

**EULER****E O ABSTRACCIONISMO**<sup>1</sup>

*Dégager les hypothèses utiles* (Abstracção). Aqui trata-se de questões como: *O que* é necessário para afirmar  $A$ ? ou – ao contrário da Lógica e na Matemática mais usual – *O que* é que se utiliza na demonstração de  $A$ ? N.B. A escolha dos conceitos, a qual tem que descrever aquele *o que*, pertence à resposta e em geral não é dada com a pergunta. Quem formou uma opinião sobre a resposta pergunta se – ou antes conjectura que – é válida para  $A$  uma generalização correspondente; por exemplo, se  $A$  afirma que nos inteiros  $n^2 - m^2 = (n + m) \cdot (n - m)$ , então utiliza-se apenas a comutatividade do Anel. Para leitores *blásés*:  $2^{p-1} \equiv 1 \pmod{p}$  foi demonstrado por Euler de modo a utilizar-se apenas propriedades de grupos comutativos finitos.

GEORG KREISEL

---

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

## I. O CONCEITO DE ORDEM MULTIPLICATIVA

[ N.B.

i) **Notação:**

O *expoente* de uma classe de congruência tem a notação

$$[x]^p.$$

O *índice* de uma classe de congruência denota o módulo e será omitido quando o módulo é conhecido.

ii) **Background:**

Para notação, terminologia e definições ver

Cap. III de “Os Elementos do Programa de Hilbert”. ]

A sucessão dos primeiros  $n$  elementos das potências de uma classe de congruência módulo 20 tem a forma:

$$[x],[x]^2,[x]^3,\dots,[x]^n.$$

**Exemplo 1:**

$$x = 3.$$

Os primeiros 9 elementos são:

$$[3]=[3]$$

$$[3]^2=[9]$$

$$[3]^3=[27]=[7]$$

$$[3]^4=[3]^3 \times [3]=[7] \times [3]=[21]=[1]$$

$$[3]^5=[3]^4 \times [3]=[1] \times [3]=[3]$$

$$[3]^6=[3]^5 \times [3]=[3] \times [3]=[9]$$

$$[3]^7 = [3]^6 \times [3] = [9] \times [3] = [27] = [7]$$

$$[3]^8 = [3]^7 \times [3] = [1]$$

$$[3]^9 = [3]^8 \times [3] = [3]$$

Assim as potências de  $[3] \bmod 20$  organizam-se num **padrão recorrente P1** com a distribuição:

$$[3], [9], [7], [1],$$

$$[3], [9], [7], [1],$$

$$[3], [9], [7], [1], \dots$$

### Exemplo 2:

$$x = 4 .$$

Se se fizer  $x = 4$  obtém-se um outro **padrão, P2**, com a distribuição:

$$[4] = [4]$$

$$[4]^2 = [16]$$

$$[4]^3 = [64] = [4]$$

$$[4]^4 = [16]$$

$$[4]^5 = [16] \times [4] = [64] = [4]$$

$$[4]^6 = [4] \times [4] = [16]$$

$$[\dots]$$

Assim **P2** alterna entre  $[4]$  e  $[16]$  e, em particular, nunca é igual a  $[1]$ .

### Exemplo 3:

$$x = 11.$$

Se se fizer  $x = 11$  obtém-se um outro **padrão, P3**, que alterna entre [11] e [1].

Assim no *mod* 20 existem classes que têm uma potência igual a [1].

Isto serve de motivação para a definição de *ordem multiplicativa*.

**Definição 1:** [ *Ordem Multiplicativa Finita Modulo  $n$  ( $n > 1$ )* ]

*Diz-se que um inteiro  $x$   
tem uma ordem multiplicativa finita  $k$  (mod  $n$ ) quando*

$$(\exists k)(k \in \mathbb{Z}) \rightarrow [x]^k = [1].$$

**Exercício 1:**

(Mod 20).

- i) indicar uma *o.m.f.* para [3];
- ii) *idem* para [11].

(Em contraste, [4] não tem uma *o.m.f.*).

**Exercício 2:**

(Mod 6).

Mostrar que [3] não tem *o.m.f. mod* 6.

