J. SEBASTIÃO E SILVA

GUIA

PARA A UTILIZAÇÃO DO COMPÊNDIO DE MATEMÁTICA

(2.º E 3.º VOLUMES)

Curso Complementar
do Ensino Secundário

Edição GEP

LISBOA

V

INDUÇÃO EXPERIMENTAL E INDUÇÃO MATEMÁTICA

1. A introdução de novos assuntos no programa liceal só é possível, obviamente, eliminando outros que eram desenvolvidos tradicionalmente. Um dos assuntos que, infelizmente, se torna forçoso sacrificar em grande parte é o da chamada 'artimética racional'. E dizemos 'infelizmente', porque esta é o exemplo simples de uma teoria dedutiva, baseada numa axiomática categórica – muito embora suceda, na maior parte dos casos, que por falta de tempo ou por outras razões, o ensino da aritmética racional se tenha reduzido quase unicamente à resolução de mais uns tantos exercícios-cliché, muitos deles desprovidos de qualquer interesse.

Mas há um mínimo da aritmética dos inteiros que é necessário preservar – e nesse mínimo achamos por bem incluir o método de indução matemática. Simplesmente, este método deve ser tratado agora com maior largueza de vistas, em íntima ligação com assuntos situados fora do âmbito estrito da aritmética, especialmente os que se referem aos *fundamentos matemáticos do método experimental,* que o devem preceder (ver capítulo anterior). Pois se é verdade, como parece, que a matemática está a assumir cada vez mais as funções de FILOSOFIA DAS CIÊNCIAS – onde podem estes assuntos ser tratados de maneira conveniente senão no programa de matemática do 3.º ciclo?

2. O estudo do método de indução matemática deve ser amplamente motivado, como tema de filosofia das ciências, se quisermos que tenha alguma eficácia e não seja mais uma *forma de doutrina imposta,* a que o espírito do aluno não adere espontaneamente.

Um dos modos possíveis de introduzir naturalmente este assunto é o que vamos sugerir.

Apresente-se, como tema de discussão, a seguinte pergunta:

O que é mais valioso: descobrir um teorema ou demonstrar esse teorema?

Poderá objectar-se, desde logo, que um teorema não está definitivamente descoberto, enquanto não for demonstrado com todo o rigor: antes disso não temos a certeza de que seja verdadeiro e de que seja, portanto, um teorema autêntico. Mas várias vezes temos lembrado que, na investigação matemática, a *intuição* precede normalmente a *lógica,* isto é, começa-se por ter o *pressentimento* dos factos e só depois este pressentimento (ou intuição) é confirmado ou confirmado por *demonstração*.

Consideremos, por exemplo, a seguinte proposição:

'Se uma função tem derivada positiva em todos os pontos de um intervalo, a função é crescente nesse intervalo'.

No *Compêndio de Álgebra, 6.º ano,* pp. 242-243, este facto é admitido como verdadeiro apenas por intuição geométrica (considerando o gráfico da função), do mesmo modo que se podem admitir como verdadeiros, por exemplo, os seguintes factos:

'Dados um ponto e um plano, existe sempre um plano e um só que passa pelo ponto dado e é paralelo ao plano dado'.

'Dados um ponto e um plano, existe sempre uma infinidade de rectas que passam pelo ponto e são paralelas ao plano; e a reunião dessas rectas é um plano paralelo ao plano dado'.

Nestes casos, a *intuição sensível* apresenta-nos os factos com tal grau de evidência, que nos parece desnecessário demonstrá-los. E, todavia, só podemos ter a certeza de que são verdadeiros (relativamente aos axiomas adoptados), uma vez que sejam demonstrados com todo o rigor lógico, *prescindindo por completo da intuição baseada em figuras.*

Aliás, esses factos são *triviais,* isto é, podem ser *descobertos* por qualquer pessoa que não seja desprovida de intuição geométrica: é bastante mais difícil *demonstrá-los,* do que *descobri-los.* Mas os factos com real interesse em matemática, como por exemplo o teorema de Pitágoras, certas regras de derivação ou integração, etc., não são geralmente triviais, não são *evidentes,* e não podem, portanto, ser descobertos por qualquer pessoa.

Por isso mesmo, vários teoremas, fórmulas ou métodos que foram descobertos antes de serem demonstrados rigorosamente, têm o nome dos matemáticos que os descobriram, mesmo que estes não os tenham demonstrado, pelo menos de maneira completa. *A bem dizer, quase todos os teoremas, fórmulas e métodos descobertos em análise infinitesimal, desde Newton até Lagrange, figuram nessa categoria.*

3. Assim, a demonstração, constituída por uma cadeia de silogismos, segundo as regras da lógica dedutiva, é um processo técnico que se usa em matemática para distinguir o verdadeiro do falso, o certo do errado – e não *propriamente* um método que permita

chegar a resultados essencialmente novos. *A criação científica, tal como a criação artística, não obedece a regras.*

Podemos, pois, dizer que as técnicas de demonstração representam para o matemático, o que as técnicas de experimentação representam para o físico: são meios para confirmar ou infirmar *hipóteses,* concebidas *a priori.* Sob este aspecto são comparáveis às provas das operações aritméticas: prova dos nove em física, prova real em matemática.

Todavia, a demonstração (tal como a experiência), é muitas vezes o ponto de partida para *novas descobertas:* uma vez demonstrado o que tinha apenas pressentido, o matemático começa a ver as questões de maneira muito mais clara, e assim lhe ocorrem *novas ideias,* que o fazem progredir, por vezes com maior vigor.

Não é, portanto, exacto dizer que a lógica nada tem que ver com a descoberta – *que a razão não influi no processo de criação.* Na verdade o matemático, quando disciplinado pelo raciocínio, no processo dialéctico *intuição-lógica, lógica-intuição,* acaba por refinar a sua própria intuição, adquirindo uma espécie de *intuição supra-sensível* que o torna muito mais apto a apreender novos factos. A esta quase poderíamos chamar *intuição racional* (apesar da aparente contradição nos termos), pois que, na realidade, não há uma fronteira nítida entre intuição e lógica: não se pode dizer exactamente onde acaba uma e começa a outra.

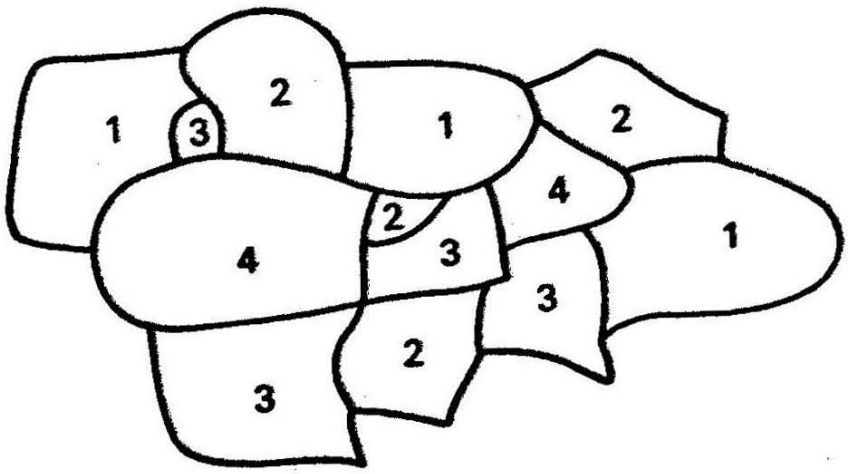
4. Também não se pode dizer exactamente onde acaba a indução e começa a dedução. A matemática é, todos o sabemos, essencialmente dedutiva na confirmação dos seus resultados. Mas isto não impediu o electrotécnico Heaviside (a quem se devem progressos importantes em matemática) de proclamar em dado momento:

A matemática é uma ciência experimental.

Ora tal afirmação é em parte verdadeira: há, com efeito, diversos factos que, em matemática, se apresentam primeiro por indução, a partir de *experiências* feitas com figuras, com símbolos, etc. Começaremos por apresentar três exemplos históricos (1):

1.º *exemplo* (TEOREMA DAS QUATRO CORES). Consideremos o seguinte problema:

Pretende-se colorir um mapa, de modo que dois países figurem representados com cores diferentes, desde que tenham fronteira comum e que essa fronteira não se reduza a pontos isolados. Quantas cores são necessárias, no mínimo, para tal fim?



