 .$$

A fórmula resultante é

$$\vdash ( \overline{k_1} = \overline{k_1} ) \wedge (0 = 0) .$$

Logo, a condição 1) é satisfeita.

ii) A univocidade do zero garante a condição 2). A fórmula resultante é

$$(\exists^1 y) [ (x = x) \wedge (y = 0) ] .$$

**Definição 4.**      [ *Função Sucessor* ]

*A função aritmética N, tal que para qualquer número natural x*

*se tem*

$$N(x) = x + 1 ,$$

*chama-se função sucessor.*

**Proposição 3.** [ *A Função Sucessor é  $\varphi$ -Representável em Z* ]

*A função sucessor é  $\varphi$ -representável em Z.*

Dem.:

Como fórmula bem formada de Z podemos escolher a fórmula

$$y = N(x) .$$

i) Para qualquer  $k_1$ ,

$$N(k_1) = k_2$$

implica que

$$k_2 = k_1 + 1 .$$

Logo,

$$\overline{k_2} = N(\overline{k_1}) .$$

Então,

$$\vdash \overline{k_2} = N(\overline{k_1}) .$$

Logo a condição 1) da Def. 2 é satisfeita.

ii) O Axioma Z4 assegura que a condição 2) é satisfeita e a fórmula resultante é

$$(\exists^1 y) [ y = N(x) ] .$$

**Definição 5.** [ *Função Identidade* ]

*A função aritmética U tal que para qualquer  
n-tuplo de números naturais*

$$x_1, \dots, x_n$$

se tem

$$U(x_1, \dots, x_n) = x_i$$

chama-se função identidade.

O número

$$U(x_1, \dots, x_n) = x_i$$

representa-se pela notação

$$U_i^n(x_1, \dots, x_n) = x_i.$$

**Exemplo 1.:**

A função

$$U_1^2(3, 1) = 3$$

é uma função identidade.

**Exemplo 2.:**

A função

$$U_2^2(0, 5) = 5$$

é uma função identidade.

**Proposição 4.** [ A Função Identidade é  $\varphi$ -Representável em  $\mathbf{Z}$  ]

*A função identidade é  $\varphi$ -representável em  $\mathbf{Z}$ .*

Dem.:

Para fórmula bem formada de Z escolha-se a fórmula

$$(x_1 = x_1) \wedge (x_2 = x_2) \wedge \dots \wedge (x_n = x_n) \wedge (x_{n+1} = x_i).$$

É fácil verificar que as duas condições da definição 2 são satisfeitas pela função  $U$ .

i) Se

$$U_i^n(k_1, \dots, k_n) = k_{n+1}$$

então

$$k_{n+1} = k_i .$$

Logo,

$$\overline{k_{n+1}} = \overline{k_i} .$$

E assim,

$$\begin{aligned} \vdash & (\overline{k_1} = \overline{k_1}) \wedge (\overline{k_2} = \overline{k_2}) \wedge \dots \\ & \dots \wedge (\overline{k_n} = \overline{k_n}) \wedge (\overline{k_{n+1}} = \overline{k_i}). \end{aligned}$$

ii)

$$\begin{aligned} \vdash & (\exists^1 x_{n+1}) [(x_1 = x_1) \wedge (x_2 = x_2) \wedge \dots \\ & \dots \wedge (x_n = x_n) \wedge (x_{n+1} = x_i) ]. \end{aligned}$$

**Definição 6.** [ *Substituição* ]

Considere-se a seguinte sucessão de funções aritméticas:

$$h_1(x_1, \dots, x_n)$$

·  
·  
·

$$h_m(x_1, \dots, x_n)$$

e ainda a função aritmética

$$g(x_1, \dots, x_m).$$

Por hipótese, considere-se que as funções

$$g(x_1, \dots, x_m)$$

$$h_1(x_1, \dots, x_n)$$

⋮

$$h_m(x_1, \dots, x_n)$$

são  $\varphi$ -representáveis em  $\mathbb{Z}$  pelas fórmulas bem formadas seguintes:

i)  $g(x_1, \dots, x_m)$  pela fórmula bem formada

$$\beta(x_1, \dots, x_m, x_{m+1})$$

ii) A sucessão de funções

$$h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)$$

pelas fórmulas bem formadas

$$\alpha_1(x_1, \dots, x_{n+1}), \dots, \alpha_m(x_1, \dots, x_{n+1}).$$

Defina-se agora uma nova função aritmética  $f$

por meio da equação seguinte:

$$f(x_1, \dots, x_n) = g[h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)].$$

Então diz-se que a função  $f$

é obtida a partir da função  $g$  e da sucessão de funções

$$h_1, \dots, h_m$$

por substituição.

Uma função  $f$  definida por uma aplicação da Definição 6 representa--se por vezes pela notação

$$\Sigma_m^n (g, h_1, \dots, h_m) .$$

**Proposição 5.** [ *O Processo de Substituição Conserva a Propriedade de Ser  $\varphi$ -Representável* ]

*Uma função aritmética*

$$f(x_1, \dots, x_n)$$

*obtida de*

$$g(x_1, \dots, x_m)$$

*e da sucessão de funções*

$$h_1, \dots, h_m$$

*por substituição é  $\varphi$ -representável em Z, se*

$$g(x_1, \dots, x_m) \text{ e } h_1, \dots, h_m$$

*o são.*

Dem.:

Escolheremos como a fórmula bem formada de Z

$$\alpha(x_1, \dots, x_{n+1})$$

a expressão seguinte:

$$(\exists y_1), \dots, (\exists y_m) [ \alpha_1(x_1, \dots, x_n, y_1) \wedge \dots \\ \dots \wedge \alpha_m(x_1, \dots, x_n, y_m) \wedge \beta(y_1, \dots, y_m, x_{n+1}) ] .$$

Dem.: (Parte I.: **Condição 1**)

$$1. \quad f(k_1, \dots, k_n) = k_{n+1} \quad \text{Hipótese}$$

$$2. \quad h_i(k_1, \dots, k_n) = t_i \quad \text{Hipótese } (1 \leq i \leq m)$$

3.  $g(t_1, \dots, t_m) = k_{n+1}$  Definição "g"
4.  $\vdash \alpha_i(\overline{k_1}, \dots, \overline{k_n}, \overline{t_i})$  2, Def. " $\alpha_i$ "
5.  $\vdash \beta(\overline{t_i}, \dots, \overline{t_m}, \overline{k_{n+1}})$  3, Def. " $\beta$ "
6.  $\vdash \alpha_1(\overline{k_1}, \dots, \overline{k_n}, \overline{t_1}) \wedge \dots \wedge$  4, 5, Def. " $\wedge$ "  
 $\wedge \alpha_m(\overline{k_1}, \dots, \overline{k_n}, \overline{t_m}) \wedge \beta(\overline{t_1}, \dots, \overline{t_m}, \overline{k_{n+1}})$
7.  $\vdash (\exists y_1), \dots, (\exists y_m) [ \alpha_1(\overline{k_1}, \dots, \overline{k_n}, \overline{y_1}) \wedge \dots \wedge$  6,  $\exists$ -Int.  
 $\wedge \alpha_m(\overline{k_1}, \dots, \overline{k_n}, \overline{y_m}) \wedge \beta(\overline{y_1}, \dots, \overline{y_m}, \overline{k_{n+1}}) ]$
8.  $[f(k_1, \dots, k_n) = k_{n+1}] \rightarrow \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$  1, 7, T. Ded.
9.  $\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$  1, 8, MP

Dem.: (Parte II.: **Condição 2** [ *Reductio* ])

1.  $(\exists y_1), \dots, (\exists y_m) [ \alpha_1(x_1, \dots, x_n, y_1) \wedge \dots \wedge$  Hip. Red.  
 $\wedge \alpha_m(x_1, \dots, x_n, y_m) \wedge \beta(y_1, \dots, y_m, u_1) ]$
2.  $(\exists y_1), \dots, (\exists y_m) [ \alpha_1(x_1, \dots, x_n, y_1) \wedge \dots \wedge$  Hip. Red.  
 $\wedge \alpha_m(x_1, \dots, x_n, y_m) \wedge \beta(y_1, \dots, y_m, u_2) ]$
3.  $\alpha_1(x_1, \dots, x_n, b_1) \wedge \dots \wedge \alpha_m(x_1, \dots, x_n, b_m) \wedge$  1,  $\exists$ -Elim.  
 $\wedge \beta(b_1, \dots, b_m, u_1)$
4.  $\alpha_1(x_1, \dots, x_n, c_1) \wedge \dots \wedge \alpha_m(x_1, \dots, x_n, c_m) \wedge$  2,  $\exists$ -Elim.  
 $\wedge \beta(c_1, \dots, c_m, u_2)$
5.  $\vdash (\exists^1 x_{n+1}) \alpha_i(x_1, \dots, x_n, x_{n+1})$  Def. "h" como " $\phi$ -repres."
6.  $b_i = c_i$  3, 4, 5

7.  $[\beta (b_1, \dots, b_m, u_1) \wedge b_1 = c_1 \wedge \dots \wedge b_m = c_m] \rightarrow$  3, 6  
 $\rightarrow \beta (c_1, \dots, c_m, u_1)$
8.  $\vdash (\exists^1 x_{n+1}) \beta (x_1, \dots, x_{n+1})$  Def. "g" como " $\varphi$  - repres."
9.  $[\beta (c_1, \dots, c_m, u_1) \wedge \beta (c_1, \dots, c_m, u_2)] \rightarrow u_1 = u_2$  7, 8
10.  $\vdash [\alpha (x_1, \dots, x_n, u_1) \wedge \alpha (x_1, \dots, x_n, u_2)] \rightarrow u_1 = u_2$  9
11.  $\vdash (\exists x_{n+1}) \alpha (x_1, \dots, x_n, x_{n+1})$  9 (parte I.),  $\exists$ -Int.
12.  $\vdash (\exists^1 x_{n+1}) \alpha (\overline{k}_1, \dots, \overline{k}_n, x_{n+1})$  10, 11

## SECÇÃO 4

### EXPRESSÃO E REPRESENTAÇÃO

#### **Definição 1.** [ *Função Característica* ]

*Seja*

$$R(x_1, \dots, x_n)$$

*uma relação aritmética.*

*Então diz-se que a notação*

$$K_R(x_1, \dots, x_n)$$

*designa a função característica de*

$$R(x_1, \dots, x_n)$$

*e define-se pela seguinte tabela:*

$R(x_1, \dots, x_n)$	$K_R(x_1, \dots, x_n)$
V	0
F	1

#### **Proposição 1.** [ *Expressão e Representação em Z* ]

*Uma relação aritmética*

$$R(x_1, \dots, x_n)$$

é esprimível em  $Z$  se e somente se  
a sua função característica é  $\varphi$ -representável em  $Z$ .

Dem.: (Parte I.)

1. Seja  $R(x_1, \dots, x_n)$  esprimível em  $Z$ .

2. Então existem as fórmulas

$$\vdash \alpha(x_1, \dots, x_n) \text{ ou } \vdash \neg \alpha(x_1, \dots, x_n)$$

conforme  $R(x_1, \dots, x_n)$  é verdadeira ou falsa,

i. e.,  $K_R(x_1, \dots, x_n) = 0$  ou  $K_R(x_1, \dots, x_n) = 1$ .

3. Logo, a fórmula  $\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$  tem a forma

$$[\alpha(x_1, \dots, x_n) \wedge x_{n+1} = 0] \vee [\neg \alpha(x_1, \dots, x_n) \wedge x_{n+1} = \overline{1}].$$

4. A univocidade de 0 e  $\overline{1}$  garantem a fórmula

$$\begin{aligned} & (\exists^1 x_{n+1}) [\alpha(x_1, \dots, x_n) \wedge x_{n+1} = 0] \vee \\ & \vee [\neg \alpha(x_1, \dots, x_n) \wedge x_{n+1} = \overline{1}]. \end{aligned}$$

Dem.: (parte II.)