**Teorema 1:** [ *O.M.F.* ]

*Condição necessária e suficiente  
para um inteiro  $x$  ter *o.m.f. mod*  $n$*

$$\begin{aligned} & \acute{e} \\ & \{ (x, n) = 1 \}. \end{aligned}$$

Demonstração:

(Parte I.):

1.  $(\exists k)[x]^k = [1]$  Hip.
2.  $[x^{k-1}] \times [x] = [x]^k$
3. Logo  $[x^{k-1}]$  é o inverso multiplicativo de  $[x]$ .
4.  $\{ (x, n) = 1 \}$  Teor. da Existência  
do Inverso Multiplicativo

(Parte II.):

1.  $\{ (x, n) = 1 \}$  Hip.
2. Logo  $[x]$  tem um inverso *mod n*.
3. Então existem inversos para  $[x]^k$ .
4. Formar os primeiros  $n + 1$  termos da sucessão:
 
$$(*) \quad [x], [x]^2, \dots, [x]^{n+1}$$
5. Ora como  $\mathbb{Z}_n$  tem  $n$  elementos diferentes,  
então existem em (\*) pelo menos duas potências iguais.
6. Se  $k$  e  $m$  forem essas potências então

$$[x]^k = [x]^m$$

de tal modo que

$$1 \leq k,$$

$$m \leq m + 1,$$

$$1 \leq m - k.$$

$$7. [x]^k - [x]^m = [0]$$

$$8. [x]^{-k} \times [x]^k - [x]^m = [0] \times [x]^{-k} \quad \text{I, 3}$$

$$9. [1] - [x]^{m-k} = [0]$$

$$10. [1] = [x]^{m-k}$$

**Definição 2:** [ *Ordem* ]

*Se x tem uma o.m.f. mod n*

*então a ordem de [x] mod n*

*é igual a*

$$\mu k \{ [x]^k = [1] \}.$$

Isto significa que

$$x^k \equiv 1 \pmod{n}.$$

**Exemplos e Exercícios:**

i) A ordem de 3 (*mod* 20) = 4.

ii) A ordem de 11 (*mod* 20) = 2.

iii) Qual é a ordem de 8 (*mod* 7) ?

iv) Qual é a ordem de 3 (*mod* 7) ?

Como  $3^6 = 729$

e

$$729 = 14 \times 7 + 1,$$

tem-se

$$3^6 \equiv 1 \pmod{7}.$$

Logo a solução (de *iv*) acima) é 6.

Se a ordem de  $x \pmod{n}$  é  $k$  então tem-se o seguinte importante teorema: duas potências de  $x$  são congruentes  $\pmod{n}$  se e somente se os expoentes são congruentes  $\pmod{k}$ .

**Teorema 2:** [ *Congruência dos expoentes* ]

$$x^a \equiv x^b \pmod{n} \leftrightarrow a \equiv b \pmod{k}.$$

Demonstração:

(Parte I.:

- |    |                                                |           |
|----|------------------------------------------------|-----------|
| 1. | $a \equiv b \pmod{k}$                          | Hip.      |
| 2. | $(\exists m)(a = b + k \cdot m)$               | 1, Def.   |
| 3. | $x^a = x^{b+k \cdot m}$                        | 2, Subst. |
| 4. | $x^{b+k \cdot m} = x^b \cdot x^{k \cdot m}$    |           |
| 5. | $x^b \cdot x^{k \cdot m} = x^b \cdot (x^k)^m$  |           |
| 6. | $x^b \cdot (x^k)^m = x^b \cdot (1)^m \pmod{n}$ | 5, Def. 2 |

$$7. \quad x^a \equiv x^b \cdot (1)^m \pmod{n}$$

$$8. \quad x^a \equiv x^b \pmod{n}$$

(Parte II.):

$$1. \quad x^a \equiv x^b \pmod{n} \quad \text{Hip.}$$

$$2. \quad a \leq b \quad \text{Hip.}$$

$$3. \quad \{(x, n) = 1\} \quad \text{Teor. 1}$$

4. Então existe um inverso para  $x^a$ .

$$5. \quad x^a \cdot [x^a]^{-1} \equiv x^b \cdot [x^a]^{-1} \quad \text{1, Canc.}$$

$$6. \quad 1 \equiv x^{b-a} \pmod{n}$$

7. Com o algoritmo da divisão reformular  $b - a$  em

$$q \cdot k + r \text{ (com } r < k \wedge r \in \mathbb{N})$$

$$8. \quad x^{b-a} \equiv x^r \pmod{n} \quad \text{4. a 8. (Parte I)}$$

$$9. \quad x^r \equiv 1 \pmod{n} \quad \text{6, 8}$$

$$10. \quad [x^k] = [x^r] \pmod{n}$$

$$11. \quad r = 0 \quad \text{7}$$

$$12. \quad k \mid b - a$$

$$13. \quad a \equiv b \pmod{k}$$

## II. O TEOREMA DE FERMAT

Os nossos objectos são os Grupos  $\langle \mathbb{Z}_p^*, \cdot \rangle$ ,  $\langle \Pi(\mathbb{Z}_p^*), \circ \rangle$ , em que este é o grupo formado por todas as permutações em  $\mathbb{Z}_p^*$  sob Composição.