Têm-se experimentado os mais diversos mapas, relativamente a países reais ou imaginários e o resultado tem sido sempre o mesmo:

Não são precisas mais de 4 cores para colorir o mapa de modo que seja verificada a referida condição.

---

(1) Estes exemplos poderão, eventualmente, ser aconselhados aos alunos como tema de leitura.

Podemos pois, segundo o método de indução experimental, admitir que *esta conclusão é válida em qualquer caso.* Estamos assim em presença de uma *lei,* a que é costume chamar 'TEOREMA DAS QUATRO CORES'. *Mas ninguém, até hoje, conseguiu demonstrar tal teorema, embora tenham sido já apresentadas algumas supostas demonstrações, que, depois de uma análise lógica mais ou menos profunda, se verifica estarem erradas.*

Como se pode então chamar 'teorema' a uma proposição que não foi ainda demonstrada? Quem nos garante que não se venha a descobrir um mapa para o qual sejam precisas mais de 4 cores nas referidas condições? Trata-se pois, quando muito, de uma *hipótese de teorema,* a não ser que convencionemos chamar teoremas também a proposições falsas ou duvidosas.

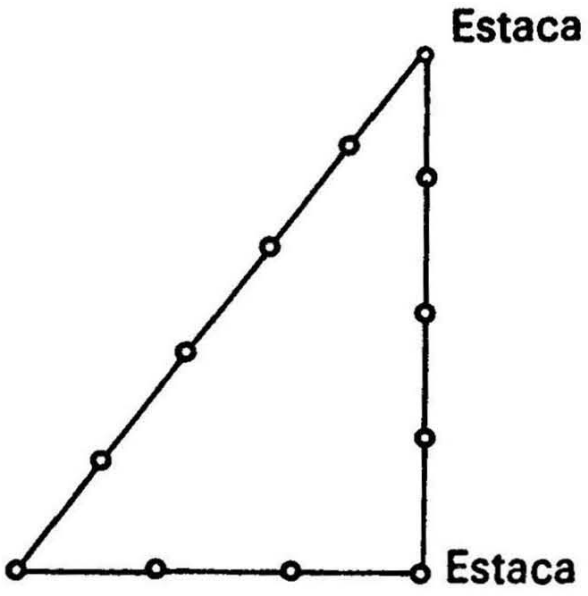
Verdadeiro ou falso, o TEOREMA DAS QUATRO CORES diz respeito a um novo ramo importante da geometria – chamado *topologia* – em que só interessam as *propriedades topológicas* das figuras, isto é, as propriedades de posição relativa que não se alteram por *deformação contínua* (1).

2.º *exemplo* (TEOREMA DE PITÁGORAS). Ao que parece, o teorema de Pitágoras foi sendo a pouco e pouco desvendado por via experimental. Assim, os Egípcios tinham verificado o seguinte facto, milhares de anos antes de Cristo:

'Se os três lados de um triângulo medem respectivamente 3 unidades, 4 unidades e 5 unidades, o triângulo é rectângulo, sendo os dois primeiros lados os catetos'.

---

(1) Dito de maneira intuitiva, sem pretensões de rigor.



Os Egípcios utilizavam, na prática, este *facto experimental* para construir ângulos rectos, recorrendo a uma corda com vários nós equidistantes. Fixavam, por exemplo, dois desses nós por meio de estacas, deixando 3 nós intermédios, e procuravam depois formar com a corda um triângulo como se indica na figura. Ao que parece, foi este o processo utilizado para construir as bases quadradas das pirâmides: assim, o referido facto será já conhecido há cerca de 500 anos!

Verificava-se ao mesmo tempo o seguinte:

$$3^2 + 4^2 = 5^2$$

e, analogamente, para outros ternos de números tais como (6, 8, 10) (9, 12, 15), etc., aos quais os Egípcios atribuíam *carácter místico*.

Por sua vez, os Indianos e os Chineses, em épocas também muito remotas, tinham *observado* que, para construir um ângulo recto, se podia utilizar uma corda dividida em partes de comprimentos 5, 12, 13 ou em partes de comprimentos 8, 15, 17. E também nestes casos acontecia que

$$5^2 + 12^2 = 13^2 \quad , \quad 8^2 + 15^2 = 17^2$$

Estranhas e curiosas coincidências estas, que não podiam deixar de impressionar vivamente a *imaginação poética, mitológica,* dos antigos, inclinados naturalmente a ver em tais coincidências SÍMBOLOS MÍSTICOS, reveladores de uma divina harmonia subjacente à natureza.

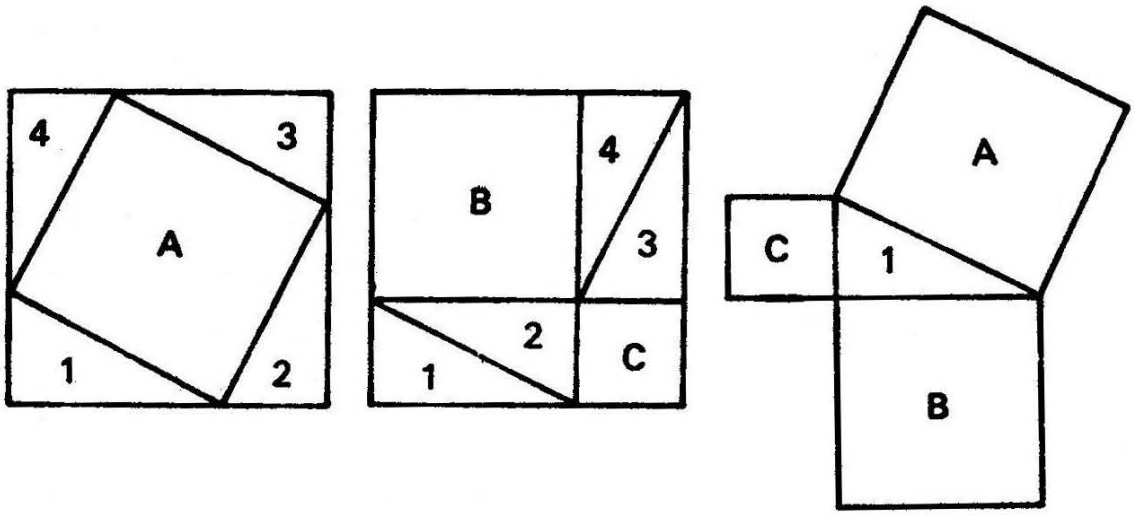
Mas estava-se então apenas numa *fase empírica,* em que não se conseguia sequer subir, por *indução,* dos factos particulares observados, a uma *lei experimental* (1). O salto para a *fase racional* foram os Gregos que o deram, começando por admitir, como hipóteses, o seguinte facto geral:

'O quadrado da medida da hipotenusa é igual à soma dos quadrados das medidas dos catetos'.

Foi, segundo se diz, Pitágoras, quem primeiro *demonstrou* este facto, partindo de outros que são (ou parecem) *evidentes.* Hoje, o TEOREMA DE PITÁGORAS pode ser demonstrado com o máximo rigor lógico, sem apelo à intuição, a partir de uma axiomática bem definida da geometria euclidiana, como por exemplo a axiomática de Hilbert. Porém, a demonstração que se atribui a Pitágoras tem um carácter fortemente intuitivo, que nos *rende à evidência,* fazendo-nos *ver,* num relance, a veracidade do teorema. Os *factos evidentes* a que tal demonstração reduz o teorema são essencialmente *propriedades intuitivas das áreas,* que poderiam ser tomadas como

---

(1) Ainda hoje, em algumas regiões, por exemplo no Sul da França, os camponeses aplicam o referido *método da corda,* como simples *receita empírica,* transmitida por tradição, desde tempos imemoriais. Sobre este assunto, veja-se a bela obra da Prof.ª Emma Castelnuovo, 'La Geometria' (Ed. La Nuova Italia, Firenza), para a Escola Média Italiana, correspondente aos 3 primeiros anos dos nossos liceus.



axiomas (numa axiomática larga, *não independente*), mas que é difícil demonstrar a partir dos axiomas usuais.