1. Se a função característica  $K_R(x_1, \dots, x_n)$  é  $\varphi$ -representável em  $Z$ , então tem-se a fórmula

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}}).$$

2. Se  $R(x_1, \dots, x_n)$  é verdadeira então pode ser expressa pela fórmula  $\alpha(\overline{k_1}, \dots, \overline{k_n}, 0)$  e se é falsa pela fórmula

$$\alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{1}).$$

## SECÇÃO 5

### O ANEL COMUTATIVO $\mathbb{Z}_n$

Depois de termos provado que as funções iniciais e o processo de substituição são  $\varphi$ -representáveis, segue-se provar que o processo de recursão também é  $\varphi$ -representável. Assim qualquer função recursiva é  $\varphi$ -representável.

Para levar a cabo esta representação, no entanto, é necessário dispor da notação e de alguns resultados da Teoria da Congruência de Gauss.

Para dar uma ideia do que é a Teoria da Congruência de Gauss temos que regressar aos conceitos de divisibilidade e resto, já introduzidos. Para orientação usamos um exemplo numérico: a tabela dos restos da divisão por 5.

<i>Dividendo</i>	<i>divisor</i>	<i>Quociente</i>	<i>Resto</i>	$D = d \cdot Q + R$
0	5	0	0	$0 = 5 \cdot 0 + 0$
1	5	0	1	$1 = 5 \cdot 0 + 1$
2	5	0	2	$2 = 5 \cdot 0 + 2$
3	5	0	3	$3 = 5 \cdot 0 + 3$
4	5	0	4	$4 = 5 \cdot 0 + 4$
5	5	1	0	$5 = 5 \cdot 1 + 0$

6	5	1	1	$6 = 5 \cdot 1 + 1$
7	5	1	2	$7 = 5 \cdot 1 + 2$
8	5	1	3	$8 = 5 \cdot 1 + 3$
9	5	1	4	$9 = 5 \cdot 1 + 4$
10	5	2	0	$10 = 5 \cdot 2 + 0$
11	5	2	1	$11 = 5 \cdot 2 + 1$
12	5	2	2	$12 = 5 \cdot 2 + 2$
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Assim o resto deixado por qualquer inteiro  $n$  ao ser dividido por 5 é um dos números

$$0, 1, 2, 3, 4.$$

**Definição 1.** [ *Congruência* ]

*Dois números inteiros  $a$  e  $b$  que ao serem divididos por  $m$  têm o mesmo resto,*

*estão entre si na relação de “identidade quanto ao resto”.*

*À relação de “identidade quanto ao resto” chama Gauss congruência.*

*O número  $m$ , a respeito do qual os números  $a$  e  $b$  estão na relação de congruência, é o modulus da relação.*

*Assim, a expressão*

*« $a$  e  $b$  são congruentes modulo 5»*

*denota a relação de “identidade quanto ao resto” entre os números  $a$  e  $b$  quando são divididos por 5.*

A notação de Gauss para a relação de congruência é a seguinte:

$$a \equiv b \pmod{d}$$

que representa a congruência entre  $a$  e  $b$  modulo  $d$ .

**Exemplo 1.:**

Os números 27 e 15 são congruentes modulo 4.

*i)*  $27 = 6 \cdot 4 + 3$

*ii)*  $15 = 3 \cdot 4 + 3 .$

27 e 15 são idênticos quanto ao resto ao serem divididos por 4 – o resto idêntico é 3.

Em geral, se  $a$  e  $b$  são congruentes modulo  $d$ , então existe um número  $x$ , que é a solução da equação

$$a - b = x \cdot d .$$

Logo

$$x = \frac{a-b}{d} .$$

**Exemplo 1. (conti.):**

$$27 - 15 = 4 \cdot x$$

$$12 = 4 \cdot x$$

$$x = \frac{12}{4}$$

$$x = 3 .$$

Em particular, se

$$a - b = x \cdot d$$

então

$$a = b + x \cdot d .$$

Assim as seguintes proposições são equivalentes:

1.  $a \equiv b \pmod{d}$  ;
2.  $(\exists x) [ a = b + x \cdot d ]$  ;
3.  $d \mid (a - b)$  .

**Proposição 1.**     [ *Congruência é Identidade Quanto ao Resto* ]

$$a \equiv b \pmod{m} \leftrightarrow R(a, m) = R(b, m) .$$

Dem.: (Parte I:  $a \equiv b \pmod{m} \rightarrow R(a, m) = R(b, m)$ )

1.  $a \equiv b \pmod{m}$
2.  $a - b = k \cdot m$
3.  $R(b, m) = b - Q \cdot m$   
 $(0 \leq R \leq m)$
4.  $a = b + k \cdot m$
5.  $a = (Q \cdot m + R) + k \cdot m$
6.  $a = m \cdot (Q + K) + R$
7.  $R(a, m) = R$
8.  $R(b, m) = R(a, m)$

Dem.: (Parte II:  $R(a, m) = R(b, m) \rightarrow a \equiv b \pmod{m}$ )

1.  $R(a, m) = R(b, m)$
2.  $a = Q \cdot m + R$   
 $b = Q^* \cdot m + R$
3.  $a - b = (Q - Q^*) \cdot m$
4.  $m \mid (Q - Q^*) \cdot m$
5.  $m \mid a - b$
6.  $a \equiv b \pmod{m}$

**Proposição 2.** [ *Congruência como Relação de Equivalência* ]

*A relação de congruência  
é uma relação de equivalência.*

Dem.:

A identidade quanto ao resto satisfaz a definição usual de uma relação de equivalência. Assim,

**1. Reflexividade**

$$a \equiv a \pmod{d}$$

**2. Simetria**

$$(a \equiv b) \rightarrow (b \equiv a) \pmod{d}$$

**3. Transitividade**

$$[(a \equiv b) \wedge (b \equiv c)] \rightarrow (a \equiv c) \pmod{d}$$

As classes de equivalência induzidas pela relação de congruência chamam-se *classes de congruência* e são formadas pelos conjuntos

de todos os números que deixam o mesmo resto ao serem divididos por  $d$ .

Na última tabela (dos restos da divisão por 5) é fácil verificar que a coluna dos restos se deixa organizar em ciclos de ocorrências sucessivas do conjunto de números

$$\{ 0, 1, 2, 3, 4 \}.$$

No nosso exemplo há justamente

$$\frac{n}{5}$$

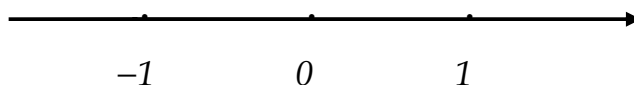
ciclos de ocorrências dos números

$$0, 1, 2, 3, 4$$

quando

$$n = 0, 1, \dots, n .$$

Esta observação está na origem de uma representação geométrica dos números inteiros que é diferente da usual. Na representação usual, os números são representados como pontos de uma recta



e a cada número corresponde um e um só ponto.

Mas do ponto de vista da relação de congruência, dois números que são congruentes  $mod\ d$  são iguais quanto ao resto da sua divisão por  $d$  e são por isso representados pelo mesmo ponto.

Para representar a coluna dos restos da nossa tabela vamos começar por representar um ciclo de ocorrências. Para isso adopta-se uma circunferência dividida num número igual,  $d$ , de partes.

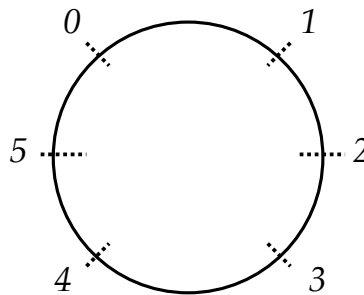
Qualquer inteiro, ao ser dividido por  $d$ , deixa como resto um dos números

$$0, 1, \dots, d - 1$$

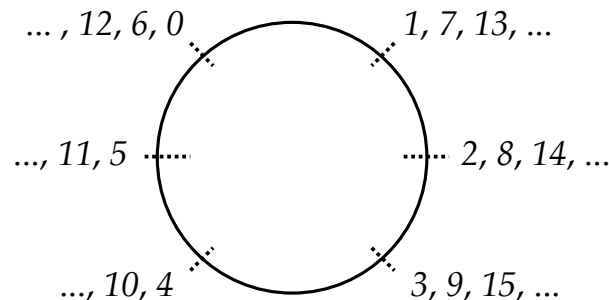
os quais constituem o ciclo recorrente  $\text{mod } d$  e aos quais é atribuído um dos pontos da circunferência.

**Exemplo 2.:**

Representação dos restos modulo 6:



Mas qualquer inteiro é congruente  $\text{mod } 6$  com um dos números aqui representados e por isso é representado pelo mesmo ponto que representa o número com o qual é congruente. Isto torna possível fazer uma representação *de todos os inteiros* à volta dos restos de um *modulus*. Para  $\text{mod } 6$  a figura a que isso dá origem tem os seguintes valores positivos:



Aqui as classes de congruência são as seguintes classes de equivalência:

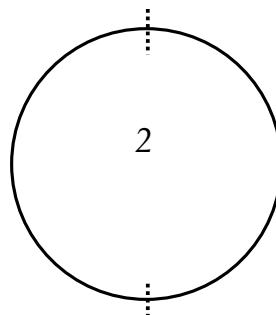
- [ 0 ]
- [ 1 ]
- [ 2 ]
- .
- .
- .
- [ 5 ].

Para um tratamento elementar do conceito de congruência começamos por identificar os valores de  $x$  que satisfazem uma fórmula, por exemplo,

$$4 \cdot x \equiv 0 \pmod{2} .$$

Estas fórmulas são conhecidas como “congruências” e são tratadas como equações para as quais se determina o conjunto de soluções. Estas soluções são

..., -4, -2, 0, 2, 4, ...



..., -5, -3, 1, 3, 5, ...

Em todo o caso é possível distinguir estes dois conjuntos de soluções, pelo facto de em cada conjunto todos os inteiros são

congruentes entre si  $\text{mod } 2$  mas nenhum inteiro no primeiro conjunto é congruente com um inteiro no outro conjunto  $\text{mod } 2$ .

**Definição 2.** [ *Classe de Congruência* ]

*A classe de congruência de  $a$  modulo  $n$ ,  
que se denota por*

$$[a]_n$$

*é o conjunto de todos os inteiros que são congruentes com  $a$  mod  $n$ .*

$$[a]_n = \{ b : b \equiv a \pmod{n} \}$$

**Definição 3.** [  $\mathbb{Z}_n$  ]

*O conjunto de todas as classes de congruência mod  $n$ ,  
que se denota por*

$$\mathbb{Z}_n$$

*é o conjunto de todos os inteiros mod  $n$ .*

Como se vê pela anterior tabela dos restos da divisão por 5 este conjunto tem exactamente  $n$  elementos, uma vez que só há  $n$  restos na divisão de um inteiro por  $n$ . [ No exemplo da tabela 0, 1, 2, 3, 4.]

**Definição 4.** [ *Classe de Congruência Nula* ]

*A classe de congruência nula ou a 0-classe de congruência é  
a classe de congruência de 0.*

É uma consequência das definições que

$$[a]_n = [b]_n \leftrightarrow a \equiv b \pmod{n} .$$

**Exemplo 3.:**

Quando  $n = 2$ , como no exemplo acima, há exactamente duas classes de congruência

$$[0]_2, [1]_2$$

as quais são também as soluções da equação

$$4 \cdot x \equiv 0 \pmod{2} .$$

**Definição 5.**      [ *Elemento Representativo* ]

*Um elemento representativo de uma classe de congruência é qualquer inteiro que pertence à classe.*

**Exemplo 4.:**

$$\mathbb{Z}_n = \{ [0]_n, [1]_n, \dots, [n-1]_n \} ;$$

$$\mathbb{Z}_5 = \{ [0]_5, [1]_5, \dots, [4]_5 \} ;$$

$$\mathbb{Z}_2 = \{ [0]_2, [1]_2 \} .$$

Em particular tem-se a igualdade

$$\oplus \quad k \cdot n + a = [a]_n .$$

Para identificarmos a estrutura de  $\mathbb{Z}_n$  precisamos de introduzir as funções Adição e Multiplicação entre classes de congruência.

