

<sup>1</sup> **HOLISMO:****O SENTIDO ESTÁ NA FUNÇÃO-AMBIENTE -  
QUAIS SÃO OS DOIS ÚLTIMOS DÍGITOS DE  $3^{283}$ ?****I. [ NOTAÇÃO POSICIONAL ]**

É útil começar por tirar partido da diferença entre um elemento de  $\mathbb{Z}$  e o símbolo usado para o representar, o numeral, visto que o mesmo elemento pode ser representado por símbolos diferentes, por numerais árabes, romanos, gregos, etc.

No sistema decimal os dígitos 0, 1, 2, ..., 9 são usados para os primeiros nove elementos de  $\mathbb{Z}^+$ . E assim um número inteiro, como *duzentos e vinte e dois*, pode ser representado como

$$200 + 20 + 2$$

*i.e.*

$$2 \cdot 10^2 + 2 \cdot 10 + 2$$

e esta expressão é, *no sistema decimal*, codificada na expressão simbólica 222.

O ponto crucial é que um símbolo individual como 2 não é um nome, não tem sentido isoladamente, desligado do papel que desempenha na função-ambiente em que ocorre. O seu sentido depende do seu local de acção: nas unidades, ou nas dezenas ou nas centenas.

---

<sup>1</sup> Lourenço, M.S.: 2006, Julho.

Numa *notação posicional* qualquer inteiro pode ser representado por meio de diversas combinações dos 10 símbolos 0, 1, ..., 9. Em geral numa fórmula como

$$x = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d$$

os símbolos  $a, b, c, d$  chamam-se *os coeficientes* e são os inteiros de 0 a 9. Assim  $x$  pode ser codificado na abreviatura

$$a \ b \ c \ d.$$

Estes coeficientes, na ordem  $d, c, b, a$  são os restos deixados nas sucessivas divisões de  $x$  por 10. (Exemplo: 1984 deixa 4 como resto na 1ª divisão por 10, deixa 8 na segunda, etc.).

Para representar estes factos com a devida generalidade adaptamos a notação, de modo a representar os coeficientes com uma única letra com índice e as diversas potências descendentes de 10 a partir de  $n$ .

Assim a fórmula a que se é conduzido é

$$x = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0.$$

A abreviatura que codifica  $x$  será então

$$a_n \ a_{n-1} \ a_{n-2} \ \dots \ a_1 \ a_0.$$

Os números  $a_n, \dots, a_0$  são os restos deixados por  $x$  nas sucessivas divisões por 10.

Esta forma de representação é independente do sistema decimal, *i. e.*, da escolha de 10 como base. Pode-se adoptar, p. ex., um sistema *octimal* (de base 8). No sistema octimal um inteiro  $x$  é representado por

$$k_n \cdot 8^n + k_{n-1} \cdot 8^{n-1} + \dots + k_1 \cdot 8 + k_0.$$

Os coeficientes  $k$  são os números de 0 a 7 e  $x$  é codificado na abreviatura

$$k_n k_{n-1} \dots k_1 k_0.$$

Ex.: o número 123 no sistema decimal seria denotado no sistema octimal por

$$1 \cdot 8^2 + 7 \cdot 8 + 3.$$

É fácil de verificar que a sua abreviatura, 173, reúne os restos das divisões sucessivas de 123 por 8.

Leibniz considerava que o sistema diádico, cujos únicos dígitos são 0 e 1, era uma imagem da Criação, em que 1 representa Deus e 0 representa o vazio. E assim como Deus criou todos os seres a partir do vazio, assim também 0 e 1 representam todos os números.

Qualquer número  $x$  é representado por uma sucessão destes dois símbolos. A adição e a multiplicação têm as seguintes tabelas:

$$1 + 1 = 10 \quad \text{e} \quad 1 \cdot 1 = 1.$$

Assim para representar em notação diádica o número cuja notação decimal é 79 o polinómio a que se é conduzido é:

$$2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

O seu código diádico é 1 0 0 1 1 1 1.

As multiplicações no sistema binário são especialmente simples.

**Exemplo:**

$7 \cdot 5 = 35$  terá a seguinte configuração:

$$\begin{array}{r}
 1\ 1\ 1 \\
 1\ 0\ 1 \\
 \hline
 1\ 1\ 1 \\
 0\ 0\ 0 \\
 1\ 1\ 1 \\
 \hline
 1\ 0\ 0\ 0\ 1\ 1
 \end{array}$$

Mas este número é justamente 35 em notação decimal.