Assim apareceu o MÉTODO DA DEMONSTRAÇÃO MATEMÁTICA, que consistia em provar um facto geral, sem recorrer à experiência, mas apenas por *dedução,* reduzindo esse facto a outros que são (ou parecem ser) evidentes. As provas por este método, ao contrário das que se baseavam na experiência, davam um sentimento de *certeza absoluta*. Por isso mesmo, a sua descoberta – que marca o nascimento histórico do *racionalismo* e da *matemática como ciência dedutiva* – foi causa de deslumbramento para os pitagóricos, que se sentiam assim mais próximos dos deuses.

Aos referidos ternos de números naturais, que verificam a equação em três incógnitas

$$x^2 + y^2 = z^2$$

chamados hoje *números pitagóricos,* e a que eram atribuídas, desde os Egípcios, virtudes mágicas, induziram naturalmente os filósofos da escola de Pitágoras a admitir como certa uma outra hipótese mais ousada:

'Qualquer que seja o triângulo rectângulo, é sempre possível escolher uma unidade de comprimento tal que as medidas dos cate-

tos e da hipotenusa sejam números inteiros [portanto números pitagóricos]'.

Mais geralmente ainda, foram ao ponto de admitir que *toda a linha é formada por um número finito de unidades indivisíveis (a que poderíamos chamar 'átomos' ou 'mónadas')* e que, portanto, *dois comprimentos são sempre comensuráveis entre si* (cf. *Compêndio de Álgebra*. 'Nota Histórica' do Cap. I).

Assim, aos pitagóricos, a natureza aparecia como um ente geométrico perfeito, em que as relações entre todas as coisas, desde os corpos celestes aos sons musicais, se podiam exprimir harmonicamente por meio de números – e precisamente *números inteiros*. Era isso, no fundo, o que eles queriam dizer quando afirmavam: 'Os números são a essência de todas as coisas'.

Mas foi o próprio teorema de Pitágoras que, por ironia, os levou a descobrirem que *era falsa a hipótese segundo a qual duas grandezas são sempre comensuráveis entre si!* Assim, caía pela base esta primeira tentativa da matematização do universo – e compreende-se bem o drama que tal descoberta representou, atendendo ao carácter religioso que os pitagóricos atribuíam à sua teoria. Foram portanto eles, provavelmente, os primeiros seres humanos que, depois de terem descoberto, com deslumbramento, as potencialidades do método racional, conheceram em seguida o seu rigor inexorável e as amargas desilusões a que conduz – ao verem ruir, à luz crua desse método, as generalizações apressadas a que os tinha conduzido o seu entusiasmo. Quais Ícaros ingénuos, lançados na aventura do espírito, o sol da Razão derreteu-lhes a cera com que tinham colado as asas do pensamento.

3.º *exemplo* (TEOREMA DE FERMAT). **É fácil ver que existe uma infinidade de soluções inteiras e positivas da equação $x^2 + y^2 = z^2$**

(números pitagóricos), dadas pelas fórmulas:

$$x = \sqrt{uv} \quad , \quad y = \frac{u - v}{2} \quad , \quad z = \frac{u + v}{2}$$

em que *u* e *v* são números naturais arbitrários (distintos).

Neste momento, ocorre naturalmente considerar equações tais como

$$x^3 + y^3 = z^3 \quad , \quad x^4 + y^4 = z^4 \quad , \quad x^5 + y^5 = z^5 \quad , \quad \text{etc.}$$

e procurar *ternos de números naturais* que as verifiquem. Ora, por mais tentativas que se façam, não se consegue encontrar nenhum terno de números nessas condições, o que leva a admitir como hipótese o seguinte facto:

Qualquer que seja o número natural $n > 2$, *não existe nenhum terno de números naturais* x, y, z tal que $x^n + y^n = z^n$; isto é, simbolicamente:

$$n \in \mathbb{N} \wedge n > 2 \underset{n}{\Rightarrow} \sim \exists (x, y, z) \in \mathbb{N}^3 : x^n + y^n = z^n$$

Esta proposição é hoje conhecida com o nome de ÚLTIMO TEOREMA DE FERMAT. A razão é a seguinte:

Durante as leituras de uma edição da aritmética de Diofanto, Fermat tinha, por hábito, escrever observações à margem do livro. Ora, precisamente quando Diofanto trata do problema das soluções inteiras da equação $x^2 + y^2 = z^2$, Fermat observa que o problema análogo é impossível para equações da forma $x^n + y^n = z^n$, sendo *n* um número natural > 2, e acrescenta, a propósito deste facto:

'J'ai découvert une démonstration vraiment admirable que cette marge est trop petite pour contenir'.

Já lá vão três séculos e nenhum matemático conseguiu até hoje encontrar uma demonstração de tal teorema! No entanto, Fermat disse que tinha uma demonstração *admirável*. Mais ainda, em todos os outros casos em que omitiu as demonstrações dos seus teoremas, estes acabaram por ser demonstrados, por vezes com dificuldade. Que pensar então?

Vários matemáticos estão convencidos de que Fermat se enganou, dessa vez, ao dizer que tinha descoberto uma demonstração do facto enunciado. Porém, até hoje, o *teorema* (se podemos chamar-lhe assim) ainda não foi desmentido. Mais do que isso, já pôde ser demonstrado, no *caso particular* em que o expoente n é um número primo < 14000 e em que nenhum dos números x, y, z é múltiplo de n, o que, *do ponto de vista da indução experimental,* aumenta em nós a convicção de que é verdadeiro *no caso geral*. Mas continuamos a não ter a *certeza absoluta* (ou antes, *a certeza matemática*), de que a proposição geral seja de facto verdadeira.

Acontece até que certos matemáticos, nomeadamente os INTUICIONISTAS, se inclinam para a seguinte

HIPÓTESE: *Existem proposições a respeito das quais é impossível demonstrar se são verdadeiras ou falsas.*

O chamado 'teorema de Fermat' poderia estar, precisamente, nestas condições, e, sendo assim, não seria *nem verdadeiro nem falso,* pois que, segundo os intuicionistas, só é verdadeiro ou falso em matemática, aquilo que se pode demonstrar como tal (1). Chama-se *indecidível* um problema que não se pode decidir nem pela afirmativa

---

(1) Neste ponto, o intuicionismo transporta para a matemática o PRINCÍPIO DE MACH, atribuindo à *demonstração* o papel da *verificação experimental.*

nem pela negativa. Exemplo de uma questão indecidível pode ser precisamente a seguinte:

Saber se a hipótese anterior é verdadeira ou falsa.

Tem-se verificado, porém, que uma questão pode ser indecidível num dado *formalismo* (com determinados processos de demonstração) e tornar-se decidível num *formalismo mais rico* (com processos mais potentes de demonstração).

Na verdade, a matemática é apta a *criar* para seu uso – sobretudo graças à lógica simbólica — sistemas de linguagem precisa (chamadas 'formalismos rigorosos') cada vez mais ricos, que oferecem novos processos de demonstração (e, portanto, novos tipos de silogismo) cada vez mais potentes. Isto é semelhante ao que sucede com a aparelhagem da física experimental, que se torna cada vez mais complexa e poderosa. Entre os processos de demonstração que se tornam progressivamente mais complexos figuram os MÉTODOS DE INDUÇÃO MATEMÁTICA, de que bastará apresentar o caso mais simples no ensino liceal.

Mas, antes disso, impõem-se ainda mais algumas observações:

I. O facto de haver problemas que são indecidíveis num dado formalismo e depois se tornarem decidíveis em formalismos mais potentes veio pôr em evidência o *poder criador do espírito humano e o carácter dialéctico* do desenvolvimento da matemática, cuja evolução é em parte imprevisível, tal como a evolução do mundo físico. Para os intuicionistas, o chamado 'teorema de Fermat' é comparável a uma frase como a seguinte:

'No dia 12 de Março do ano 3000, chove em Lisboa pelas 3 horas da tarde'.