**Definição 6.**       $[+, \times]$

1.     $(n > 1) \wedge (a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \rightarrow$   
       $\rightarrow [a]_n + [b]_n = [a+b]_n.$
2.     $(n > 1) \wedge (a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \rightarrow$   
       $\rightarrow [a]_n \times [b]_n = [a \times b]_n.$

**Proposição 3.**

Se

$$[a]_n = [c]_n,$$

então

$$\left\{ \begin{array}{l} i) \quad [a+b]_n = [c+b]_n ; \\ ii) \quad [a \times b]_n = [c \times b]_n . \end{array} \right.$$

Dem.: (Parte I.: i) )

1.     $[a]_n = [c]_n$
2.     $n \mid c - a$
3.     $c = a + k \cdot n$
4.     $[c+b]_n = [a+k \cdot n+b]_n$

$$5. [a+k \cdot n+b]_n = [a+b+k \cdot n]_n$$

$$6. [a+b+k \cdot n]_n = [a+b]_n \quad \oplus$$

$$7. [c+b]_n = [a+b]_n$$

$$8. [a+b]_n = [c+b]_n$$

Dem.: (Parte II.: ii) )

$$1. [c \times b]_n = [(a+k \cdot n) \cdot b]_n$$

$$2. [c \times b]_n = [a \cdot b + k \cdot n \cdot b]_n$$

$$3. [c \times b]_n = [a \cdot b]_n$$

$$4. [a \times b]_n = [c \times b]_n$$

Em particular, se

$$[a]_n = [c]_n \wedge [b]_n = [d]_n$$

então

$$i) [a+b]_n = [c+d]_n ;$$

$$ii) [a \times b]_n = [c \times d]_n .$$

[Dem.: substituir (na Proposição anterior)  $b$  por um outro elemento  $d$  que pertence à mesma classe do que  $b$ . ]

É possível construir tabelas para a Adição e para a Multiplicação em  $\mathbb{Z}_n$ . A ideia básica é que na intersecção da fila  $i$  com a coluna  $j$

ocorre o número

$$[a]_n + [b]_n$$

no caso da Adição e

$$[a]_n \times [b]_n$$

no caso da Multiplicação.

<b>+</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
<b>0</b>	0	1	2	3	4
<b>1</b>	1	2	3	4	0
<b>2</b>	2	3	4	0	1
<b>3</b>	3	4	0	1	2
<b>4</b>	4	0	1	2	3

<b>×</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
<b>0</b>	0	0	0	0	0
<b>1</b>	0	1	2	3	4
<b>2</b>	0	2	4	1	3
<b>3</b>	0	3	1	4	2
<b>4</b>	0	4	3	2	1

**Definição 7.**      [ *Inverso Multiplicativo* ]

*Diz-se que uma classe de congruência  $[a]_n$   
tem um inverso multiplicativo modulo  $n$*

se existe um  $b \in \mathbb{Z}$  tal que

$$[a]_n \times [b]_n = [1]_n.$$

Diz-se assim que  $[b]_n$  é o inverso multiplicativo de  $[a]_n$ ,

o qual se denota por

$$[a]_n^{-1}.$$

Logo

$$[a]_n \times [a]_n^{-1} = [1]_n.$$

Em particular se o inverso existe, então o produto

$$[a]_n \times [b]_n$$

é igual à classe de congruência  $[1]_n$ , o que significa que o número  $a \times b$  está na classe congruência  $[1]_n$ . Logo é congruente com 1 modulo  $n$  e assim

$$a \cdot b \equiv 1 \pmod{n}.$$

A Estrutura de  $\mathbb{Z}_n$  tem as seguintes descrições possíveis:

1. Sob a Adição e a Multiplicação modulo  $n \geq 2$ , o conjunto

$$0, 1, 2, \dots, n-1$$

constitui um Anel Comutativo.

2. O conjunto das classes de congruência que têm inverso multiplicativo modulo  $n$  é um Grupo sob a multiplicação. O Elemento Identidade é  $[1]_n$  e o Inverso de um elemento  $[a]_n$

$$\text{é } [a]_n^{-1}.$$

3. O conjunto das classes de congruência modulo  $n$  sob a Adição é um Grupo. O Elemento Identidade é a classe de congruência  $[0]_n$  e o Inverso Aditivo de  $[k]_n$  é  $[-k]_n$ .

**Definição 8.**      [ *Divisor-Zero* ]

*Diz-se que uma classe de congruência não-nula  $[a]_n$*

*é um Divisor-Zero*

*se existe um inteiro  $b$  tal que:*

*i)  $[b]_n \neq [0]_n$  ;*

*ii)  $[a]_n \times [b]_n = [0]_n$  .*

**Exemplo 5.:**

i)  $\mathbb{Z}_5$  tem inversos multiplicativos além de  $[1]_5$ , como  $[3]_5$  e  $[2]_5$  uma vez que

$$[3]_5 \times [2]_5 = [6]_5 = [1]_5.$$

ii)  $\mathbb{Z}_5$  não tem divisores-zero além de  $[0]_5$  mas é fácil de ver que  $\mathbb{Z}_6$  tem divisores-zero além de  $[0]_6$  como  $[2]_6$ , uma vez que

$$[2]_6 \times [3]_6 = [0]_6.$$

**Definição 9.**      [ *Primos Relativos aos Pares* ]

*Num conjunto de números inteiros positivos*

$$m_1, \dots, m_k$$

*diz-se que os elementos  $m_1, \dots, m_k$*

*são primos relativos aos pares*

*se nenhum par tem um factor inteiro comum excepto  $\pm 1$ .*

Se dois números  $a$  e  $b$  satisfazem a Definição 9, então a notação

$$\{ (a, b) = 1 \}$$

denota que os números  $a$  e  $b$  são primos relativos aos pares.

**Exemplo 3.:**

$$\{ 3, 4, 5 \}.$$

Pela Definição 9, estes números são primos relativos aos pares.

**Proposição 4.**

*Qualquer conjunto de inteiros  $M \neq \emptyset$  fechado*

*sob a Adição e a Subtracção ou*

*consiste apenas em 0 ou contém um elemento mínimo  $\mu$ ,*

*juntamente com todos os múltiplos de  $\mu$ .*

Dem.: (Parte I.:  $M$  contém um mínimo)

1. Seja  $a \in M \wedge a \neq 0$ .
2. Então pelo fecho sob a subtracção  
 $a - a \in M, i. e., 0 \in M$ .
3. Como

$$0 - a \in M$$

também  $-a \in M$ .

4. Assim  $(\exists a) (|a| = \pm a) \wedge |a| \in M$ .
5. Pela Boa Ordem de  $Z$ , seja  $\mu$  o menor desses elementos  $a$ .

Dem.: (Parte II.: *Todos os Múltiplos de  $\mu$  estão em  $M$  (Indução)*)

Dem.: (Parte II. 1.: *Base da Indução ( $n = 1$ )*)

1.  $n = 1$
2.  $\mu \cdot 1 = \mu$
3.  $\mu \cdot 1 \in M$

Dem.: (Parte II. 2. *Passo Indutivo*)

- |   |               |
|---|---------------|
| 1. $k \cdot \mu \in M$  | Hip. Indutiva |
| 2. $(k + 1) \cdot \mu = k \cdot \mu + \mu$  | Distrib.      |
| 3. $[(k \cdot \mu \in M) \wedge (\mu \in M)] \rightarrow [(k + 1) \cdot \mu \in M]$ | Fecho         |

Em particular, se  $-n$  é um múltiplo negativo,  $-n \cdot \mu \in M$ , uma vez que pelo Fecho sob “-”

$$-n \cdot \mu = 0 - n \cdot \mu .$$

Dem.: (Parte III.:  *$M$  só contém Múltiplos de  $\mu$* )

1. Seja  $a \in M$  um elemento arbitrário de  $M$ .
2. Então

$$\mu \mid a \rightarrow (a = \mu \cdot q + R).$$

3. E assim

$$R = a - \mu \cdot q .$$

4. Ora

$$0 \leq R < \mu .$$

5. Mas como  $\mu$  é o menor elemento em  $M$ ,  $R$  tem que ser igual a  $0$ .

6. Assim a fórmula 2.  $a = \mu \cdot q + R$  simplifica em

$$a = \mu \cdot q .$$

7. Logo qualquer  $a \in M$  é um múltiplo de  $\mu$ .

**Proposição 5.** [ *Existência de Inverso Multiplicativo* ]

$$\{ (p, q) = 1 \} \rightarrow (\exists x) (\exists y) [ p \cdot x + q \cdot y = 1 ]$$

$$(p > 0, q > 0, x \in \mathbb{Z}, y \in \mathbb{Z}).$$

Dem.:

1. Seja  $M$  o conjunto de todos os números da forma

$$p \cdot x + q \cdot y$$

que são maiores do que  $0$ .

2. Então pela proposição 4,  $M$  tem um mínimo  $\mu$ , que se representa por

$$(*) \mu = p \cdot x_0 + q \cdot y_0 .$$

3. Para demonstrar

$$p \cdot x + q \cdot y = 1$$

em  $M$  é suficiente provar que  $p$  e  $q$  são múltiplos de  $\mu$ .

4. A divisão de  $p$  por  $\mu$  pode ser representada pela fórmula

$$(**) p = \mu \cdot \alpha + R$$

em que

$$0 \leq R < \mu .$$

5. Multiplicando ambos os lados de (\*) por  $\alpha$  tem-se

$$p \cdot x_0 \cdot \alpha + q \cdot y_0 \cdot \alpha = \mu \cdot \alpha .$$

6. Mas por (\*\*)

$$\mu \cdot \alpha = p - R .$$

7. Assim, por 5. e 6.,

$$p - R = p \cdot x_0 \cdot \alpha + q \cdot y_0 \cdot \alpha .$$

8. Logo, por 7.,

$$R = p \cdot (1 - x_0 \cdot \alpha) + q \cdot (-y_0 \cdot \alpha) .$$

9. Ora, pelo passo 1.,  $\mu$  é o mínimo positivo e por 4.

$$0 \leq R < \mu .$$

10. Logo  $R$  tem que ser igual a  $0$  .

11. Logo  $p$  é múltiplo de  $\mu$  .

12. Pelo mesmo raciocínio  $q$  é múltiplo de  $\mu$  .

13. Assim  $\mu$  é um divisor comum de  $p$  e de  $q$  e, pela hipótese 2., é o mínimo.

14. Logo  $0 < \mu \leq 1$  e assim

$$\mu = 1 .$$

**Proposição 6.** [ *Máximo Divisor Comum Como Combinação Linear* ]

*Qualquer par de inteiros*

$$p \neq 0, q \neq 0$$

*têm um máximo divisor comum positivo,*

$$(p, q),$$

*o qual pode ser representado como uma combinação linear de  $p$  e  $q$   
com coeficientes inteiros  $x$  e  $y$  com a seguinte forma:*

$$(p, q) = p \cdot x + q \cdot y .$$

Dem.:

1. Formar o conjunto  $M$  de todos os números da forma

$$p \cdot x + q \cdot y .$$

2. Para qualquer par de  $M$  tem-se a igualdade

$$\begin{aligned} (p \cdot x_1 + q \cdot y_1) \pm (p \cdot x_2 + q \cdot y_2) &= \\ &= p \cdot (x_1 \pm x_2) + q \cdot (y_1 \pm y_2) . \end{aligned}$$

3. Logo  $M$  é fechado sob a Adição e a Subtracção e pela Proposição 4 consiste em todos os múltiplos de um mínimo  $\mu \in M$  com a forma

$$p \cdot x + q \cdot y = \mu .$$

4. Assim, qualquer factor comum  $k$  de  $p$  e  $q$  tem que ser um factor de  $\mu$ .
5. Por outro lado, pela proposição 5, os números  $p$  e  $q$  podem-se representar por

$$p = 1 \cdot p + 0 \cdot q$$

$$q = 0 \cdot p + 1 \cdot q ,$$

e são múltiplos do número  $\mu$ .