É útil começar por ver como estes objectos actuam em exemplos numéricos.

(I.: A permutação  $\pi = [2] \cdot \mathbb{Z}_7^*$ )

1. Se o módulo do nosso exemplo é 7 então a notação  $\mathbb{Z}_7^*$  denota o conjunto dos elementos de  $\mathbb{Z}_7$  que têm inversos.
2. Então pelo Teorema de Euler  $\mathbb{Z}_7^*$  tem os seguintes 7-1 elementos :

[1], [2], [3], [4], [5], e [6] todos *mod* 7.

3. A nossa primeira definição é a de uma operação sobre  $\mathbb{Z}_7^*$ , por exemplo, formar o conjunto das classes *pares* de  $\mathbb{Z}_7^*$ , por meio da multiplicação

$$[2] \cdot \mathbb{Z}_7^*.$$

4. Temos assim uma definição deste produto por meio da notação usual:

$$[2] \cdot \mathbb{Z}_7^* = \{[2] \cdot [x] : [x] \in \mathbb{Z}_7^*\}.$$

5. A sua descrição é assim:

$$[2] \cdot \mathbb{Z}_7^* = \{[2] \cdot [1], [2] \cdot [2], \dots, [2] \cdot [6]\}.$$

6. Mas  $[2]$  é também um elemento de  $\mathbb{Z}_7^*$ , como se vê por 2. acima.

7. Realizando os produtos, o valor que vem para  $[2] \cdot \mathbb{Z}_p^*$  é

$$\{ [2], [4], [6], [8], [10], [12] \} \text{ todos } \textit{mod} 7,$$

o que na verdade é igual a

$$\{ [2], [4], [6], [1], [3], [5] \}.$$

8. Comparando o resultado com 2., vê-se que a multiplicação é uma permutação  $\pi = [2] \cdot \mathbb{Z}_7^*$  dos elementos de  $\mathbb{Z}_7^*$ , com a seguinte forma

$$\begin{pmatrix} [1][2][3][4][5][6] \\ [2][4][6][1][3][5] \end{pmatrix}.$$

(II.:  $\pi = [2] \cdot \mathbb{Z}_7^*$  é uma Bijecção)

Como garantir que se  $[3] \neq [5]$ , não se tem

$$[2] \cdot [3] = [2] \cdot [5]?$$

Um argumento por *Reductio* dá-nos o resultado desejado. A

Hipótese da *Reductio* é

$$[2] \cdot [3] = [2] \cdot [5].$$

Ora o Teorema da Cancelação permite cancelar  $[2]$  de ambos os lados e concluir que  $[3] = [5]$ , em contradição com a nossa hipótese de que  $[3]$  é diferente de  $[5]$ .

Logo  $[2] \cdot \mathbb{Z}_7^*$  é 1-1 e é uma sobrejecção, uma vez que todos os elementos de  $\mathbb{Z}_7^*$  são imagens pelo passo 7., parte II.

(III.: O Grupo  $\langle \Pi(\mathbb{Z}_7^*), \circ \rangle$ )

1. A nossa segunda definição é a de um elemento  $[\varphi]$ , que depende de  $\mathbb{Z}_7^*$ , e que é o número de todos os elementos em  $\Pi(\mathbb{Z}_7^*)$ , i.e.,

$$\mathbb{Z}_7^*!$$

2. Assim

$$\mathbb{Z}_7^*! = [1] \cdot [2] \cdot [3] \cdot [4] \cdot [5] \cdot [6]$$

e portanto  $[\varphi] = [720]_7$  e, *pelo Teorema do Fecho para a Multiplicação em  $\mathbb{Z}_7^*$ ,*

$$[\varphi] \in \mathbb{Z}_7^*.$$

3. Pelo algoritmo da divisão  $720 = 102 \cdot 7 + 6$  e portanto

$$[\varphi] = [6]_7.$$

4. Por outro lado o produto

$$[2] \cdot \mathbb{Z}_7^* = [2] \cdot [1] \cdot [2] \cdot [2] \cdot [2] \cdot [3] \cdot [2] \cdot [4] \cdot [2] \cdot [5] \cdot [2] \cdot [6], \text{i.e.,}$$

$$[2] \cdot [4] \cdot [6] \cdot [1] \cdot [3] \cdot [5] = [\varphi].$$

5. Assim tem-se a igualdade

$$[1] \cdot [2] \cdot [3] \cdot [4] \cdot [5] \cdot [6] =$$

$$= [2] \cdot [1] \cdot [2] \cdot [2] \cdot [2] \cdot [3] \cdot [2] \cdot [4] \cdot [2] \cdot [5] \cdot [2] \cdot [6].$$