Que é que nos leva, inconscientemente, a convencer-nos de que o teorema de Fermat é, por força, *verdadeiro ou falso?* Apenas a ideia *platónica* de que, experimentando *todos* os possíveis ternos (x, y, z) de números naturais e *todos* os números naturais *n* maiores que 2, se pode saber se existe ou não algum terno (x, y, z) e algum número $n > 2$ tal que $x^n+y^n = z^n$. Mas essas verificações seriam em número *infinito* e, portanto, irrealizáveis na sua totalidade (1). Assim:

> *Uma demonstração só é válida quando é constituída por uma cadeia finita de silogismos.*

O carácter *finitista* das demonstrações matemáticas é exigido não só pelos *intuicionistas* (escola de Brouwer), mas também pelos *formalistas* (escola de Hilbert). Mas estes, ao contrário dos primeiros, aceitam o PRINCÍPIO DO TERCEIRO EXCLUÍDO (e até o PRINCÍPIO DE ZERMELO) como axiomas da lógica (ver *Compêndio de Matemática, 2.º volume,* p. 103).

Note-se que os intuicionistas *não afirmam nem negam explicitamente a existência de um terceiro valor lógico.* Há, no entanto, lógicas que admitem explicitamente a existência de mais de dois valores (*lógicas plurivalentes*).

---

(1) Platão e os filósofos neoplatónicos, em especial Santo Agostinho, diriam neste caso: 'Os números existem desde a Eternidade, independentes de nós, no Mundo das Ideias, onde são abrangidos, *na sua totalidade,* pela Inteligência Divina'. Note-se como este ponto de vista é semelhante ao de Laplace ao formular o *determinismo mecanicista* (1.º volume, 2.º tomo, p. 223). No fundo, o determinismo absoluto na física, assim como o *fixismo* em biologia, são formas de racionalismo platónico. Mas já é diferente o ponto de vista de Aristóteles, depois retomado por S. Tomás de Aquino (ver no *Compêndio, 2.º volume,* a nota sobre *nominalismo e realismo,* p. 371).

II. Os exemplos anteriores mostram que, em certos casos excepcionais, é mais importante encontrar a demonstração de um teorema do que descobrir o próprio teorema. Assim, por exemplo, se alguém vier a descobrir uma demonstração do 'teorema das 4 cores' ou do 'último teorema de Fermat', esse alguém ficará para sempre, *ipso facto,* na história da matemática. Mas nunca se aconselhe um principiante a tentar a sua *chance* contra esses baluartes praticamente inexpugnáveis! Vários matemáticos, altamente experimentados, têm já tentado o mesmo. Alguns obtiveram resultados parciais importantes; por exemplo Kummer, nas suas tentativas de demonstração do teorema de Fermat, foi levado a introduzir novos conceitos que fizeram progredir grandemente a álgebra e a teoria dos números. Mas as investigações sobre este caso parece terem chegado a ponto morto – a não ser que surjam inesperadamente novos métodos de ataque.

Em 1908 um professor alemão deixou em testamento um prémio de 100 000 marcos para quem conseguisse demonstrar o último teorema de Fermat; mas a inflação consecutiva à 1.ª Grande Guerra reduziu quase a zero esse prémio.

III. Como regra, um jovem que deseje fazer investigação em qualquer ramo da ciência, deve procurar ser encaminhado para a *fronteira do conhecimento,* onde se desenvolvem as mais recentes pesquisas, procurando evitar campos muito explorados, *onde é extremamente improvável obter resultados positivos, que não tenham sido já obtidos por outrem no passado.*

5. A última observação anterior aplica-se, em particular, a uma tentativa de investigação do aluno Hélio Bernardo Lopes, de uma turma clássica do 7.º ano do Liceu D. João de Castro. Essa tentativa é sem dúvida interessante, pelo que representa de imaginação

e de esforço prometedor da parte de um aluno liceal, e pode constituir um *centro de interesse eficaz,* como motivação para introduzir o método de indução matemática.

Meditando sobre a propriedade $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$, que despertou o seu interesse, o referido aluno começou a fazer *experiências* com o triângulo de Pascal e concluiu, por *indução experimental,* que deve ser válida a seguinte fórmula sobre arranjos:

$$^{m}A_{p} = p\,(^{m-1}A_{p-1} + {}^{m-2}A_{p-1} + \ldots + {}^{p-1}A_{p-1}) \text{ para } m \geqslant p \geqslant 1$$

A sua professora, a quem apresentou este resultado, em vez de o desencorajar, aconselhou o aluno, e muito bem, a tentar *demonstrar* a fórmula, indicando-lhe, para esse fim, o método de *indução matemática.* Passado algum tempo, o aluno conseguiu, por este método, provar o que se pretendia. A demonstração, que se reduz à aplicação simples do referido método, será apresentada mais adiante.

Entretanto, surge a questão:

Será esta fórmula um resultado novo?

Num campo tão explorado e tão elementar como o da análise combinatória, a probabilidade de encontrar um resultado *essencialmente* novo é muito pequena. A única dificuldade pode estar em descobrir um livro, um artigo, uma enciclopédia, onde se encontre esse resultado ou um outro equivalente. No caso presente não foi necessário procurar muito: a fórmula em questão deduz-se *trivialmente* da seguinte, já conhecida, relativa a combinações(1):

$$\binom{m}{p} = \binom{m-1}{p-1} + \binom{m-2}{p-1} + \ldots + \binom{p-1}{p-1} \quad , \text{ para } m \geqslant p \geqslant 1$$

---

(1) No *Compêndio de Álgebra* faz-se uma breve referência a esta *propriedade,* em *linguagem comum.*

Basta multiplicar ambos os membros por factorial de p.

Mas o aluno Hélio Lopes ganhou alguma coisa com esta sua primeira tentativa: 1.º, ficou a ter uma primeira ideia de como se pode fazer investigação, que proporciona a aventura do espírito e a conhecer as emoções – alegrias e desenganos; 2.º, tornou-se muito mais consciente da necessidade da demonstração matemática, assim como do significado e do alcance do método de indução matemática; 3.º, aprendeu que, para conseguir resultados essencialmente novos, é preciso evitar assuntos que não estejam na fronteira actual do conhecimento. E, para que não fique desanimado, bastará dizer-lhe o seguinte:

Mesmo trabalhando na fronteira do conhecimento, um investigador arrisca-se a encontrar resultados que já foram obtidos por outrem, algum tempo antes. Por vezes, os resultados são *exactamente* iguais, sem que tenha havido a mínima influência de um investigador sobre o outro. É por isso mesmo que, quando um matemático encontra resultados novos que lhe parecem importantes, se apressa a publicá-los, *a fim de não perder a prioridade;* muitas vezes anuncia-os, antes disso, *sem demonstração,* em breves comunicações a Academias ou Congressos. E, antes ainda de fazer qualquer espécie de publicação, tem geralmente o cuidado de se informar com colegas e de averiguar se não há referência a resultados análogos, em certas revistas internacionais, que fazem *mensalmente* um resumo de quase todos os trabalhos de matemática que se publicam no mundo inteiro, incluindo as simples comunicações.

6. Ficam atrás sugeridas várias possíveis maneiras de motivar o estudo do método de indução matemática. O professor poderá aproveitar estas sugestões, na medida em que a sua experiência e o seu bom senso o aconselharem.

A introdução do referido método pode fazer-se como no Cap. III do 2.º volume, tentando traduzir por símbolos na lógica matemática a seguinte propriedade, que o aluno conhece intuitivamente:

O número 1 *gera todos os outros números naturais, por adição sucessiva:*

$$1+1\ ,\ 1+1+1\ ,\ 1+1+1+1\ ,\ 1+1+1+1+1\ ,\ \ldots$$

A tradução simbólica desta propriedade – O PRINCÍPIO DE INDUÇÃO MATEMÁTICA EM IN — é feita no n.º 2 desse capítulo *em termos de conjuntos*. Não interessa, por enquanto, tratar da propriedade VI, nem das restantes que caracterizam o grupóide aditivo IN.