6. Logo  $\mu$  é um divisor comum.
7. Assim, por 3.,  $\mu$  é o máximo divisor comum.

**Proposição 7.**

$$(p \cdot x) + (q \cdot y) = 1 \rightarrow p \cdot x \equiv 1 \pmod{q}.$$

Dem.:

1. Se a equação  $(p \cdot x) + (q \cdot y) = 1$  é reduzida ao *modulo*  $q$ , obtém-se

$$[p \cdot x]_q + [q \cdot y]_q = [1]_q.$$

2. Como no *modulo*  $q$ ,  $q \cdot y$  é congruente com  $0$ , tem-se

$$[p \cdot x]_q + [0]_q = [1]_q.$$

3. Logo

$$[p \cdot x]_q = [1]_q.$$

4. Assim  $x$  é o inverso multiplicativo de  $[p]_q$ .

5. Em particular,  $p \cdot x$  é congruente com  $1$  *modulo*  $q$  e assim

$$p \cdot x \equiv 1 \pmod{q}.$$

### Proposição 8.

Se  $[p]_q$  tem um inverso multiplicativo

então  $\{(p, q) = 1\}$ .

Dem.:

1.  $[p]_q$  tem um inverso  $[x]_q$  Hip.
2.  $[p]_q \times [x]_q = [1]_q$
3.  $p \cdot x \equiv 1 \pmod{q}$
4.  $q \mid p \cdot x - 1$

$$5. (\exists y) p \cdot x - 1 = q \cdot y$$

$$6. p \cdot x - q \cdot y = 1$$

$$7. \{ (p, q) = 1 \}$$

**Exemplo 6.:**

$$1 = 3 \cdot 2 + 5 \cdot (-1)$$

$$1 = 6 - 5$$

Logo 2 é o inverso multiplicativo de 3 *modulo* 5.

**Exemplo 7.:**

Se  $p = 50$  e  $x = 25$ , então não se tem

$$\{ (50, 25) = 1 \},$$

uma vez que  $5 | 50 \wedge 5 | 25$ .

Logo 50 não tem um inverso *modulo* 25.

**Exemplo 8.:**

Com número pequenos é fácil detectar um inverso num *modulo*.

Para encontrar  $[8]_{11}^{-1}$  é suficiente encontrar um número  $x$  tal que

$$8 \cdot x \equiv 1 \pmod{11}.$$

Como o Resto de  $11 | 56$  é 1,

$$x = 7.$$

**Exemplo 9.:**      [ *Auto-Inverso* ]

No *modulo 20* tem-se

$$121 \equiv 1 .$$

Mas como  $121 = 11^2$ , tem-se

$$[11]_{20} \times [11]_{20} = [1]_{20}$$

e logo

$$[11]_{20} = [11]_{20}^{-1} .$$

### Proposição 9.

$$\{ \{ (R, a) = 1 \} \wedge [R | (a \cdot b)] \} \rightarrow R | b.$$

Dem.:

- |    |   |                   |
|----|---|-------------------|
| 1. | $a \cdot b = p \cdot R$                     | Hip., Definição   |
| 2. | $k \cdot R + m \cdot a = 1$                 | Prop. 5           |
| 3. | $k \cdot R \cdot b + m \cdot a \cdot b = b$ | 2, Subst.         |
| 4. | $k \cdot R \cdot b + m \cdot p \cdot R = b$ | 1, 3, Ax. Identi. |
| 5. | $R \cdot (k \cdot b + m \cdot p) = b$       | 4, Distrib.       |
| 6. | $R   b$                                     | 5, Def. “   ”     |

A definição de um número  $p$  como primo quando tem exactamente 2 divisores positivos, 1 e  $p$ , exclui 1 como número primo, uma vez que 1 não tem 2 divisores positivos diferentes.

Em particular, o menor número primo é 2 e qualquer outro número par  $p > 2$  tem pelo menos 3 divisores, 1, 2 e  $p$ .

**Proposição 10.**

$$[ P(p) \wedge p|(a \cdot b) ] \rightarrow [ (p|a) \vee (p|b) ].$$

Dem.:

1.  $P(p)$  implica que os únicos factores de  $p$  são  $\pm 1$  e  $\pm p$ .
2. Se  $\neg (p|a)$ , então os únicos divisores comuns de  $p$  e de  $a$  são  $\pm 1$ .
3. Logo  $\{ (p, a) = 1 \}$ .
4.  $(\exists x) (\exists y) [ x \cdot a + y \cdot p = 1 ]$
5. Logo  $b = b \cdot (x \cdot a) + b \cdot (y \cdot p)$ .
6. Como por hipótese  $p|(a \cdot b)$ , então  $p$  divide  $b \cdot (x \cdot a) + b \cdot (y \cdot p)$ .
6. Logo  $p|b$ .

**Proposição 11.**

$$[ P(p) \wedge p|(a_1 \cdot \dots \cdot a_n) ] \rightarrow (\exists i) p|a_i.$$

Dem. [ *Indução sobre n* ]:

Dem.: (Parte I.: *Base indutiva (n = 1)*)

1.  $p|a_1 \rightarrow p|a_1$

Dem.: (Parte II.: *Passo indutivo*)

1. Supor

$$p|(b_1 \cdot b_2 \cdot \dots \cdot b_{n-1}) \rightarrow (\exists i) p|b_i.$$

2. Reformular

$$a_1 \cdot \dots \cdot a_n$$

num produto de  $n - 1$  inteiros

$$b_1 \cdot \dots \cdot b_{n-1}.$$

3. Definir a seguir

$$\begin{cases} b_i = a_i, & i \leq n - 2 \\ b_{n-1} = a_{n-1} \cdot a_n \end{cases}$$

4. Introduzindo parêntesis, a fórmula

$$a_1 \cdot a_2 \cdot \dots \cdot a_{n-2} \cdot (a_{n-1} \cdot a_n)$$

reproduz o produto dos primeiros  $n - 1$  inteiros.

5. Logo

$$p \mid a_1 \cdot a_2 \cdot \dots \cdot a_{n-2} \vee p \mid (a_{n-1} \cdot a_n).$$

6. Se

$$p \mid a_1 \cdot a_2 \cdot \dots \cdot a_{n-2}$$

então pela Hipótese Indutiva

$$(\exists i) p \mid a_i.$$

7. Se  $p \mid (a_{n-1} \cdot a_n) \rightarrow p \mid a_{n-1} \vee p \mid a_n.$

8. Logo  $(\exists i) p \mid a_i.$

9. Logo  $(\exists i) p \mid a_i$ , por  $\vee$ -Elim.

**Proposição 12.** [ *Teorema de Gauss, Teorema Fundamental da Aritmética* ]

i) Qualquer inteiro positivo  $x \geq 2$  tem uma representação sob a forma

$$x = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

em que  $p_1, p_2, \dots, p_n$  são números primos e  $n \geq 1$ .

ii) Esta representação é única.

Assim se existe uma outra representação

$$x = t_1 \cdot t_2 \cdot \dots \cdot t_k$$

então  $k = n$  e é possível redenominar  $t_1, \dots, t_k$  de modo a que

$$p_i = t_i \text{ com } i = 1, 2, \dots, n.$$

Dem. [Parte I.: *Indução Completa* ]:

Dem.: (Parte I. 1: *Base da Indução* ( $x = 2$ ))

1. Se  $x = 2$ , então o Teorema reduz-se em  $2 = 2^1$ .

Dem.: (Parte I. 2.: *Passo Indutivo*)

A Hipótese Indutiva é que o Teorema é verdadeiro para todos os valores  $< x$ .

1. Se  $x > 2$  então ou  $x$  é primo ou  $x$  é compósito.

2. Se  $x$  é primo, o Teorema é verdadeiro e  $x$  tem uma representação com um único factor.

3. Se  $x$  é compósito então pode ser expresso como um produto

$$a \cdot b$$

em que  $a$  e  $b$  são menores do que  $x$ .

4. Mas pela hipótese indutiva  $a$  e  $b$  têm uma representação respectivamente  $\Pi_i$  e  $\Pi_j$  como um produto de primos.

5. Logo, pela Proposição 12 (Cap. I, secção 4),  $x$  tem a representação

$$x = \prod_i * \prod_j .$$

Dem. [Parte II.: *Indução sobre o Comprimento da Representação n* ]:

Dem.: (Parte II. 1.: *Base Indutiva (n = 1)*)

1. Supor que  $x$  é primo com uma representação

$$x = \prod_{i=1}^s t_i .$$

2. Se  $s \geq 2$ , então  $x$  tem como divisores  $1, t_1, t_1 \cdot t_2, \dots, x$  divisores.

3. Logo não pode ser primo.

4. Logo  $s = 1$ .

Dem.: (Parte II. 2.: *Passo Indutivo*)

A Hipótese Indutiva garante a univocidade da representação até a um comprimento  $n - 1$ .

1. Supor que

$$x = \prod_{i=1}^r t_i .$$

$$x = \prod_{i=1}^s m_i .$$

2. Como  $t_1$  divide  $x$ , tem-se que existe um  $m_i$  que  $t_1$  também divide, pela Proposição 11.

3. Pode-se redenominar  $m_i$  de modo a que  $t_1$  divida  $m_1$ .

4. Mas como  $m_1$  é primo, então tem-se

$$t_1 = m_1 .$$

5. Eliminando o índice 1 em ambas as fórmulas fica-se com

$$x = \prod_{i=2}^r t_i$$

$$x = \prod_{i=2}^s m_i .$$

6. Mas

$$x = \prod_{i=2}^r t_i$$

é o produto dos  $r - 1$  primos, o qual é igual ao produto dos  $s - 1$  primos pela Hipótese da Indução.

7. Logo

$$r = s$$

e fazendo a redenominação

$$(\forall i) t_i = m_i .$$

**Proposição 13.** [ *Teorema de Euclides* ]

*O conjunto dos números primos é infinito.*

Dem. [*Reductio*]:

1. A Hipótese da *Reductio* é

$$(*) \quad p_1, \dots, p_n \quad (\text{com } p_1 = 2)$$

ser a totalidade dos números primos.

2. Definir a seguir um número  $E$  como

$$E = p_n! + 1 .$$

3. Assim  $E$  deixa resto  $1$  ao ser dividido por qualquer dos  $p_i$ .

4. Mas pelo Teorema de Gauss  $E$  tem uma representação com um divisor primo  $p$ .
5. Logo  $p \mid E$  e  $(\forall i) p \neq p_i$ .
6. Logo  $p$  é primo e não está em (\*).

A Lei da Cancelação usada entre equações não é sempre satisfeita com congruências.

Embora

$$2 \cdot 3 \equiv 2 \cdot 8 \pmod{5}$$

implique

$$3 \equiv 8 \pmod{5}$$

em geral o resultado não obtém.

**Exemplo 10.:**

$$2 \cdot 4 \equiv 2 \cdot 1 \pmod{4}$$

não implica

$$4 \equiv 1 \pmod{4}.$$

Isto é devido ao facto de 2 ser um divisor do *Modulus*. Mas a cancelação pode ser restrita à proposição seguinte:

**Proposição 14.**                    [ *Teorema da Cancelação* ]

$$\{ (k, m) = 1 \} \rightarrow [ k \cdot a \equiv k \cdot b \pmod{m} ] \rightarrow a \equiv b \pmod{m} .$$

Dem.:

1.  $k \cdot a \equiv k \cdot b \pmod{m}$
2.  $[k]_m \times [a]_m = [k]_m \times [b]_m$
3.  $\{(k, m) = 1\}$  implica que existe o inverso de  $[k]_m$
4.  $[k]_m \times [a]_m \times [k]_m^{-1} = [k]_m \times [b]_m \times [k]_m^{-1}$
5.  $[a]_m \times [1]_m = [b]_m \times [1]_m$
6.  $[a]_m = [b]_m$
7.  $a \equiv b \pmod{m}$

**Proposição 15.** [ *Divisibilidade de Múltiplos de Primos Relativos* ]

$$\{(a, b) = 1\} \rightarrow \{[(a|m) \wedge (b|m)] \rightarrow (a \cdot b|m)\}.$$

Dem.:

1. Se  $m$  é um múltiplo de cada um dos primos relativos  $a$  e  $b$  e tal que

$$a|m \wedge b|m$$

então

$$m = a \cdot k.$$

2. Como por hipótese  $b|m$ , então

$$b|k, \text{ uma vez que}$$

$$b|a \cdot k \rightarrow b|k.$$

3. Como  $a|a$ , tem-se

$$a|a \wedge b|k.$$

4. Mas  $\frac{a}{a} \cdot \frac{k}{b} = \frac{a \cdot k}{a \cdot b}$ .
5. Logo  $a \cdot b \mid a \cdot k$  e assim  
 $a \cdot b \mid m$ .