### Exercícios:

- i) Escrever a tabela da adição na base 5.
- ii) Qual é a notação diádica do número cuja notação decimal é 222?
- iii) Qual é a notação decimal do número cuja notação de base 5 é 1 1 1 1 1?

Mais interessante ainda é constatar que o local de acção informa sobre o conteúdo. Exemplo: quais são *os dois últimos* dígitos do número

$$3^{283} ?$$

Um mínimo de teoria é necessário para se apreciar o problema e a sua solução. A ideia básica é proceder a uma generalização do pequeno teorema de Fermat e a aplicação segue-se imediatamente.

## II. [ PARA A GENERALIZAÇÃO DE FERMAT ]

**Definição 1** [ A Função  $\varphi$  de Euler ]

O número de elementos em  $\mathbb{Z}_n^*$ ,  
que se denota por  
 $\varphi(n)$ ,  
é igual ao número de inteiros entre  
 $1, \dots, n$  (inclusive)  
que são primos relativos com  $n$ .

**Exemplo 1:**

Se  $n = 25$ , qual é o valor de  $\varphi(n)$ ?

1, 2, 3, 4, 5,

6, 7, 8, 9, 10,

11, 12, 13, 14, 15,

16, 17, 18, 19, 20,

21, 22, 23, 24, 25.

1. Os únicos inteiros entre 1 e 25 ( $=5^2$ ) que têm um factor em comum com  $5^2$  são aqueles inteiros que são divisíveis por 5.

2. Eles são precisamente:

$$(*) \quad 1 \cdot 5 = 5,$$

$$2 \cdot 5 = 10,$$

$$3 \cdot 5 = 15,$$

$$4 \cdot 5 = 20,$$

$$5 \cdot 5 = 25 = 5^2$$

$$\text{e } 5^2 = 5^{2-1} \cdot 5.$$

3. Logo há em (\*)  $5^{2-1} = 5$  números que são divisíveis por 5.

4. Assim em (\*) há

$$5^2 - 5^{2-1} = 20$$

números que *não* são divisíveis por 5.

5. Estes 20 números são primos relativos com 25 ( $=5^2$ ) e logo são o valor de  $\varphi(5^2)$ .

### **Teorema 1** [ A Função de Euler ]

Se  $p$  é primo e  $n \in \mathbb{Z}^+$

então

$$\varphi(p^n) = p^n - p^{n-1}.$$

#### **Demonstração:**

1. Os únicos inteiros entre 1 e  $p^n$  que têm um factor em comum com  $p^n$  são aqueles inteiros que são divisíveis por  $p$ .

2. Eles são:

$$1 \cdot p = p,$$

$$2 \cdot p,$$

$$3 \cdot p,$$

...

$$p \cdot p = p^2,$$

$$p^2 \cdot p = p^3$$

...

$$p^{n-1} \cdot p = p^n.$$

3. Assim existem  $p^{n-1}$  números nesta sucessão que são divisíveis por  $p$ .

4. Logo entre 1 e  $p^n$  existem

$$p^n - p^{n-1}$$

números que não são divisíveis por  $p$ .

5. Então são primos relativos com  $p^n$  e portanto o valor de

$$\varphi(p^n).$$

### Exemplos:

1. 1, 2, 3, 4, 5.

Determinar o valor de  $\varphi(5)$ .

$$\begin{aligned}\varphi(5) &= 5^1 - 5^{1-1} \\ &= 5 - 5^0 \\ &= 5 - 1 \\ &= 4.\end{aligned}$$

2. 1, 2, 3, 4.

$$\begin{aligned}\varphi(4) &= \varphi(2^2) \\ &= 2^2 - 2^1 \\ &= 4 - 2 \\ &= 2.\end{aligned}$$