Pode apresentar-se, depois, a seguinte definição por recorrência (de uma sucessão u_n):

$$u_1 = \frac{1}{2}\ ,\quad u_{n+1} = \frac{1}{2-u_n}\ ,\quad \forall n \in \mathbb{N}$$

Pede-se ao aluno que determine alguns termos e que indique uma *possível* expressão do termo geral (isto é, uma *expressão analítica* desta função de n). A expressão sugerida será:

$$u_n = \frac{n}{n+1}$$

Verifica-se que, *para muitos valores de* n, tal expressão é efectivamente válida. Mas resta provar que é válida para *todos* os valores de *n*, isto é, que se tem de facto:

$$u_n = \frac{n}{n+1}\ ,\quad \forall n \in \mathbb{N}$$

Para isso, há que recorrer ao METODO DE INDUÇÃO MATEMÁTICA, baseado no princípio anterior. *Mas antes é preciso formular este princípio em termos de compreensão, tal como se faz no n.º* 3 (substituindo o exemplo que se considera nesse número, pelo anterior).

Repare-se na *metáfora dos soldados de chumbo*. Essa imagem preciosa, como tantas outras que se devem utilizar no ensino, à semelhança do que se faz na investigação, estimula a *imaginação* (como *imagem* que é). Como já temos observado, uma das graves deficiências do ensino tradicional, sobretudo entre nós, é a de não falar à imaginação dos alunos.

Uma vez posto o princípio da indução sob a forma de silogismo, pode-se demonstrar o que se pretendia. Em geral começa-se por provar a premissa menor e só depois se prova a premissa maior. Neste caso P(n) é a propriedade

$$u_n = \frac{n}{n+1}$$

Esta propriedade é, evidentemente, verificada para n = 1:

$$u_1 = \frac{1}{1+1} = \frac{1}{2}$$

Seja, agora, k um *determinado* número natural, tomado *arbitrariamente* (1), e suponhamos que a propriedade P(n) é verificada para n = k, isto é, que

$$u_k = \frac{k}{k+1} \quad \textit{(hipótese de indução)}$$

---

(1) O símbolo k será pois, neste caso, uma *constante arbitrária*.

Trata-se de provar que a propriedade é verificada também para $n = k + 1$. Ora tem-se, por definição,

$$u_{k+1} = \frac{1}{2 - u_k}$$

donde, *pela hipótese de indução,*

$$u_{k+1} = \frac{1}{2 - \frac{k}{k+1}} = \frac{1}{\frac{k+2}{k+1}}$$

e, portanto

$$u_{k+1} = \frac{k+1}{(k+1)+1}$$

Ficou, assim, provado que a referida propriedade é *hereditária* e, como além disso, é verificada para $n = 1$, fica provado que é verificada para todo o $n \in \mathbb{N}$, q. e. d.

Um segundo exemplo pode ser o da definição de recorrência

$$u_1 = 5 \quad ; \quad u_{n+1} = u_n + 3 \quad , \quad \forall n \in \mathbb{N}$$

Trata-se, como se vê, da progressão aritmética cujo primeiro termo é 5 e cuja razão é 3. O aluno já *sabe* que a expressão do termo geral, neste caso, é:

$$u_n = 5 + 3(n - 1)$$

Mas ainda não conhece uma demonstração rigorosa deste facto. Uma tal demonstração pode ser dada pelo método de

indução matemática, cuja aplicação, neste caso, é muito simples.

Em seguida pode passar-se ao caso geral da definição:

$$u_1 = a \;\; ; \;\; u_{n+1} = u_n + r \;\; , \;\; \forall n \in \mathbb{N}$$

em que *a* e *r* são constantes arbitrárias (progressão aritmética cujo primeiro termo é *a* e cuja razão é *r*).

Prova-se então, pelo mesmo método, que, neste caso,

$$u_n = a + (n-1)\,r \;\; , \;\; n \in \mathbb{N} \;\; ; \;\; a, r \in \mathbb{R}$$

(Mais geralmente ainda, *a* e *r* podem ser elementos de um *módulo qualquer*).

Depois virá o caso geral da *progressão geométrica:*

$$u_1 = a \;\; ; \;\; u_{n+1} = u_n r \;\; , \;\; \forall n \in \mathbb{N}$$

que difere do caso anterior apenas em que *a linguagem aditiva é substituída pela linguagem multiplicativa.*

A propósito destes exemplos simples, o aluno terá aprendido a distinguir as *constantes arbitrárias* das *variáveis de indução,* nas demonstrações por indução matemática. Será depois mais fácil tratar dos exemplos I e II directamente, *sem ser já necessário particularizar as constantes arbitrárias.*

Devem seguir-se os exemplos III, IV, V e VI. Note-se que os exemplos IV e V têm a vantagem, sempre importante, de constituirem novidade para o aluno, sendo por isso mais aptos a despertar o seu interesse. Mas importa levá-lo a reconhecer que, nestes casos, o método de indução matemática é, cem por cento, uma *técnica de demonstração,* que nada nos diz sobre a maneira de chegar a essas fórmulas – sobre a *ideia* que conduziu ao resultado. Para isso, é bom comparar, por exemplo, a dedução

intuitiva habitual das fórmulas dos exemplos III e VI, com a demonstração por indução matemática(1).

6. E chegou agora o momento, por certo emocionante, de demonstrar por indução matemática a fórmula redescoberta pelo aluno Hélio Lopes. Vamos expô-la tal qual este aluno a apresenta numa sua nota.

1.ª parte: $m = p$

$$p \cdot {}^{p-1}A_{p-1} = p\,(p-1)\,! = p! = {}^{p}A_{p}$$

Está então verificado que ${}^{p}A_{p} = p \cdot {}^{p-1}A_{p-1}$

2.ª parte:

Hipótese: ${}^{m}A_{p} = p({}^{m-1}A_{p} + {}^{m-2}A_{p-1} + \ldots + {}^{p-1}A_{p-1})$

Tese: ${}^{m+1}A_{p} = p({}^{m}A_{p-1} + {}^{m-1}A_{p-1} + \ldots + {}^{p-1}A_{p-1})$

$$p({}^{m}A_{p-1} + {}^{m-1}A_{p-1} + {}^{m-2}A_{p-1} + \ldots + {}^{p-1}A_{p-1}) =$$

$$= p \cdot {}^{m}A_{p-1} + p({}^{m-1}A_{p-1} + {}^{m-2}A_{p-1} + \ldots + {}^{p-1}A_{p-1})$$

---

(1) É também muito importante — é mesmo imprescindível — salientar que a indução matemática não é *indução* (no sentido experimental), mas sim *dedução*: é uma das muitas formas de raciocínio dedutivo, embora menos trivial do que as de tipo clássico.

$$= p \cdot {}^{m}A_{p-1} + {}^{m}A_{p} = p \cdot \frac{m!}{(m-p+1)!} + \frac{m!}{(m-p)!}$$

$$= p \cdot \frac{m!}{(m-p+1)!} + \frac{m!\,(m-p+1)}{(m-p+1)!} = \frac{m!\,p + m!(m-p+1)}{(m-p+1)!}$$

$$= \frac{m!\,(p+m-p+1)}{(m-p+1)!} = \frac{m!\,(m+1)}{(m-p+1)!} = \frac{(m+1)!}{(m-p+1)!} = {}^{m+1}A_{p}$$

Está assim provado que

$${}^{m}A_{p} = p({}^{m-1}A_{p-1} + \ldots + {}^{p-1}A_{p-1}) \Rightarrow {}^{m+1}A_{p} = p({}^{m}A_{p-1} + \ldots + {}^{p-1}A_{p-1})$$

Como se vê, a demonstração é perfeitamente correcta, mas o método não foi aplicado *com o aspecto habitual*. Para o aplicar, tal como foi indicado, haverá que pôr $m = p + n$ e tomar *n* para *variável de indução,* sendo p uma *constante arbitrária*. Por outro lado, teremos de fazer a indução em $\mathbb{N}_0$ e não em $\mathbb{N}$.

Assim, na 1.ª parte demonstrou-se que a fórmula é verdadeira para $n = 0$, pois que então ${}^{n+p}A_{p} = {}^{p}A_{p}$ e

$${}^{p}A_{p} = p \cdot {}^{p-1}A_{p-1} \quad , \quad \forall p \in \mathbb{N}$$

Por sua vez, na 2.ª parte, demonstrou-se que, se a fórmula é verdadeira para $m = p+n$, também é verdadeira para $m = p+(n+1)$, quaisquer que sejam $n \in \mathbb{N}_0$, $p \in \mathbb{N}$.