**Proposição 16.**

*Seja  $n > 1$ . Então um elemento  $\neq [0]_n$  em  $\mathbb{Z}_n$   
ou tem um Inverso ou é um Divisor-0 mas não ambos.*

Dem.: (Parte I:)

1. Supor que  $[a]_n$  não tem um Inverso.

2. Então

$$(n, a) = d \wedge d > 1.$$

3. Logo

$$d \mid n \wedge d \mid a$$

e assim tem-se

$$a = k \cdot d$$

$$n = p \cdot d, \text{ com } p < n.$$

4. Como  $p = \frac{n}{d}$ , tem-se

$$a \times \frac{n}{d} = k \cdot \frac{n}{d} \times d$$

e assim que

$$a \cdot p = k \cdot n.$$

5. Logo  $[a]_n \times [p]_n = [k]_n \times [n]_n$

6.  $[a]_n \times [p]_n = [0]_n$
7.  $[a]_n$  é um Divisor-Zero.

Dem.: (Parte II.):

1. Supor que  $[a]_n$  tem um Inverso,  $[b]_n$ , e que é dada uma equação

$$[a]_n \times [b]_n = [0]_n .$$

2. Então tem-se

$$[a]_n^{-1} \times [a]_n \times [b]_n = [a]_n^{-1} \times [0]_n .$$

3. Assim

$$[b]_n = [0]_n .$$

4. Logo  $[a]_n$  não é um Divisor-Zero.

**Proposição 17.**     [ *Teorema de Euler* ]

*Se  $p$  é primo*

*então qualquer elemento não-nulo de  $\mathbb{Z}_p$  tem um Inverso.*

Dem.:

1. Se  $[a]_p \neq [0]_p$ , então  
 $\neg (p | a)$ .
2. Logo  $\{ (a, p) = 1 \}$ .
3. Logo  $[a]_p$  tem um Inverso.

Notação:

Para  $n > 1$ , o conjunto das classes de congruência de  $\mathbb{Z}_n$  que têm um Inverso denota-se por

$$\mathbb{Z}_n^*.$$

Assim

$$[a]_n \in \mathbb{Z}_n^* \leftrightarrow \{(a, n) = 1\}.$$

**Proposição 18.** [ *Fecho de  $\mathbb{Z}_n^*$  Sob a Multiplicação* ]

$$\begin{aligned} n > 2 \wedge [a]_n \in \mathbb{Z}_n^* \wedge [b]_n \in \mathbb{Z}_n^* &\rightarrow \\ &\rightarrow [a]_n \times [b]_n \in \mathbb{Z}_n^* . \end{aligned}$$

Dem.:

1.  $[a]_n \in \mathbb{Z}_n^* \wedge [b]_n \in \mathbb{Z}_n^*$
2.  $\{(a, n) = 1\} \wedge \{(b, n) = 1\}$
3. Mas pela Proposição 10
 
$$p | a \cdot b \rightarrow p | a \vee p | b .$$
4. Assim  $a \cdot b$  e  $n$  não têm um factor comum além de 1.
5. Logo
 
$$\{(a \cdot b, n) = 1\}$$
6. Assim  $a \cdot b$  tem um Inverso *modulo*  $n$ , i.e.,

$$[a]_n \times [b]_n \in \mathbb{Z}_n^*.$$

[ Estrutura em  $\mathbb{Z}_n$  ]

$\langle \mathbb{Z}_{n'}, + \rangle$	Grupo Comutativo
$\langle \mathbb{Z}_{n'}, \times \rangle$	Grupo Comutativo
$\langle \mathbb{Z}_{n'}, +, \times \rangle$	Anel Comutativo
$\langle \mathbb{Z}_{n'}^*, +, \times \rangle$	Corpo

**Definição 10.** [ *Congruência Linear* ]

*Uma congruência linear é  
uma equação da forma  
 $a \cdot x \equiv b \pmod{m}$ .*

**Proposição 19.** [ *Soluções de uma Congruência Linear* ]

- i)  $\{ (a, m) = 1 \} \rightarrow a \cdot x \equiv b \pmod{m}$   
tem uma solução inteira  $x$ .*
- ii)  $\{ (a, m) = 1 \} \rightarrow [ a \cdot x_1 \equiv b \pmod{m} \wedge$   
 $\wedge a \cdot x_2 \equiv b \pmod{m} ] \rightarrow x_1 \equiv x_2 \pmod{m}$ .*

Dem.: (Parte I: Cláusula i))

1.  $\{ (a, m) = 1 \}$
2.  $(\exists p) (\exists q) [ p \cdot a + q \cdot m = 1 ]$
3.  $[p \cdot a]_m + [q \cdot m]_m = [1]_m$
4.  $[p \cdot a]_m + [0]_m = [1]_m$
5.  $[p \cdot a]_m = [1]_m$
6.  $[b]_m \times [p \cdot a]_m = [b]_m$
7.  $[b \cdot p]_m \times [a]_m = [b]_m$
8.  $b \cdot p \cdot a \equiv b \pmod{m}$
9. Logo  $x = b \cdot p$

Dem.: (Parte II.: Cláusula ii): *Congruência das Soluções*)

1.  $(x = x_1) \wedge (x = x_2)$
2.  $[a \cdot x_1 \equiv b \pmod{m}] \wedge [a \cdot x_2 \equiv b \pmod{m}]$
3.  $(a \cdot x_1 \equiv b) \wedge (b \equiv a \cdot x_2) \rightarrow (a \cdot x_1 \equiv a \cdot x_2)$
4.  $a \cdot x_1 \equiv a \cdot x_2$
5.  $x_1 \equiv x_2 \pmod{m}$

### Exemplo 11.:

$$6 \cdot x \equiv 5 \pmod{17}$$

Solução:

1.  $\{ (6, 17) = 1 \} \rightarrow (\exists p) (\exists q) [ p \cdot 6 + q \cdot 17 = 1 ]$
2.  $[p \cdot 6]_{17} + [q \cdot 17]_{17} = [1]_{17}$
3.  $[p \cdot 6]_{17} = [1]_{17}$

4.  $[6]_{17}^{-1} = [3]_{17}$
5.  $[6]_{17} \cdot [3]_{17} \cdot x \equiv [5]_{17} \cdot [3]_{17}$
6.  $x \equiv [15]_{17}$
7.  $x = [15]_{17}$

**Exemplo 12.:**

$$2 \cdot x \equiv 3 \pmod{5}$$

Solução:  $x = [4]_5$

**Proposição 20.** [ *Congruências Simultâneas* ]

*i) Se os Moduli  $m_1$  e  $m_2$  são primos relativos e  $b_1$  e  $b_2$  são números naturais, então as congruências simultâneas*

$$(*) \quad x \equiv b_1 \pmod{m_1}$$

$$(**) \quad x \equiv b_2 \pmod{m_2}$$

*têm uma solução comum  $x$ .*

*ii) Qualquer par de soluções  $x_1, x_2$  é congruente modulo  $m_1 \cdot m_2$*

$$x_1 \equiv x_2 \pmod{m_1 \cdot m_2}.$$

Dem.: (Parte I.)

1. Se por hipótese se tem

$$(*) \quad x \equiv b_1 \pmod{m_1}$$

então

$$(\forall y) (x = b_1 + y \cdot m_1) .$$

2. Mas a condição necessária e suficiente para este valor

$$x = b_1 + y \cdot m_1$$

satisfazer a congruência (\*\*) é

$$b_1 + y \cdot m_1 \equiv b_2 \pmod{m_2} .$$

3. Isto equivale a dizer que

$$m_2 \mid b_1 + y \cdot m_1 - b_2 .$$

4. Assim

$$m_2 \mid y \cdot m_1 - b_2 + b_1 .$$

5. Logo

$$y \cdot m_1 \equiv b_2 - b_1 \pmod{m_2} .$$

6. Mas como  $\{ (m_1, m_2) = 1 \}$  pela hipótese, o Teorema anterior garante a existência de uma solução  $y$  para esta congruência.

Dem.: (Parte II.:)

1. Suponha-se agora que  $x_1$  e  $x_2$  são duas soluções das congruências simultâneas

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2} .$$

2. Então pela Proposição anterior

$$x_1 \equiv x_2 \pmod{m_1} .$$

3. Logo

$$m_1 \mid x_1 - x_2 .$$

4. Do mesmo modo

$$m_2 \mid x_1 - x_2 .$$

5. Logo pela Proposição 15 [ *Divisibilidade de Múltiplos de Primos Relativos* ]

$$m_1 \cdot m_2 \mid x_1 - x_2 .$$

6. Assim

$$x_1 \equiv x_2 \pmod{m_1 \cdot m_2} .$$

A doutrina do Teorema anterior pode ser aplicada a uma sucessão de *moduli*  $m_1, \dots, m_k$ , os quais são primos relativos aos pares e a um  $n$ -tuplo de números naturais. A Proposição a que se é conduzido é conhecida como o Teorema do Resto Chinês.

**Proposição 21.** [ *Teorema do Resto Chinês* ]

*i) Se os moduli*

$$m_1, \dots, m_k$$

*são primos relativos aos pares*

*e*

$$b_1, \dots, b_k$$

*são números naturais,*

*então as congruências simultâneas*

$$x \equiv b_1 \pmod{m_1}$$

$\cdot$

$\cdot$

$\cdot$

$$x \equiv b_k \pmod{m_k}$$

*têm uma solução comum  $x$ .*

ii) Qualquer par de soluções é congruente modulo

$$m_1 \cdot m_2 \cdot \dots \cdot m_k.$$

Dem. [ *Indução em k* ]:

Dem.: (Parte I. 1.):

1. Se  $k = 1$  então a equação

$$x \equiv b_1 \pmod{m_1}$$

tem uma solução

$$x = Q \cdot m_1 + b_1.$$

Dem.: (Parte I. 2.):

1. A hipótese indutiva é que

$$x \equiv b_{k-1} \pmod{k-1}.$$

2. Logo esta congruência tem uma solução

$$x = Q \cdot m_{k-1} + b_{k-1}.$$

3. Mas resolver

$$x \equiv b_k \pmod{m_k}$$

é equivalente a mostrar que

$$Q \cdot m_{k-1} + b_{k-1} \equiv b_k \pmod{m_k}.$$

4. Logo

$$Q \cdot m_{k-1} \equiv b_k - b_{k-1} \pmod{m_k}.$$

5. Mas pela hipótese tem-se

$$\{(m_{k-1}, m_k) = 1\}.$$

6. Logo

$$Q \cdot m_{k-1} \equiv b_k - b_{k-1} \pmod{m_k}$$

é uma congruência linear que tem uma solução pela proposição 19 [ *Soluções de uma Congruência Linear* ].

Dem.: (Parte II.)

Qualquer par de soluções é congruente *modulo*

$$m_1 \cdot m_2 \cdot \dots \cdot m_k$$

pelo mesmo argumento da parte II. da proposição 20 [ *Congruências Simultâneas* ].

### Exemplo 13.:

As congruências simultâneas

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

têm uma solução comum  $x$ .