### Lema 1

Se  $a$  e  $b$  são números naturais e  $(a \neq 0)$

então com  $k \in \mathbb{Z}^+$  e  $r \in \mathbb{Z}^+$ ,

$$(b = a \cdot k + r) \rightarrow (b, a) = (a, r).$$

**Demonstração** (Parte I.):

1. Seja  $\delta = (a, b)$ .
2. Então  $\delta \mid a \wedge \delta \mid b$ .
3.  $r = b - a \cdot k$ .
4. Logo  $\delta \mid b - a \cdot k$ , o que implica que

$$\delta \mid r.$$

5. Assim  $\delta$  é um divisor comum de  $a$  por 2. e de  $r$  por 4.
6. Logo  $\delta \mid (a, r)$ .

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

1.  $b = a \cdot k + r$ .
2.  $(a, r) \mid a \wedge (a, r) \mid r$ .

o que implica que

$$(a, r) \mid b.$$

3. Assim  $(a, r)$  é um divisor comum de  $a$  por 2. e de  $b$  também por 2.
4. Então  $(a, r)$  divide  $(a, b)$  o que implica que

$$(a, r) \text{ divide } \delta.$$

**Dem.** (*Parte III.:*)

1. Então  $d \mid (a, r)$  e  $(a, r) \mid d$ .
2. Pela anti-simetria da relação " $\mid$ "  $\delta = (a, r)$ .
3. Logo  $(a, b) = (a, r)$ .

## Teorema 2

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

**Demonstração** (*Parte I.: Existência de  $\mathbb{Z}_{a \cdot b}^*$* )

1.  $[m]_a$  e  $[n]_b$  são elementos de, respectivamente,

$$\mathbb{Z}_a^* \text{ e } \mathbb{Z}_b^*.$$

2. Se os elementos  $[m]_a$  e  $[n]_b$  são dados, então podemos definir um elemento

$$[x]_{a \cdot b}$$

em  $\mathbb{Z}_{a \cdot b}^*$ .

3. Para provar

$$[x]_{a \cdot b} \in \mathbb{Z}_{a \cdot b}^*$$

é suficiente provar que  $[x]_{a \cdot b}$  tem um inverso multiplicativo modulo  $a \cdot b$ .

4. Como a hipótese do teorema garante que  $a$  e  $b$  são primos relativos, o *Teorema das Congruências Simultâneas* (Prop. 20 em *EPH*) assegura a existência de um único inteiro  $x$  que é a solução das congruências simultâneas

$$x \equiv m \pmod{a}$$

$$x \equiv n \pmod{b}.$$

5. Em particular  $x$  é único até à congruência modulo  $a \cdot b$ .
6. Então para provar que  $[x]_{a \cdot b}$  tem um inverso começamos por representar  $m$  como a combinação linear

$$m = a \cdot k + x.$$

7. Assim  $a$  não divide  $m$  e portanto

$$\{(m, a) = 1\}.$$

8. Mas  $m = a \cdot k + x$  implica pelo Lema que

$$(m, a) = (a, x).$$

9. Logo  $\{(a, x) = 1\}$ .

10. Para  $n$  também se tem a representação

$$n = b \cdot k + x$$

e com o mesmo argumento de 6. tem-se

$$\{(b, x) = 1\}.$$

11. Logo pelo Teorema de Euclides

$$\{(a, c) = 1\} \wedge \{(b, c) = 1\} \rightarrow \{(a \cdot b, c) = 1\}$$

tem-se

$$\{(a, x) = 1\} \wedge \{(b, x) = 1\} \rightarrow \{(a \cdot b, x) = 1\},$$

e, pelos passos 6. e 8., tem-se

$$\{(a \cdot b, x) = 1\}.$$

12. Logo  $x$  e  $a \cdot b$  são primos relativos e a Prop. 5 de *EPH* assegura que  $x$  tem um inverso multiplicativo mod  $a \cdot b$ .

Dem. (*Parte II.: A Bijecção  $f$* )

1. Vamos definir uma bijecção

$$f : \mathbb{Z}_{a \cdot b}^* \rightarrow [A]_a \times [B]_b$$

em que o codomínio  $[A]_a \times [B]_b$  denota o produto cartesiano das duas classes:

$$[A]_a \times [B]_b = \{ \langle [m]_a, [n]_b \rangle : [m]_a \in \mathbb{Z}_{a \cdot b}^* \wedge [n]_b \in \mathbb{Z}_{a \cdot b}^* \}.$$

Assim  $(\forall x)(x \in \mathbb{Z}_{a \cdot b}^*) f(x) = \langle [m]_a, [n]_b \rangle$

i. e.,  $f$  faz corresponder a qualquer elemento  $[x]_{a \cdot b}$  um par

$$\langle [m]_a, [n]_b \rangle.$$

2. Seja  $[x]_{a \cdot b}$  um elemento de  $\mathbb{Z}_{a \cdot b}^*$

e seja  $m$  o representante padrão de  $[x]_{a \cdot b}$ .