7. No ensino deste método, como em geral no ensino da aritmética, convém alternar os assuntos *essencialmente novos,* de

interesse palpitante (como o anterior), com *assuntos já conhecidos do aluno,* que se trata agora de demonstrar com todo o rigor lógico (1). Mas, até neste caso, convém introduzi-los de maneira *imprevista,* como *problemas* que o aluno terá de resolver por si (sempre de acordo com o método activo e heurístico!).

Resolvam-se primeiro os exercícios I e V do n.º 2 do 2.º volume (Cap. III), que põem o aluno em contacto com diversas modalidades de definições de recorrência. Note-se que é infinita a variedade de tais definições e que esse infinito é qualitativo, isto é: *estão sempre a surgir novas formas imprevisíveis de definição por recorrência (assim como novas formas imprevisíveis de demonstração por indução matemática*).

Note-se também que não existe nenhuma expressão usual para a sucessão φ do exercício II: *este facto não é excepção, mas sim a regra, em sucessões definidas por recorrência.*

Posto isto, proponha-se ao aluno o seguinte exercício: determinar vários termos das sucessões f e g, definidas em $\mathbb{N}_0$ pelo seguinte *sistema de condições:*

$$g(0) = 0 \quad , \quad f(0) = 0$$

$$g(n+1) = g(n) + 1 \Leftarrow g(n) < 3$$

$$g(n+1) = 0 \Leftarrow g(n) = 3$$

$$f(n+1) = f(n) \Leftarrow g(n) < 3$$

$$f(n+1) = f(n) + 1 \Leftarrow g(n) = 3$$

---

(1) Os assuntos deste número só serão tratados se houver tempo para isso.

Pode começar-se pela sucessão g; os seus 20 primeiros termos são:

0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3,...

Os 12 primeiros termos da sucessão f são:

0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, ...

Por indução experimental, o aluno *verá* que

f(n) = quociente inteiro da divisão de *n* por 4

g(n) = resto da divisão de *n* por 4

Que quer isto dizer? Recordemos que o PROBLEMA DA DIVISÃO INTEIRA consiste no seguinte:

Dados dois números $a \in \mathbb{N}_0$ *e* $b \in \mathbb{N}$, *determinar dois números* $q, r \in \mathbb{N}_0$ *tais que*

$$a = bq + r \quad , \quad \textit{sendo} \quad r < b$$

Os números q e r serão chamados, respectivamente, *quociente inteiro* e *resto, da divisão de* a *por* b.

Ora no caso presente tem-se a = n, b = 4 e quer-se provar que q = f(n) e r = g(n). Pretende-se, pois, provar que

$$(1) \qquad n = 4\,f(n) + g(n) \quad \wedge \quad g(n) < 4 \quad , \quad \forall n \in \mathbb{N}_0$$

A demonstração será feita por *indução matemática:*

$$f(0) = 0 \quad , \quad g(0) = 0 \,.\cdot.\, 0 = 4\,f(0) + g(0) \quad , \quad g(0) < 4$$

Hipótese de indução: $n = 4\,f(n) + g(n)$, $g(n) < 4$

Tese de indução: $n+1 = 4\,f(n+1) + g(n+1)$, $g(n+1) < 4$

Para provar esta, há que distinguir dois casos:

1.º caso: $g(n) < 3$. Então:

$$g(n+1) = g(n) + 1 < 4 \quad , \quad f(n+1) = f(n)$$

$$\therefore \quad 4f(n+1) + g(n+1) = 4f(n) + g(n) + 1 = n+1 \quad , \quad g(n+1) < 4$$

$$\therefore \quad n+1 = 4f(n+1) + g(n+1) \quad , \quad g(n+1) < 4$$

2.º caso: $g(n) = 3$. Então:

$$g(n+1) = 0 < 4 \quad , \quad f(n+1) = f(n) + 1$$

$$\therefore \quad 4f(n+1) + g(n+1) = 4f(n) + 4 = 4f(n) + g(n) + 1 = n+1$$

$$\therefore \quad n+1 = 4\,f(n+1) + g(n+1) \quad , \quad g(n+1) < 4$$

q.e.d.

É claro que, em vez do número 4, se pode considerar um *outro número natural* qualquer: as considerações serão perfeitamente análogas. Mas agora surge-nos, de improviso, uma *nova ideia:*

Deve ser possível demonstrar, por este processo, que o problema DA DIVISÃO INTEIRA é sempre *possível* e *determinado,* isto é, que:

$$\forall\, a \in \mathbb{N}_0 \quad , \quad b \in \mathbb{N} \quad , \quad \exists\, q,r \in \mathbb{N}_0 : \quad a = bq + r \wedge r < b$$

Para a demonstração convém tomar *a* para *variável de indução,* b *para constante arbitrária* e pôr:

$$(1) \qquad q = f(a) \quad , \quad r = g(a)$$

O problema exige que se tenha $q, r \in \mathbb{N}_0$ e

$$(2) \qquad a = bq + r \quad , \quad \text{com } r < b$$

Então é óbvio que, sendo $a = 0$, só pode ser $q = 0$ e $r = 0$, isto é:

$$(3) \qquad f(0) = 0 \quad e \quad q(0) = 0$$

Por outro lado, se o dividendo aumenta de uma unidade, dois casos se podem dar: ou aumenta o resto ou aumenta o quociente. Mais precisamente, de (1) e (2) deduz-se:

$$(4) \qquad \begin{array}{l} g(a) < b-1 \Rightarrow f(a+1) = f(a) \wedge g(a+1) = g(a) + 1 \\ g(a) = b-1 \Rightarrow f(a+1) = f(a) + 1 \wedge g(a+1) = 0 \end{array}$$

Como é fácil ver, estas fórmulas definem por recorrência duas funções f e g em $\mathbb{N}_0$ para cada $b \in \mathbb{N}$. Ora, como no caso particular anterior, demonstra-se, por indução matemática, que, para todo o $a \in \mathbb{N}_0$, os números $q = f(a)$ e $r = g(a)$ constituem de facto *uma* solução do problema. Por outro lado, essa solução é *única,* visto que as condições (3) e (4) são impostas pelo problema.

Como já foi dito a propósito dos *métodos de iteração,* o estudo dos processos de recorrência tornou-se muito importante e tem-se desenvolvido com a expansão do uso dos computadores.

8. Uma vez terminado o estudo do método de indução matemática, convirá que o professor refira, sem entrar em pormenores, que as propriedades A1−A5 consideradas no n.º 6 *caracterizam a estrutura do grupóide* (IN,+). Quer isto dizer o seguinte: qualquer outro grupóide (A, θ) que verifique tais propriedades, com A no lugar de N e θ no lugar de +, é *necessariamente isomorfo a* (IN,+). Daí resulta que *qualquer outra proposição verdadeira em* IN *(que não seja definição) é consequência lógica das proposições* A1−A5 *(e das definições que porventura forem introduzidas)*. Sendo assim, as proposições A1−A5 podem ser tomadas para *axiomas* da teoria dos números naturais e então as outras (que não forem definições) chamam-se *teoremas*.

O facto de qualquer grupóide que verifique a axiomática A1−A5 ser isomorfo a (IN,+) exprime-se dizendo que esta axiomática é *categórica*. Pelo contrário, a axiomática dos grupóides, a dos grupos, a dos anéis, a dos corpos, a dos conjuntos ordenados, a dos espaços vectoriais, etc., etc., são axiomáticas *não categóricas,* embora sejam *compatíveis* (isto é, existem realizações de cada uma dessas axiomáticas não isomorfas entre si).

Convém, por último, apresentar a axiomática de Peano, tal como esta aparece no *Compêndio*.

9. Há um assunto que ainda não ficou inteiramente esclarecido no *Guia do 6.º ano* e que convém, de futuro, ir a pouco e pouco precisando, a propósito do exemplo do BAILADO DAS HORAS e outros análogos: é o da *noção de congruência*. Note-se que em $\mathbb{Z}$ a definição deste conceito pode ser a seguinte:

Dados a, b, $m \in \mathbb{Z}$, sendo $m \neq 0$, diz-se que a é *congruente com* b *módulo* m, sse a−b é múltiplo de m.