1. Pelo Teorema do Resto Chinês

$$x \equiv 2 \pmod{3}$$

tem uma solução

$$x = Q \cdot 3 + 2 .$$

2. Mas  $x$  ser uma solução da 2ª equação é equivalente a

$$Q \cdot 3 + 2 \equiv 3 \pmod{5} .$$

3. Logo

$$[Q \cdot 3]_5 + [2]_5 = [3]_5 .$$

4. Assim

$$[Q \cdot 3]_5 = [3 - 2]_5 .$$

5. Calculando  $[3]_5^{-1}$ , obtém-se  $[2]_5$ .

6. Assim (por 4. obtém-se)

$$[3]_5^{-1} \times [3]_5 \times Q \equiv [1]_5 \times [3]_5^{-1}.$$

7. Logo

$$Q \equiv [2]_5.$$

8. Mas  $[2]_5 = 5 \cdot p + 2$ .

9. Assim o conjunto de soluções com a forma comum

$$x = Q \cdot 3 + 2$$

é

$$x = (5 \cdot p + 2) \cdot 3 + 2.$$

10.  $x = 15 \cdot p + 8$

e assim

$$x = [8]_{15}.$$

É fácil verificar que um dos valores de  $x$  é 23, uma vez que

$$23 \equiv 8 \pmod{15}$$

$$23 \equiv 2 \pmod{3}$$

$$23 \equiv 3 \pmod{5}.$$

## SECÇÃO 6

### RECURSÃO E REPRESENTAÇÃO

#### **Definição 1.** [ *Sucessão $\Gamma$ de Gödel* ]

*Seja*

$1, \dots, n$

*uma sucessão de números naturais.*

*Então existe o número  $n!$  tal que*

$$n \cdot n - 1 \cdot \dots \cdot 1 = n! .$$

*Assim o número  $n!$  é divisível por cada um dos elementos de  $1, \dots, n,$*

*de tal modo que se obtém a sucessão de divisibilidades*

$$1 | n!, 2 | n!, \dots, n | n! .$$

*Seja  $n!$  representado por  $l$ . Então os elementos da sucessão  $\Gamma$  de Gödel*

*são os números da forma*

$$(k + 1) \cdot l + 1.$$

*A sua representação é*

$$\Gamma = 1 \cdot l + 1, 2 \cdot l + 1, \dots, n \cdot l + 1, (n + 1) \cdot l + 1 .$$

#### **Proposição 1.** [ *Divisibilidade na Sucessão $\Gamma$* ]

*Os elementos de  $\Gamma$*

*são primos relativos.*

Dem. [ *Reductio* ]:

1. A Hipótese da *Reductio* é a de que existe um número primo  $p$  tal que  $p$  divide

$$1 + (j + 1) \cdot l$$

e  $p$  divide também

$$1 + (j + k + 1) \cdot l.$$

2. Então

$$[ 1 + (j + k + 1) \cdot l ] \equiv [ 1 + (j + 1) \cdot l ] \pmod{p}.$$

3. Logo  $p$  divide a diferença

$$[ 1 + (j + k + 1) \cdot l ] - [ 1 + (j + 1) \cdot l ] .$$

4. Assim  $p$  divide

$$1 + j \cdot l + k \cdot l + l - 1 - j \cdot l - l.$$

5. Logo  $p$  divide  $k \cdot l$ .

6. Então

$$p | k \cdot l \rightarrow [ (p | l) \vee (p | k) ].$$

**Caso 1.:** [  $p | l$  ]

- |    |   |           |
|----|---|-----------|
| 1. | $p   l \rightarrow [ p   (j + 1) \cdot l ]$ | Definição |
| 2. | $p   1 + (j + 1) \cdot l$                   | Hipótese  |
| 3. | $\neg (p   l)$                              | 1, 2      |

**Caso 2.:** [  $p | k$  ]

- |    |                                    |           |
|----|------------------------------------|-----------|
| 1. | $k \leq n \leq \max (1, \dots, n)$ | Definição |
| 2. | Logo,                              | Definição |

$$(\forall k) (k|l)$$

$$3. (p|k) \wedge (k|l) \rightarrow p|l \quad \text{Hipótese, 2}$$

$$4. \neg (p|l) \wedge p|l \quad \text{3, Caso 1. passo 3}$$

Para exprimir em  $Z$  asserções acerca de sucessões finitas de números naturais é essencial dispor da função  $\beta$  de Gödel.

**Definição 2.**      [ *Função  $\beta$  de Gödel* ]

*Se  $m, l, k$  são números naturais então a função*

$$\beta (m, l, k)$$

*calcula o resto da divisão de  $m$  por um termo*

$$(k + 1) \cdot l + 1$$

*da sucessão  $\Gamma$ .*

*Assim,*

$$\beta (m, l, k) = R [ m, (k + 1) \cdot l + 1 ]$$

**Proposição 2.**      [ *Representabilidade de Sucessões de Números Naturais pela Função  $\beta$*  ]

$$\langle a_0, \dots, a_n \rangle \in \mathbb{N} \rightarrow (\exists m) (\exists l) [ a_k = \beta (m, l, k) ].$$

Dem.:

1. Seja

$$a_0, \dots, a_n$$

uma sucessão de números naturais.

2. Então existe um número  $l$  tal que a sucessão

$$\Gamma = 1 \cdot l + 1, 2 \cdot l + 1, \dots, n \cdot l + 1, (n + 1) \cdot l + 1$$

pode ser construída.

3. Seja

$$l \geq \max (a_1, \dots, a_n) .$$

4. Então

$$a_k < (k + 1) \cdot l + 1 .$$

5. Mas pela Proposição anterior os números

$$(k + 1) \cdot l + 1$$

são primos relativos aos pares.

6. Então as congruências simultâneas

$$x_1 \equiv a_0 \ [ \text{mod } (1 \cdot l + 1) ]$$

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

$$x_n \equiv a_n \ [ \text{mod } (n + 1) \cdot l + 1 ]$$

têm uma solução comum  $m$ , pelo T. do Resto Chinês.

7. Logo  $m \equiv a_k \ [ \text{mod } (k + 1) \cdot l + 1 ]$ .

8. Assim  $a_k = R (m, (k + 1) \cdot l + 1)$ .

9. Logo  $a_k = \beta (m, l, k) .$

Seja

$$a_0, \dots, a_n$$

uma sucessão de números naturais.

Então  $a_0, \dots, a_n$  tem uma representação por meio da função  $\beta$  com as congruências simultâneas nos *moduli*

$$1 \cdot l + 1, \dots, k \cdot l + 1, (k + 1) \cdot l + 1.$$

Essa representação é possível para qualquer sucessão

$$a_0, \dots, a_n.$$

Para demonstrar o carácter recursivo primitivo da função  $\beta$  de Gödel é útil redenominar as variáveis do seguinte modo:

$$m = x_1$$

$$l = x_2$$

$$k = x_3.$$

**Proposição 3.** [ *Recursão na Função  $\beta$  de Gödel* ]

*Seja  $\beta$  a função de Gödel. Então a função*

$$\beta(x_1, x_2, x_3)$$

*é recursiva primitiva.*

Dem.:

1. A função

$$\beta(x_1, x_2, x_3) = R[x_1, (x_3 + 1) \cdot x_2 + 1].$$

2. Como as funções “ + ”, “ · ”, e “ R ” são recursivas primitivas,  $\beta$  é recursiva primitiva.

Convém agora recordar que uma função

$$f(x_1, \dots, x_n)$$

é  $\Phi$ -representável em Z se e somente se existe uma fórmula bem formada

$$\alpha(x_1, \dots, x_n, x_{n+1})$$

de Z com  $x_1, \dots, x_{n+1}$  variáveis livres, tal que a expressão

$$f(k_1, \dots, k_n) = k_{n+1}$$

é representada por

$$\vdash \alpha(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$$

para qualquer

$$k_1, \dots, k_{n+1}.$$

Além disso tem-se ainda que representar em Z a univocidade de  $x_{n+1}$  por meio da fórmula

$$\vdash (\exists^1 x_{n+1}) \alpha(x_1, \dots, x_n, x_{n+1}).$$

**Proposição 4.**      [ *Representabilidade da Função  $\beta$*  ]

A função

$$\beta(x_1, x_2, x_3)$$

é  $\Phi$ -representável em Z.

Dem.:

A fórmula

$$\alpha(x_1, \dots, x_{n+1})$$

de Z tem a forma

$$B(x_1, x_2, x_3, x_4)$$

com a seguinte configuração:

$$(\exists Q) \{ x_1 = \{ [(x_3 + 1) \cdot x_2 + 1] \cdot Q + x_4 \} \wedge \\ \wedge \{ x_4 < (x_3 + 1) \cdot x_2 + 1 \} \}.$$

1.  $\beta(k_1, k_2, k_3) = k_4$  Hipótese
2.  $k_1 = [(k_3 + 1) \cdot k_2 + 1] \cdot k + k_4$
3.  $k_4 < (k_3 + 1) \cdot k_2 + 1$
4.  $\bar{k}_1 = \{ [(\bar{k}_3 + \bar{1}) \cdot \bar{k}_2 + \bar{1}] \cdot \bar{k} + \bar{k}_4 \}$  T. Repres.
5.  $\bar{k}_4 < (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2 + \bar{1}$  Expri. “<”
6.  $\bar{k}_1 = \{ [(\bar{k}_3 + \bar{1}) \cdot \bar{k}_2 + \bar{1}] \cdot \bar{k} + \bar{k}_4 \} \wedge$  4, 5  
 $\wedge [ \bar{k}_4 < (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2 + \bar{1} ]$
7.  $B(x_1, x_2, x_3, x_4)$
8.  $(\exists x_4) B(x_1, x_2, x_3, x_4)$  7,  $\exists$ -Int.
9.  $(\exists^1 x_4) B(x_1, x_2, x_3, x_4)$  8, T. Univoci. e Resto

Para concluir o tratamento elementar do raciocínio recursivo resta demonstrar que qualquer função recursiva é representável na linguagem Z. Uma função é recursiva se e somente se pode ser construída a partir das funções iniciais por um número finito de aplicações das Regras de Substituição, de Recursão e do Operador  $\mu$ .

Assim a demonstração do nosso teorema inclui uma demonstração de que as funções são representáveis em Z e de que as aplicações das regras de Substituição, Recursão e do Operador  $\mu$

conservam o conjunto das funções representáveis em  $Z$  como fechado a respeito destas aplicações.

Uma parte da nossa demonstração já foi feita no presente Capítulo, nomeadamente a parte que diz respeito à representabilidade das funções iniciais e da Regra da Substituição. Por demonstrar fica apenas que a Regra da Recursão e a Regra do Operador  $\mu$  conservam fechado o conjunto das funções representáveis em  $Z$ .

Começando pela Regra de Recursão, o nosso objectivo é demonstrar que se uma função

$$f(x_1, \dots, x_n, y)$$

é definida por recursão em  $y$  a partir das funções representáveis

$$g(x_1, \dots, x_n)$$

e

$$h[x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)]$$

então a função

$$f(x_1, \dots, x_n, y)$$

também é representável.

A concepção da demonstração consiste em conceber a função a representar

$$f(x_1, \dots, x_n, y) = z$$

como equivalente à asserção de existência de uma sucessão finita de números

$$a_0, \dots, a_n$$

construída da seguinte maneira:

- i)  $a_0 = g(x_1, \dots, x_n)$
- ii)  $a_{j+1} = h(x_1, \dots, x_n, j, a_j)$
- iii)  $a_n = z$ .

Pela Proposição 2 estas sucessões finitas de números naturais podem ser parafraseadas em termos de resultados do cálculo da função  $\beta$  de Gödel. E como a função  $\beta$  é representável em  $Z$ , a função  $f(x_1, \dots, x_n, y)$  também o é.

**Proposição 5.** [ *Fecho pela Regra da Recursão* ]

O conjunto  $R_Z$  das funções aritméticas representáveis em  $Z$   
é fechado a respeito da Regra da Recursão.