(IV.: Existência do Inverso em  $\langle \mathbb{Z}_7^*, \cdot \rangle$ )

1. Pode-se simplificar a igualdade de 5. substituindo o primeiro termo à esquerda de  $=$  por  $[\varphi]$  e, para o termo à direita, reunir os factores  $[2]$ , obtendo-se assim a fórmula

$$[6]_7 = [2]^{7-1} \cdot [6]_7.$$

2. Como  $[6]_7$  tem um inverso,  $[-1]_7$ , pode-se multiplicar de ambos os lados desta igualdade por  $[-1]_7$  e obter

$$[-1]_7 \cdot [6]_7 = [2]^{7-1} \cdot [6]_7 \cdot [-1]_7.$$

3. Assim

$$[1]_7 = [2]^{7-1} \cdot [1]_7.$$

4.  $[1]_7 = [2]^{7-1}$

e assim

$$2^{7-1} \equiv 1 \pmod{7}.$$

Passando agora para a demonstração do teorema, as nossas hipóteses são as seguintes:

- i)  $p$  é um número primo;
- ii)  $x \in \mathbb{Z}$ ;
- iii)  $p$  não divide  $x$ .

**Teorema 3:** [ *Teorema de Fermat* ]

*As duas Formulações Equivalentes:*

- I.  $(\forall x)[x]_p^{p-1} = [1]_p.$
- II.  $x^{p-1} \equiv 1 \pmod{p}.$

Demonstração:

**(Parte I:** *A permutação*  $\pi = [x] \cdot \mathbb{Z}_p^*$ )

1.  $\mathbb{Z}_p^*$  = o conjunto dos elementos de  $\mathbb{Z}_p$  que têm inversos.
2. Então pelo *Teorema de Euler*  $\mathbb{Z}_p^*$  tem os seguintes  $p - 1$  elementos:

$$[1]_p, [2]_p, \dots, [p-1]_p.$$

3. Definir agora uma operação  $\pi$  sobre  $\mathbb{Z}_p^*$  que consiste em formar o conjunto de todos os múltiplos  $[x]$  de  $\mathbb{Z}_p^*$  por meio da multiplicação

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

4. A sua definição é

$$[x] \cdot \mathbb{Z}_p^* = \{[x] \cdot [y] : y \in \mathbb{Z}_p^*\}.$$

5. A sua descrição é

$$[x] \cdot \mathbb{Z}_p^* = \{[x] \cdot [1], [x] \cdot [2], \dots, [x] \cdot [p-1]\}.$$

6. Como  $[x] \in \mathbb{Z}_p^*$  tem-se que qualquer elemento em  $[x] \cdot \mathbb{Z}_p^*$  também é elemento de  $\mathbb{Z}_p^*$  e (por 3. e 4.) que qualquer elemento de  $\mathbb{Z}_p^*$  é elemento de  $[x] \cdot \mathbb{Z}_p^*$ .

7. Finalmente,  $\pi = [x] \cdot \mathbb{Z}_p^*$  é uma bijecção em  $\mathbb{Z}_p$ .

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  $\mathbb{Z}_p^*$  são imagens,  $[x] \cdot \mathbb{Z}_p^*$  também é uma sobrejecção.

Logo  $\pi$  é uma permutação em  $\Pi(\mathbb{Z}_p^*)$ .

**(Parte II.)**

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

2. Logo

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

3. Seja  $\langle \Pi(\mathbb{Z}_p^*), \circ \rangle$  o Grupo formado pelo conjunto de todas as permutações em  $\mathbb{Z}_p^*$  sob Composição. Definir então um novo elemento  $[\varphi]$ , que depende de  $\mathbb{Z}_p^*$  e que é o número de elementos em  $\Pi(\mathbb{Z}_p^*)$ , *i.e.*,

$$\mathbb{Z}_p^*! = [1] \cdot [2] \cdot \dots \cdot [p-1]$$

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

$$[\varphi] \in \mathbb{Z}_p^*.$$

5. A bijecção implica que  $[x] \cdot \mathbb{Z}_p^*$  também é igual a  $[\varphi]$ .

6. Assim

$$[1] \cdot [2] \cdot \dots \cdot [p-1] = [x] \cdot [1] \cdot [x] \cdot [2] \cdot \dots \cdot [x] \cdot [p-1].$$

7.  $[\varphi] = [x]^{p-1} \cdot [1] \cdot [2] \cdot \dots \cdot [p-1]$ ,

uma vez que  $x$  ocorre  $p - 1$  vezes.