3. De  $\{ (x, a \cdot b) = 1 \}$  deduz-se  $\{ (x, a) = 1 \}$ .

4. Como se tem para  $x$  a representação

$$x = k \cdot a + m$$

então  $\{ (m, a) = 1 \}$ .

5. Então  $[m]_a \in \mathbb{Z}_a^*$ .

6. Repetindo o mesmo argumento para  $n$  obtém-se

$$[n]_b \in \mathbb{Z}_b^*.$$

7. Assim a cada elemento  $[x]_{a \cdot b}$  corresponde um único par

$$\langle [m]_a, [n]_b \rangle$$

em que

$$x \equiv m \pmod{a}$$

$$x \equiv n \pmod{b}.$$

8. Como  $x$  é único até à congruência modulo  $a \cdot b$  tem-se que a elementos diferentes correspondem pares diferentes.

9.  $f$  tem uma inversão  $f^{-1}$  visto que a qualquer par

$$\langle [m]_a, [n]_b \rangle$$

também corresponde um único elemento  $[x]_{a \cdot b}$ .

**Dem.** (*Parte III.:*)

1. Assim  $\mathbb{Z}_{a \cdot b}^*$  e  $[A]_a \times [B]_b$  são equicardinais.
2. Mas em  $\mathbb{Z}_{a \cdot b}^*$  existem  $\varphi(a \cdot b)$  elementos e em

$$[A]_a \times [B]_b$$

existem  $\varphi(a) \cdot \varphi(b)$  elementos, uma vez que o cardinal do produto cartesiano é igual ao produto dos cardinais dos factores.

3. Logo por 1.

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

**Exemplos:**

1.  $\varphi(100)$ .

Como  $100 = 2^2 \cdot 5^2$ , o teorema permite calcular  $\varphi(4 \cdot 25)$  como  $\varphi(4) \cdot \varphi(25)$ . Assim  $\varphi(100) = 2 \cdot 20$ .

2. Calcular  $\varphi(14)$  e  $\varphi(17)$ .

### III. [ EXTRAIR INFORMAÇÃO DA POSIÇÃO ]

**Teorema 3** [ *Teorema de Euler* ]

*As duas Formulações Equivalentes :*

$$I. \quad n \geq 2 \wedge \{(x, n) = 1\} \rightarrow [x]_n \wedge \varphi(n) = [1]_n.$$

$$II. \quad x^{\varphi(n)} \equiv 1 \pmod{n}.$$

**Demonstração** (*Parte I.:*)

1.  $\mathbb{Z}_n^*$  = conjunto dos elementos de  $\mathbb{Z}_n$  que têm inversos.
2. Definir uma permutação  $\pi$  sobre  $\mathbb{Z}_n^*$  cujo efeito é formar o conjunto de todos os múltiplos de  $\mathbb{Z}_n^*$  por meio da multiplicação

$$[x] \cdot \mathbb{Z}_n^*.$$

3. Assim  $[x] \cdot \mathbb{Z}_n^* = \{[x] \cdot [y] : [y] \in \mathbb{Z}_n^*\}$ .
  4. Como  $[x] \in \mathbb{Z}_n^*$  tem-se que qualquer elemento em  $[x] \cdot \mathbb{Z}_n^*$  também é elemento de  $\mathbb{Z}_n^*$  e reciprocamente.
  5. Finalmente  $\pi$  é uma bijecção em  $\mathbb{Z}_n^*$ .
- i) Se  $[y] \neq [z]$ , a fórmula

$$(*) \quad [x] \cdot [y] = [x] \cdot [z]$$

é falsa uma vez que o Teorema da Cancelação aplicado à fórmula (\*) permitiria derivar  $[y] = [z]$ .

ii) Como todos os elementos de  $\mathbb{Z}_n^*$  são imagens,  $\pi$  é uma sobrejecção.