Dem.:

Começamos por definir a função

$$f(x_1, \dots, x_n, y) = z$$

por meio do seguinte sistema de equações:

$$(\diamond) \begin{cases} 1) f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n) \\ 2) f(x_1, \dots, x_n, y+1) = h[x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)]. \end{cases}$$

A nossa hipótese é que as funções

$$g(x_1, \dots, x_n)$$

e

$$h[x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)]$$

são  $\varphi$ -representáveis em  $Z$  por meio das fórmulas bem formadas

$$\alpha (x_1, \dots, x_{n+1})$$

e

$$\beta (x_1, \dots, x_{n+3}) .$$

Para proceder à representação da função

$$f(x_1, \dots, x_n, x_{n+1})$$

utilizaremos a fórmula bem formada

$$\Gamma (x_1, \dots, x_{n+2})$$

com a seguinte configuração:

$$\begin{aligned} (\heartsuit) \quad & (\exists u) (\exists v) \{ (\exists w) [ B(u, v, 0, w) \wedge \alpha(x_1, \dots, x_n, w) ] \} \wedge \\ & \wedge (\forall w) \{ w < x_{n+1} \rightarrow (\exists y) (\exists z) \{ [ B(u, v, w, y) \wedge \\ & \wedge B(u, v, N(w), z) ] \wedge B(u, v, x_{n+1}, x_{n+2}) \wedge \\ & \wedge \beta(x_1, \dots, x_n, w, y, z) \} \} . \end{aligned}$$

### Sinopse da demonstração:

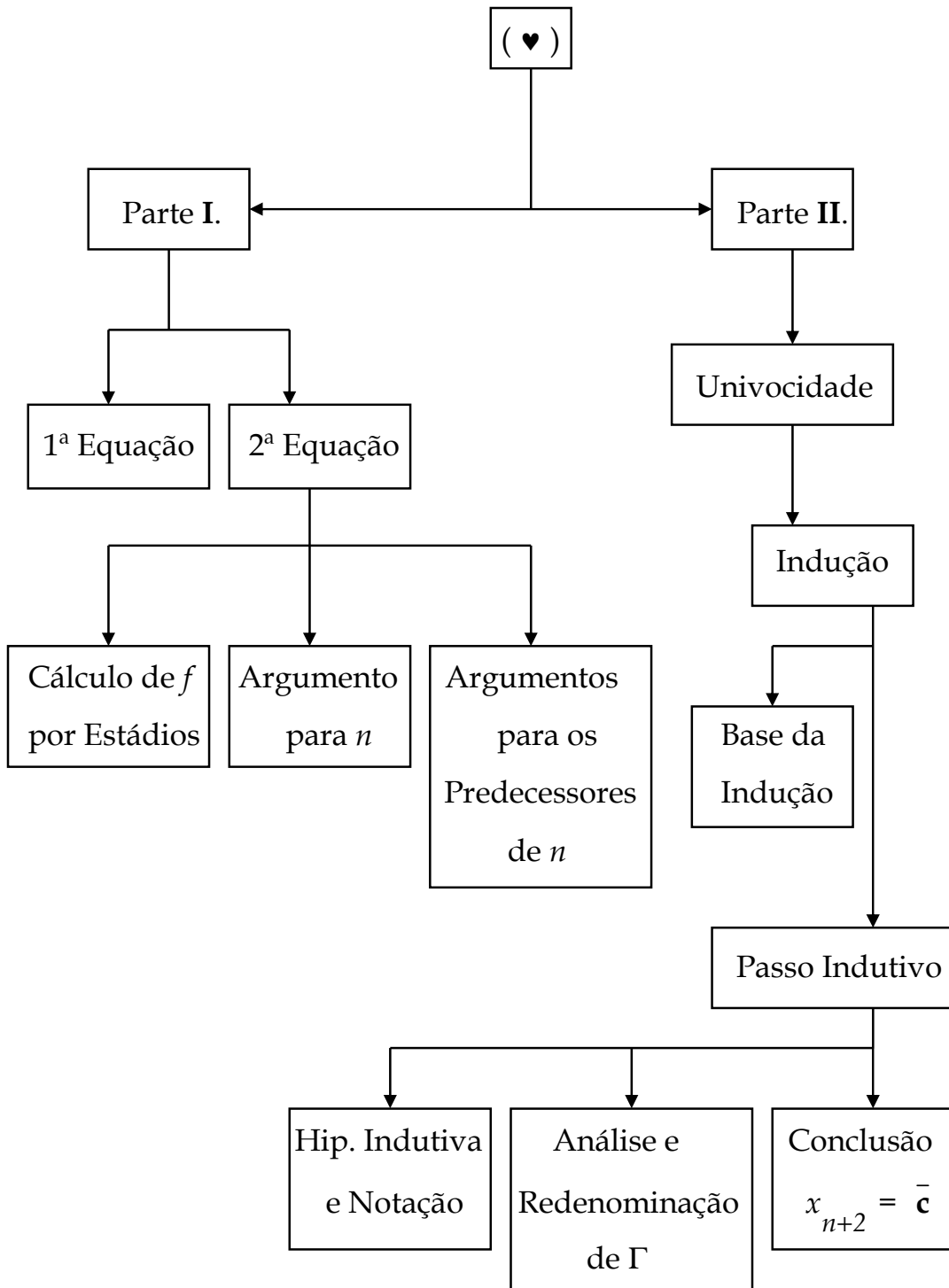
**Parte I.:** É satisfeita a primeira condição da Definição de Representabilidade.

**Parte II.:** É satisfeita a segunda condição da Definição de Representabilidade.

Como há duas equações a considerar na definição de

$$f(x_1, \dots, x_n, y) = z$$

a plano da demonstração é o seguinte:



Dem.: (**Parte I. 1.: Representabilidade da Fórmula (♥)**)

1.  $f(k_1, \dots, k_n, n) = m$  Hipótese
2.  $n = 0$  Hipótese
3.  $g(k_1, \dots, k_n) = m$  1, 2, Def. "g"
4.  $(\exists b)(\exists c) \beta(b, c, 0) = m$  Prop. 2
5.  $\vdash B(\bar{b}, \bar{c}, 0, \bar{m})$  4, Prop. 4
6.  $\vdash \alpha(\bar{k}_1, \dots, \bar{k}_n, \bar{m})$  3
7.  $\vdash B(\bar{b}, \bar{c}, 0, \bar{m}) \wedge \alpha(\bar{k}_1, \dots, \bar{k}_n, \bar{m})$  5, 6, C. Prop.
8.  $\vdash (\exists w) \{ B(\bar{b}, \bar{c}, 0, w) \wedge \alpha(\bar{k}_1, \dots, \bar{k}_n, w) \}$  7,  $\exists$ -Int.
9.  $(\exists u)(\exists v) \{ (\exists w) B(\bar{u}, \bar{v}, 0, w) \wedge \alpha(\bar{k}_1, \dots, \bar{k}_n, w) \}$  8,  $\exists$ -Int.
10.  $\Gamma(\bar{k}_1, \dots, \bar{k}_n, 0, \bar{m})$  9, Def. "Γ"

Dem.: (**Parte I. 2.: Representabilidade da Fórmula (♥)**)

Enquanto que na demonstração anterior considerámos  $n = 0$ , agora viramo-nos para o caso em que  $n > 0$ .

Crucial no argumento é a identificação dos estádios do cálculo da função

$$f(x_1, \dots, x_n, n),$$

por meio dos quais é determinado o valor genérico de  $n$ .

Dem.: (Parte I. 2.1: Cálculo de  $f$  por Estádios)

1. Se  $n > 0$   
então a função

$$f(k_1, \dots, k_n, n)$$

é calculada por meio das equações ( $\blacklozenge$ ) em  $n + 1$  estádios.

2. No estádio  $i$  o resultado do cálculo é

$$f(k_1, \dots, k_n, i) = a_i .$$

3. Formar a sucessão dos números

$$a_0, a_1, \dots, a_n .$$

4. Então existem os números  $b$  e  $c$  tais que

$$(\exists b) (\exists c) \beta(b, c, i) = a_i$$

em que o estádio  $i$  se encontra

$$0 \leq i \leq n .$$

5. Logo o resultado do cálculo no estádio  $i$  é representável em  $Z$  pela fórmula

$$\vdash B(\bar{b}, \bar{c}, \bar{i}, \bar{a}_i) .$$

6. Em particular para o primeiro estádio tem-se

$$\beta(b, c, 0) = a_0 .$$

7. Assim,

$$f(k_1, \dots, k_n, 0) = g(k_1, \dots, k_n) .$$

8. Este resultado é representável em  $Z$  pela fórmula

$$\vdash B(\bar{b}, \bar{c}, 0, \bar{a}_0) \wedge \alpha(\bar{k}_1, \dots, \bar{k}_n, \bar{a}_0) .$$

9. E assim, por  $\exists$ -Introdução,

$$(*) \quad (\exists w) \{ B(\bar{b}, \bar{c}, 0, w) \wedge \alpha(\bar{k}_1, \dots, \bar{k}_n, w) \} .$$

Dem.: (Parte I. 2.2.: *Argumento para n*)

1.  $f(k_1, \dots, k_n, n) = m .$

2. Então, pelo passo 2. (parte I. 2.1.) aplicado a  $n$ , tem-se que

$$f(k_1, \dots, k_n, n) = a_n .$$

3. Assim,

$$(\exists b) (\exists c) \beta(b, c, n) = m .$$

4. Esta fórmula é representável em  $Z$  por

$$(**) \quad B(\bar{b}, \bar{c}, \bar{n}, \bar{m}) .$$

5. Em geral tem-se para um estádio  $i$

$$0 \leq i \leq n - 1$$

que

$$\beta(b, c, i) = a_i .$$

6. E pelo passo 2. (parte I. 2.1.)

$$f(k_1, \dots, k_n, i) .$$

7. Ora

$$\beta(b, c, i + 1) = a_{i+1} .$$

8. Logo

$$f(k_1, \dots, k_n, i + 1) = a_{i+1} .$$

9. Assim,

$$\begin{aligned} f(k_1, \dots, k_n, i + 1) &= h [ k_1, \dots, k_n, i, f(k_1, \dots, k_n, i) ] = \\ &= h (k_1, \dots, k_n, i, a_i) . \end{aligned}$$

10. Este resultado é representável em  $Z$  pela fórmula

$$\begin{aligned} \vdash \quad & B(\bar{b}, \bar{c}, \bar{i}, \bar{a}_i) \wedge B(\bar{b}, \bar{c}, \overline{N(i)}, \overline{a_{i+1}}) \wedge \\ & \wedge \beta(\overline{k_1}, \dots, \overline{k_n}, \bar{i}, \bar{a}_i, \overline{a_{i+1}}) . \end{aligned}$$

11. Por  $\exists$ -Introdução

$$\vdash \quad (\exists y) (\exists z) \{ [ B(\bar{b}, \bar{c}, \bar{i}, y) \wedge B(\bar{b}, \bar{c}, \overline{N(i)}, z) ] \wedge$$

$$\wedge \beta (\bar{k}_1, \dots, \bar{k}_n, \bar{i}, y, z) \}.$$

Dem.: (Parte I. 2.3.: *Argumento para os Predecessores de n*)

1. Como já foi estabelecido no capítulo II,

$$\begin{aligned} \vdash & \quad [ \alpha (0) \wedge \alpha (1) \wedge \dots \wedge \alpha (\bar{k}-1) ] \leftrightarrow \\ & \leftrightarrow (\forall x) [ (x < \bar{k}) \rightarrow \alpha (x) ]. \end{aligned}$$

2. Assim, tem-se

$$\begin{aligned} (***) \quad (\forall w) \{ (w < \bar{n}) \rightarrow (\exists y) (\exists z) [ B (\bar{b}, \bar{c}, w, y) \wedge \\ \wedge B (\bar{b}, \bar{c}, N(w), z) \wedge \beta (\bar{k}_1, \dots, \bar{k}_n, w, y, z) ] \} \}. \end{aligned}$$

3. Formar a conjunção

$$(*) \wedge (**) \wedge (***) .$$

4. Aplicar  $\exists$ -Introdução duas vezes.

5.  $\vdash \Gamma (\bar{k}_1, \dots, \bar{k}, \bar{n}, \bar{m}) .$

Dem.: (**Parte II.:** *Univocidade*)

Nesta parte demonstraremos

$$\vdash (\exists^1 x_{n+2}) \Gamma (\bar{k}_1, \dots, \bar{k}_n, \bar{n}, x_{n+2}) .$$

A demonstração é feita por indução em  $n$  na metalinguagem.