Mas esta definição não é facilmente adaptável a $\mathbb{N}_0$, visto que, nesse caso, a−b só existe se $a \leqslant b$.

Quanto às classes de congruência, é claro que não serão as mesmas em $\mathbb{N}$, *em* $\mathbb{N}_0$ *e em* $\mathbb{Z}$. Suponhamos por, exemplo, m = 3; então as classes de congruência em $\mathbb{N}_0$ serão os conjuntos de valores que toma cada uma das expressães 3n, 3n+1, 3n+2, *quando* n *varia em* $\mathbb{N}_0$, ou seja:

$$\{3n\} = \{0,\ 3,\ 6,\ 9,\ \ldots\},$$

$$\{3n+1\} = \{1,\ 4,\ 7,\ 10,\ \ldots\},$$

$$\{3n+2\} = \{2,\ 5,\ 8,\ 11,\ \ldots\},$$

ao passo que, em $\mathbb{Z}$, são os conjuntos de valores que tomam aquelas mesmas expressões, *quando* n *varia em* $\mathbb{Z}$, ou seja:

$$\{3n\} = \{0,\ 3,\ -3,\ 6,\ -6,\ \ldots\}$$

$$\{3n+1\} = \{1,\ 4,\ -2,\ 7,\ -5,\ \ldots\}$$

$$\{3n+2\} = \{2,\ 5,\ -1,\ 8,\ -4,\ \ldots\}$$

A propósito do estudo dos anéis (no 6.º ano) convém demonstrar as seguintes propriedades, *relativamente a um módulo* m *qualquer:*

$$a \equiv a' \wedge b \equiv b' \Rightarrow a + b \equiv a' + b'$$

$$a \equiv a' \wedge b \equiv b' \Rightarrow ab \equiv a'b'$$

A demonstração é mais cómoda em $\mathbb{Z}$ do que em $\mathbb{N}_0$. As fórmulas $a \equiv a' \pmod m$, $b \equiv b' \pmod m$ significam então que a − a' e b − b' são múltiplos de *m* ou seja:

$$\exists\, p \in \mathbb{Z}:\ a - a' = mp \quad , \quad \exists\, q \in \mathbb{Z}:\ b - b' = mq$$

Por sua vez as fórmulas $a - a' = mp$, $b - b' = mq$ equivalem às seguintes:

$$a = a' + mp \quad , \quad b = b' + mq$$

donde

$$a + b = a' + b' + m(p+q)$$

$$ab = a'b' + m(a'q + b'p + mpq),$$

ou seja, pondo $p + q = h$, $a'q + b'q + mpq = k$:

$$(a+b) - (a'+b') = mh$$

$$ab - a'b' = mk$$

o que prova as teses, visto que $h, k \in \mathbb{Z}$.

Estas propriedades permitem provar que são unívocas as seguintes operações definidas no conjunto das classes de congruência módulo *m*:

$$\bar{a} + \bar{b} = \overline{a+b} \quad , \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

As mesmas propriedades permitem justificar a PROVA DOS NOVE, notando que $10 \equiv 1 \pmod 9$. Bastará fazer a justificação com exemplos numéricos, como o seguinte:

$$375 = 3 \times 10^2 + 7 \times 10 + 5 \quad , \quad 57 = 5 \times 10 + 7$$

$$375 \times 57 = 21375 = 2 \times 10^4 + 10^3 + 3 \times 10^2 + 7 \times 10 + 5$$

donde se deduz, relativamente ao módulo 9:

$$375 \equiv 3 + 7 + 5 \equiv 6 \quad , \quad 57 \equiv 5 + 7 \equiv 3$$

$$3 \times 6 = 18 \equiv 0 \quad , \quad 21375 \equiv 2 + 1 + 3 + 7 + 5 \equiv 0$$

10. Um outro ponto que ficou em suspenso foi o que se refere ao *conceito de partição*. A nossa opinião actual é que este conceito deve ser introduzido logo no 6.º ano, ou mesmo mais cedo, se a modernização do ensino da matemática se estender aos dois primeiros ciclos. Como sempre, convém partir de exemplos concretos e sugestivos.

A *classificação* dos vertebrados em *mamíferos, aves, répteis, batráquios, peixes* e *ciclóstomos* pode constituir um primeiro exemplo. Pondo (1):

V = {vertebrados} , M = {mamíferos} , A = {aves},

R = {répteis} , B = {batráquios} , P = {peixes} , C = {ciclóstomos}

vê-se que, pelo menos em teoria:

1) os conjuntos M, A, R, B, P, C são disjuntos dois a dois e nenhum deles é vazio,

2) $V = M \cup A \cup R \cup B \cup P \cup C$.

---

(1) Não esquecer que a expressão {vertebrados} se lê 'conjunto dos vertebrados', e analogamente para as outras do mesmo tipo.

Exprime-se este facto dizendo que o *conjunto de conjuntos* {M, A, R, B, P, C,} é uma *partição* (ou uma *classificação*) do conjunto V.

Analogamente, o conjunto, T, das turmas de um liceu, é uma *partição* de conjunto, A, dos alunos do liceu, visto que: 1) as turmas são conjuntos não vazios de alunos, disjuntos dois a dois; 2) a reunião desses conjuntos é A.

Por sua vez, o conjunto

$$\{\{1, 2\} , \{3, 4, 5\} , \{6\} , \{7, 8, 9, 10\}\}$$

é, por idênticas razões, uma partição de conjunto

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

A propósito, convém observar o seguinte: uma coisa é aquele *conjunto de conjuntos*, outra coisa é a sua *reunião*; o primeiro é de tipo 2 e o segundo de tipo 1, em relação a IN. Convirá, ainda, que os alunos indiquem *outras partições do mesmo conjunto.*

Consideremos, agora os seguintes conjuntos, no *universo* U *dos portugueses:*

$$C = \{\text{casados}\} , \ E = \{\text{empregados}\} , \ M = \{\text{maiores de 5 anos}\}$$

Imediatamente se reconhece que o conjunto {C, E, M} não é uma partição de U. Mas cada um destes conjuntos com o seu complementar constitui uma partição (ou classificação) do universo U:

$$\{C , \tilde{C}\} , \{E , \tilde{E}\} , \{M , \tilde{M}\}.$$

Chamam-se *classificações dicotómicas* as partições deste tipo (são também dicotómicas a classificação dos animais em vertebrados

e invertebrados, a das plantas em fanerogâmicas e criptogâmicas, etc.). Por sua vez, intersectando os conjuntos C, $\tilde{C}$, E, $\tilde{E}$, M, $\tilde{M}$ três a três, obtém-se a seguinte partição de U:

$$\{C\,E\,M\,,\ \tilde{C}\,E\,M\,,\ C\,\tilde{E}\,M\,,\ C\,E\,\tilde{M}\,,\ \tilde{C}\,\tilde{E}\,M\,,\ C\,\tilde{E}\,\tilde{M}\,,\ \tilde{C}\,E\,\tilde{M}\,,\ \tilde{C}\,\tilde{E}\,\tilde{M}\}$$

Por exemplo, $C\tilde{E}M$ = {casados, desempregados e maiores de 25 anos}.

Posto isto, o aluno será conduzido a reconhecer, também com exemplos (como se indica no *Guia do 6.º ano*), que *toda a relação de equivalência definida num universo* U *determina uma partição de* U *(em classes de equivalência).* Tal conclusão é assim obtida por indução experimental. Vamos em seguida dar a demonstração rigorosa do facto, *a título de curiosidade.*

Seja ρ uma relação de equivalência definida em U e ponhamos (1):

$$K(a) = \{x:\ x \rho a\},\ \forall\ a \in U$$

Assim, a cada elemento *a* de U o operador K faz corresponder um conjunto K(a), que *não é vazio,* visto que $a \in K(a)$ *(porquê?).* Notemos, agora, que:

$$(1) \qquad a \rho b \Leftrightarrow K(a) = K(b)$$

Com efeito, suponhamos $a \rho b$ e seja *x* um elemento qualquer de K(a). Então $x \rho a$ e, como $a \rho b$, também $x \rho b$ *(porquê?),* isto é, $x \in K(b)$. Seja agora y um elemento qualquer de K(b). Então $y \rho b$ e, como $b \rho a$ *(porquê?),* também em $y \rho a$, ou seja $y \in K(b)$. Logo K(a) = K(b).