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

1. Os conjuntos  $[x] \cdot \mathbb{Z}_n^*$  e  $\mathbb{Z}_n^*$  têm assim o mesmo número de elementos.
2. Logo

$$[x] \cdot \mathbb{Z}_n^* = \mathbb{Z}_n^*.$$

3. Seja  $\langle \Pi(\mathbb{Z}_n^*), \circ \rangle$  o Grupo formado pelo conjunto de todas as permutações em  $\mathbb{Z}_n^*$  sob Composição. Pode-se definir então

um novo elemento  $[\xi]$ , que depende de  $\mathbb{Z}_n^*$  e que é o número de elementos em  $\Pi(\mathbb{Z}_n^*)$ , i. e.,

$$[\xi] = \mathbb{Z}_n^*!.$$

4. Como  $\mathbb{Z}_n^*$  é fechado sob multiplicação

$$[\xi] \in \mathbb{Z}_n^*.$$

5. A bijecção implica

$$[x] \cdot \mathbb{Z}_n^* = [\xi].$$

6. Assim

$$[1] \cdot [2] \cdot \dots \cdot [n] = [x] \cdot [1] \cdot [x] \cdot [2] \cdot \dots \cdot [x] \cdot [n].$$

7. Como em  $1, \dots, n$   $[x]$  tem  $\varphi(n)$  ocorrências a fórmula 6. tem a reformulação

$$[\xi] = [x]^{\varphi(n)}.$$

8. Mas por 4.  $[\xi]$  tem um inverso,  $[\xi]^{-1}$ .

9. Logo por 7.

$$[\xi]^{-1} \cdot [\xi] = [x]^{\varphi(n)}.$$

10.  $1 = [x]^{\varphi(n)}$ .

11.  $x^{\varphi(n)} = 1 \pmod{n}$ .

### Exemplos:

I. Calcular o valor  $y$  da congruência

$$[3^{17}]_{16} \equiv y.$$

1. Pelo Teorema de Euler, com  $x = 3$  e  $n = 16$ , tem-se

$$3^{\varphi(16)} \equiv 1 \pmod{16}.$$

2.  $\varphi(16) = \varphi(2) \cdot \varphi(8) = 1 \cdot 4 = 4.$
3.  $3^4 \equiv 1 \pmod{16},$  por 1. e 2.
4.  $[(3)^4]^4 \cdot 3 \equiv 3^{17}.$
5.  $1^4 \cdot 3 \equiv 3^{17}.$
6.  $3 \equiv 3^{17} \pmod{16}.$
7.  $y = [3]_{16}.$

[ **N. B.** ]

A restrição no antecedente do teorema tem o seguinte *rationale*:

Ex.:

Se  $x = 2$  e  $n = 16$

então  $2^{\varphi(16)} \equiv 1 \pmod{16}.$

Como  $\varphi(16) = \varphi(8) \cdot \varphi(2) = 4 \cdot 1 = 4.$

Então  $2^4 \equiv 1 \pmod{16}.$

II. (Continuação dos exemplos.)

Quais são os dois últimos dígitos do número  $3^{283}$  ?

1. No sistema decimal um número, como por ex. 1984, tem uma representação polinômica canónica

$$1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10^1 + 4 \cdot 10^0.$$

em que os dígitos 1, 9, 8 e 4 são os coeficientes das diversas potências  $10^3, 10^2, 10^1, 10^0.$

2. Em particular aqueles dígitos representam os restos das divisões sucessivas de 1984 por 10. Assim

$$1984 = 198 \cdot 10 + 4,$$

$$198 = 19 \cdot 10 + 8,$$

$$19 = 10 \cdot 1 + 9$$

e assim 4 é o coeficiente de  $10^0$ , o resto da divisão de 1984 pela primeira vez, 8 é o resto da divisão pela 2ª vez, *etc.*, agora pela ordem 4, 8, 9, 1.

3. Isto significa que os dois últimos dígitos de um número  $n \in \mathbb{Z}^+$  são a sua classe de congruência mod  $10 \cdot 10 = 100$ .

4. Pelo Teorema de Euler, inserindo 3 em  $x$  e 100 em  $n$ ,

$$3^{\varphi(n)} \equiv 1 \pmod{100}.$$

5. Mas  $\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 40$ .

6. Logo  $3^{283} = (3^{40})^7 \cdot 3^3$ .

7.  $3^{283} = 1 \cdot 3^3 = 27$

8.  $3^{283} \equiv 27 \pmod{100}$

o que significa que os dois últimos dígitos do número  $3^{283}$  são 27.