Dem.: (Parte II. 1.: *Base da Indução (n = 0)*)

1.  $f(k_1, \dots, k_n, n) = m$

2.  $n = 0$

3.  $f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$

4.  $g(x_1, \dots, x_n) = m$

5.  $x_{n+2} = \overline{m}$
6.  $\vdash (\exists^1 x_{n+2}) \Gamma (k_1, \dots, k_n, 0, x_{n+2})$

Dem.: (Parte II. 2.1.: *Hipótese Indutiva e Notação* )

1. Supor

$$(\exists^1 x_{n+2}) \Gamma (\overline{k}_1, \dots, \overline{k}_n, \overline{n}, x_{n+2}).$$

2. O resultado do cálculo das funções  $g$  e  $f$  será representado por

$$\mathbf{a} = g(k_1, \dots, k_n)$$

$$\mathbf{b} = f(k_1, \dots, k_n, n)$$

$$\mathbf{c} = f(k_1, \dots, k_n, n + 1).$$

3. Então o número  $\mathbf{c}$  pode ser representado pela equação

$$\mathbf{c} = h [ k_1, \dots, k_n, n, f(k_1, \dots, k_n, n) ].$$

4. Logo, pelo passo 2.,

$$\mathbf{c} = h (k_1, \dots, k_n, n, \mathbf{b}).$$

5. Logo, este valor é representável por

$$\vdash \beta (\overline{k}_1, \dots, \overline{k}_n, \overline{n}, \overline{\mathbf{b}}, \overline{\mathbf{c}}).$$

6. O valor de  $g$ , por sua vez, é representado por

$$\vdash \alpha (\overline{k}_1, \dots, \overline{k}_n, \overline{\mathbf{a}}).$$

7. Então para a fórmula  $\Gamma$  tem-se no ponto  $n$

$$\vdash \Gamma (\overline{k}_1, \dots, \overline{k}_n, \overline{n}, \overline{\mathbf{b}}).$$

8. Finalmente para o sucessor de  $n$

$$\vdash \Gamma (\overline{k}_1, \dots, \overline{k}_n, \overline{n+1}, \overline{\mathbf{c}}).$$

Dem.: (Parte II. 2.2.: *Análise e Redenominação de  $\Gamma$* )

1. Suponhamos que se designa por  $x_{n+2}$  o resultado no estágio

$n + 2$  a ser representado pela fórmula

$$\Gamma (\overline{k_1}, \dots, \overline{k_n}, \overline{n+1}, \overline{x_{n+2}}).$$

2. Temos assim que demonstrar que  $x_{n+2}$  é representado pelo

numeral  $\overline{c}$  e assim,

$$x_{n+2} = \overline{c}.$$

3. Mas pela Hipótese 1. já se pode concluir

$$(\exists w) [ B (b, c, 0, w) \wedge \alpha (\overline{k_1}, \dots, \overline{k_n}, w) ].$$

4. Em particular tem-se para  $n + 1$

$$B (b, c, \overline{n+1}, x_{n+2}).$$

5. Então resulta ainda da Hipótese 1. que

$$(\forall w) \{ (w < \overline{n+1}) \rightarrow (\exists y) (\exists z) [ B (b, c, w, y) \wedge \\ \wedge B (b, c, N (w), z) \wedge \beta (\overline{k_1}, \dots, \overline{k_n}, w, y, z) ] \}.$$

6. Logo, para os predecessores de  $n$

$$(\forall w) \{ (w < n) \rightarrow (\exists y) (\exists z) [ B (b, c, w, y) \wedge \\ \wedge B (b, c, N (w), z) \wedge \beta (\overline{k_1}, \dots, \overline{k_n}, w, y, z) ] \}.$$

7. Então o Passo 5.,  $\forall$ -Elim. e a  $\exists$ -Elim. dão-nos a fórmula

$$B (b, c, \overline{n}, d) \wedge B (b, c, \overline{n+1}, e) \wedge \beta (\overline{k_1}, \dots, \overline{k_n}, n, d, e).$$

Dem.: (Parte II. 2.3.: *Conclusão:  $x_{n+2} = \overline{c}$* )

1.  $\Gamma (\overline{k_1}, \dots, \overline{k_n}, \overline{n}, d)$

Parte II. 2.2 – passos: 3, 6, 7

- |    |   |                              |
|----|---|------------------------------|
| 2. | $d = \bar{\mathbf{b}}$  | 1, Parte II. 2.1. - passo: 7 |
| 3. | $\beta (\overline{k_1}, \dots, \overline{k_n}, \bar{n}, \bar{\mathbf{b}}, e)$ | Parte II. 2.2 - passo: 7     |
| 4. | $\bar{\mathbf{c}} = e$  | Parte II. 2.1. - passo: 5    |
| 5. | $B (\mathbf{b}, \mathbf{c}, \overline{n+1}, \bar{\mathbf{c}})$                | Parte II. 2.2. - passo: 7    |
| 6. | $x_{n+2} = \bar{\mathbf{c}}$  | Parte II. 2.2. - passo: 4    |

Resta-nos demonstrar que o conjunto das funções representáveis em  $Z$  é fechado a respeito da Regra do Operador  $\mu$ . O argumento é que se a função a representar

$$f(x_1, \dots, x_n)$$

é calculada em termos de uma função representável por meio do Operador  $\mu$ , então também é representável. A função representável é a função

$$g(x_1, \dots, x_n, y)$$

e para o menor dos seus zeros usamos a notação da Secção 1 do Capítulo I

$$\mu y [g(x_1, \dots, x_n, y) = 0].$$

**Proposição 6.**      [ *Fecho pela Regra do Operador  $\mu$*  ]

*O conjunto  $R_Z$  das funções representáveis em  $Z$*

*é fechado a respeito da Regra do Operador  $\mu$ .*

Dem.:

A fim de satisfazer a definição de representabilidade, a demonstração decorre em duas partes. Mas antes de a realizar é útil considerar o seguinte:

1. A nossa hipótese é a da existência dos zeros da função  $g$  sob a forma

$$(\forall x_1, \dots, x_n) (\exists y) [ g(x_1, \dots, x_n, y) = 0 ] .$$

2. A representação de  $g$  em  $Z$  supõe-se ser realizada pela fórmula bem formada

$$\Delta(x_1, \dots, x_{n+2}) .$$

3. Seja agora

$$f(x_1, \dots, x_n) = \mu y [ g(x_1, \dots, x_n, y) = 0 ] .$$

4. Então diremos que  $f$  é representável em  $Z$  pela fórmula bem formada

$$\Phi(x_1, \dots, x_{n+1})$$

com a seguinte configuração:

$$\{ \Delta(x_1, \dots, x_{n+1}, 0) \wedge (\forall y) [ (y < x_{n+1}) \rightarrow \rightarrow \neg \Delta(x_1, \dots, x_n, y, 0) ] \} .$$

Dem.: (Parte I.: Representabilidade de  $\Phi(x_1, \dots, x_{n+1})$ )

- |    |   |             |
|----|---|-------------|
| 1. | $f(k_1, \dots, k_n) = m$  | Hipótese    |
| 2. | $g(k_1, \dots, k_n, m) = 0$   | Hip. 3, 1   |
| 3. | $(k < m) \rightarrow g(k_1, \dots, k_n, k) \neq 0$                      | 2, Def. "<" |
| 4. | $\vdash \Delta(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$ | 2           |

5.  $\vdash (k < m) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, \bar{k}, 0)$  3
6.  $\vdash (\forall y) [(y < \bar{m}) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, y, 0)]$  5,  $\forall$ -Int.
7.  $\vdash \Delta(\bar{k}_1, \dots, \bar{k}_n, \bar{m}, 0) \wedge$   
 $\wedge (\forall y) [(y < \bar{m}) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, y, 0)]$  4, 6,  $\wedge$ -Int.
8.  $\vdash \varphi(x_1, \dots, x_{n+1})$  7, Def. "Δ"

Dem.: (Parte II.: *Univocidade*)

Nesta parte estabeleceremos

$$(\exists^1 x_{n+1}) \varphi(\bar{k}_1, \dots, \bar{k}_n, x_{n+1}).$$

[ *Reductio* ]

1.  $\Delta(\bar{k}_1, \dots, \bar{k}_n, z_1, 0) \wedge$   
 $\wedge (\forall y) [(y < z_1) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, y, 0)]$  Hip.
2.  $\Delta(\bar{k}_1, \dots, \bar{k}_n, z_2, 0) \wedge$   
 $\wedge (\forall y) [(y < z_2) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, y, 0)]$  Hip.
3.  $\vdash (z_1 = z_2) \vee (z_1 < z_2) \vee (z_2 < z_1)$  Cap. II
4.  $z_2 < z_1$  Hip.
5.  $(z_2 < z_1) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, z_2, 0)$  1,  $\forall$ -Elim.
6.  $\neg \Delta(\bar{k}_1, \dots, \bar{k}_n, z_2, 0)$  4, 5, MP
7.  $\Delta(\bar{k}_1, \dots, \bar{k}_n, z_2, 0)$  2,  $\wedge$ -Elim.
8.  $z_1 < z_2$  Hip.

9.  $(z_1 < z_2) \rightarrow \neg \Delta(\bar{k}_1, \dots, \bar{k}_n, z_1, 0)$  2,  $\forall$ -Elim.
10.  $\neg \Delta(\bar{k}_1, \dots, \bar{k}_n, z_1, 0)$  8, 9, MP
11.  $\Delta(\bar{k}_1, \dots, \bar{k}_n, z_1, 0)$  1,  $\wedge$ -Elim.
12.  $z_1 = z_2$  3, 11, RAA

Uma consequência associada às Proposições 5 e 6 é a da *expressibilidade* de qualquer relação ou predicado recursivo na Linguagem Z. Esse é o conteúdo da nossa última demonstração.

**Proposição 7.** [ *Expressibilidade em Z* ]

*Qualquer relação recursiva*

$$R(x_1, \dots, x_n)$$

*é exprimível em Z.*

Dem.:

1. Seja
 
$$R(x_1, \dots, x_n)$$
 um predicado ou uma relação recursiva.
2. Então a sua função característica 1, Def. 4 (Cap. I, Sec. 4)
 
$$K_R$$
 é uma função recursiva.
3. Então a função  $K_R$  é representável em Z. 2, Prop. 4
4. Logo Cap. III ( $R$  é exprimível  $\leftrightarrow$ 

$$R(x_1, \dots, x_n) \leftrightarrow K_R \text{ é representável}$$
)

é exprimível em  $Z$ .

SUMÁRIO  
DO CAPÍTULO III

As relações e funções aritméticas têm o domínio e o contra-domínio nos números naturais.

As relações aritméticas são (numeralmente) exprimíveis em  $Z$  através de fórmulas bem formadas demonstráveis em  $Z$ . As funções aritméticas são (numeralmente) representáveis e  $\varphi$ -representáveis em  $Z$  por meio de fórmulas que denotam o valor e a univocidade do valor da função. As funções iniciais Zero, Sucessor e Identidade são assim representáveis. Uma função obtida de funções  $\varphi$ -representáveis através da regra da substituição é  $\varphi$ -representável. A função Característica de uma Relação  $R$  tem o valor 0 se  $R$  é verdadeira e 1 se é falsa. A expressão de uma relação em  $R$  é equivalente à  $\varphi$ -representação da função Característica de  $R$ . Para a representação de qualquer função recursiva em  $Z$  é necessário usar conceitos e notação da teoria da congruência de Gauss. Nos axiomas para o Anel Comutativo  $\langle \mathbb{Z}_n, +, \times \rangle$  a Identidade Aditiva *mod*  $n$  é  $[0]_n$  e o inverso de  $[a]_n$  é  $[-a]_n$ . A Identidade Multiplicativa *mod*  $n$  é  $[1]_{-n}$ . É demonstrada a existência de um Inverso Multiplicativo num *modulo* e que existe uma solução comum para congruências simultâneas em módulos que são entre si primos relativos.

A sucessão de Gödel é constituída por termos com a forma geral  $(k + 1) \cdot l + 1$  e a função  $\beta$  calcula o resto da divisão de um número  $m$

por um termo da sucessão. Esta função é recursiva,  $\varphi$ -representável e permite a representação de sucessões de números naturais. Com esta representação demonstra-se a representabilidade de qualquer função recursiva e, em particular, que recursão implica expressão em  $Z$ .