8. Logo

$$[\varphi] = [x]^{p-1} \cdot [\varphi].$$

9. Mas como  $[\varphi] \in \mathbb{Z}_p^*$ , existe um inverso,  $[\varphi]^{-1}$ .

10. Logo

$$[\varphi]^{-1} \cdot [\varphi] = [x]^{p-1} \cdot [\varphi] \cdot [\varphi]^{-1},$$

pelo Teorema da Cancelação.

$$11. [1] = [x]^{p-1} \text{ mod } p.$$

$$12. x^{p-1} \equiv 1 \text{ mod } p.$$

**(Parte III.: Desfazer a hipótese iii))**

1. Se  $p$  divide  $x$  então  $p$  também divide as potências de  $x$ .

2. Logo  $x^{p-1} \equiv 0 \text{ mod } p$ .

3. Mas por 1.,  $x \equiv 0 \text{ mod } p$ .

4. Logo  $x^p \equiv x \text{ mod } p$ .

**[ N.B.**

*Um corolário importante destes resultados é que*

*uma ordem  $k$  de  $x \text{ mod } p$  divide  $p - 1$ .*

Isto resulta do facto de que

$$[x]^k \text{ mod } p = [1]_p.$$

Logo  $p = m \cdot k + 1$  e por isso

$$p - 1 = m \cdot k + 0.$$

Assim  $k$  divide  $p - 1$ .]

[ ANÁLISE CONCEPTUAL:

O expoente  $p - 1$  na fórmula do Teorema de Fermat não significa que  $p - 1$  seja o menor inteiro tal que

$$x^{p-1} \equiv 1 \text{ mod } p.$$

Exemplo: o já utilizado  $\mathbb{Z}_7^*$ .

As classes de congruência em  $\mathbb{Z}_7^*$  são

$$[1], [2], [3], [4], [5], [6]$$

e as suas ordens são

$$1, 3, 6, 3, 6, 2 \text{ respectivamente.}$$

Todos estes números, 1, 2, 3, 6, são divisores de  $7-1$ , mas só um deles é igual a  $7-1$ .

Os outros são menores do que  $7-1$ . ]

### [ ANEXO: UM PROBLEMA DE G. KREISEL

“Para leitores blasés: Por que razão é 15 divisível por 5? Resposta:

$$15 = 16 - 1 = 2^4 - 1 = 2^{5-1} - 1$$

e segundo Fermat tem-se que para  $p > 2$  :

Para cada número primo  $p$ ,  $2^p - 1$  é divisível por  $p$ .

(Recordar que se aplica a fórmula do binómio a  $(1+1)^p$  :

$$1 + \dots \frac{p!}{r!(p-r)!} + \dots 1$$

e considere-se  $2^p - 2$ .”.

i) *O cálculo dos coeficientes*

O primeiro coeficiente é dado pela fórmula

$$\frac{5!}{0!(5-0)!} = 1.$$

O segundo coeficiente é dado pela fórmula

$$\frac{5!}{1!(5-1)!} = \frac{5!}{4!} = \frac{120}{24} = 5$$

e assim vão-se obtendo os coeficientes

$$1, 5, 10, 10, 5, 1$$

o que corresponde, como se sabe, à linha 6 do Triângulo de Pascal com vértice em 1.

ii) *A fórmula do Binómio*

Para  $p = 5$  a fórmula que se obtém é:

$$\begin{aligned} (1+1)^5 &= 1^5 + 5 \cdot 1^4 \cdot 1 + 10 \cdot 1^3 \cdot 1^2 + 10 \cdot 1^2 \cdot 1^3 + 5 \cdot 1^1 \cdot 1^4 + 1^5 = \\ &= 1+5+10+10+5+1= \\ &= 32. \end{aligned}$$

iii) *A redução ao Módulo*

No módulo 5 tem-se a igualdade

$$[2]^5 = [32]$$

e portanto

$$[2]^5 = [2](\text{mod } 5).$$

Logo

$$2^5 \equiv 2(\text{mod } 5)$$

e assim, como Kreisel pretende,

$$5 \text{ divide } 2^5 - 2.]$$

### BIBLIOGRAFIA

HARDY, G. H. & WRIGHT, E. M., *An Introduction to the Theory of Numbers*, Oxford, 1954.

MAC LANE, S. & BIRKHOFF, G., *Survey of Modern Algebra*, New York, 1967.

MAC LANE, S., *Structure in Mathematics*, *Philosophia Mathematica*, 3, Vol. 4, 1996, pp. 174-183.

WEIL, A., *Number Theory (An approach through history)*, Boston, 1984.