Reciprocamente, se K(a) = K(b), tem-se $a \in K(b)$ e portanto $a \rho b$.

---

(1) Para comodidade, a expressão $x \rho y$ pode ler-se *'x é equivalente a y'.*

Posto isto, sejam *a* e a' dois elementos quaisquer de U e suponhamos que $K(a) \neq K(a')$. Vamos ver que, neste caso, K(a) e K(a') são *disjuntos*. Com efeito, se tal não sucede, existe um x tal que $x \in K(a)$ e $x \in K(a')$, ou seja tal que $x \rho a$ e $x \rho a'$, donde $a' \rho x$ e portanto $a' \rho a$ *(porquê?)*. Mas então, segundo a conclusão anterior $K(a') = K(a)$, o que é contra a hipótese.

Assim, todos os conjuntos K(a), K(a'), K(a''),..., tais que $a \not\rho a'$, $a \not\rho a''$, $a' \not\rho a''$,... são *disjuntos dois a dois* (e *não vazios*). Além disso, *a reunião desses conjuntos é* U, visto que cada elemento x de U pertence a um deles: o conjunto K(x). Por conseguinte, esses conjuntos (classes de equivalência) constituem uma partição de U,

q. e. d.

É evidente que, reciprocamente, *toda a partição de um conjunto* U *determina uma relação de equivalência em* U, *cujas* classes de equivalência *são os conjuntos da partição.*

Por exemplo, à partição do conjunto dos alunos de um liceu em turmas corresponde a relação de equivalência:

x *pertence à mesma turma que* y

Em resumo:

TEOREMA. *Qualquer que seja o conjunto* U *não vazio, cada relação de equivalência* ρ *em* U *determina uma partição* $\mathcal{P}$ *de* U *tal que*

$$x \rho y \Leftrightarrow \exists\, C \in \mathcal{P} :\ x,\ y \in C$$

Reciprocamente, cada partição de* U *determina uma relação de

equivalência ρ *em* U *que verifica esta condição. Em qualquer dos casos, pondo*

$$K(x) = \{y:\ y \rho x\}$$

K *é uma aplicação de* U *sobre* $\mathcal{P}$.

Como já foi observado no 6.º ano, a propósito das *definições por abstracção,* é mais natural, em muitos casos, considerar, em vez das classes de equivalência, as *propriedades* que definem essas classes (ou conjuntos). Neste caso, podíamos definir K como o operador que faz corresponder a cada $a \in U$ a *propriedade* que é comum a todos os elementos x tais que $x \rho a$ (e só a esses).

Em qualquer dos casos, diremos que K é um *operador de abstracção.* São exemplos de operadores de abstracção os seguintes:

direcção de, forma de, comprimento de, cor de, volume de, peso de, nacionalidade de, etc.

Assim, tem-se:

$$r//s \Leftrightarrow \text{direcção de r} = \text{direcção de s}$$

$$\mathcal{F} \sim \mathcal{G} \Leftrightarrow \text{forma de } \mathcal{F} = \text{forma de } \mathcal{G}, \text{ etc.}$$

sendo r, s rectas e $\mathcal{F}, \mathcal{G}$ figuras quaisquer de $\mathcal{E}$.

Em qualquer dos casos, o operador de abstracção converte a relação de equivalência em relação de identidade. Por isso mesmo se chama 'operador de abstracção', visto que *abstrai,* por assim dizer das diferenças que há entre dois elementos equivalentes.

Recordemos, ainda, o seguinte exemplo:

$$A \text{ é equivalente a } B \Leftrightarrow \# A = \# B$$

sendo A e B conjuntos *quaisquer*. Neste caso, como também já foi observado no *Guia do 6.º ano,* o universo *não é um conjunto,* mas sim uma *classe* (a classe de *todos* os conjuntos), na acepção mais larga atribuída à palavra 'classe'.

11. No decurso das suas aulas – e em especial no 6.º ano, a propósito do estudo da lógica – o professor deverá recordar como se definem os conceitos de *divisor, de múltiplo,* de *máximo divisor comum,* de *mínimo múltiplo comum* e de *número primo* (de preferência em IN). Convirá definir 'máximo divisor comum' e 'mínimo múltiplo comum', atribuindo às palavras 'máximo' e 'mínimo' o sentido usual, ligado à *relação de grandeza.*

Deverá ainda ser recordado o *algoritmo de Euclides* para o m. d. c., bem como o facto de um número natural ser sempre decomponível em factores primos (e de um só modo, à parte a ordem).

Quanto a demonstrações, poucas são necessárias e podem ser feitas no 6.º ano, após o capítulo III do *Compêndio, com introdução heurística:*

1.º CENTRO DE INTERESSE: *Redescobrir o algoritmo de Euclides.* São dados dois números naturais a, b e pretende-se achar o m. d. c. (a, b). Suponhamos $a \geqslant b$. Dois casos se podem dar:

1) a *é divisível* por b. Qual é então o máximo divisor comum? Evidentemente, b.

2) a *não é divisível por* b. Seja, então, q o quociente inteiro e r o resto da divisão de *a* por *b* (1):

$$(1) \qquad a = bq + r$$

(1) Admite-se nesta altura que o PROBLEMA DA DIVISÃO INTEIRA é sempre possível e determinado.

Seja, agora, *n* um divisor comum qualquer de a e de b. Será *n* também divisor de r? *Parece que sim.* Vamos ver se é verdade. Designemos por a' e b' os quocientes de a e de b por n:

$$a = a'n, \quad b = b'n$$

Então de (1) vem:

$$a'n = b'nq + r$$

donde:

$$r = (a' - b'q)n$$

Portanto *n* também é divisor de r, *como se previu.*

Seja por sua vez *m* um divisor comum qualquer de b e de r. Será também divisor de *a*? Designemos por b' e r' os quocientes de b e de r por m:

$$b = b'm \quad , \quad r = r'm$$

Então, $a = b'mq + r'm = (b'q + r')m$

Logo $m \dashv a$, *como se previu.*

CONCLUSÕES QUE O ALUNO DEVE TIRAR POR SI:

O conjunto dos divisores comuns de a *e* b *é o mesmo que o conjunto dos divisores comuns de* b *e* r (porquê?).

Logo

$$\text{m. d. c. } (a, b) = \text{m. d. c. } (b, r) \qquad \textit{(porquê?)}$$

Pergunta-se: *Que ideia nos sugere este resultado para achar o* m. d. c. (a, b)? A resposta deve partir espontaneamente do aluno(1):

O problema de achar o m. d. c. (a, b) foi reduzido ao de achar o m. d. c. (b, r). Seja

$$b = rq' + r' \quad , \quad \text{com } r' < r \ (q' \in \mathbb{N},\ r' \in \mathbb{N}_0).$$

Se $r' = 0$, então $r \dashv b$ e, portanto, $r = \text{m. d. c. } (b, r) = \text{m. d. c. } (a, b)$.

Se $r' \neq 0$, seja

$$r = r'q'' + r'' \quad , \quad \text{com } r'' < r' \ (q'' \in \mathbb{N},\ r'' \in \mathbb{N}_0).$$

E, agora, a situação repete-se. Pergunta-se:

Pode acontecer que nunca se chegue a resto zero por este caminho? É preciso lembrar que

$$a > b > r' > r'' > \ldots$$

Ora, se nunca se chegasse a resto zero, teríamos assim uma *sucessão infinita decrescente de números naturais,* o que é impossível. Impossível porquê? O aluno sabe-o por intuição ou por experiência. Mas o facto só pode ser demonstrado por indução matemática, o que não interessa fazer no 6.º ano (2).

Por consguinte, o referido processo (*algoritmo de Euclides* ou *método das divisões sucessivas)* conduz, sempre, a um resto

---

(1) Antes das considerações gerais que vão seguir-se, agora, convém considerar um caso particular, por exemplo a = 950 e b = 144.

(2) Ver-se-á mais adiante.

nulo: *o último resto não nulo que se obtém é precisamente o* m. d. c. (a, b).

Posto isto, nova pergunta:

O que acontece quando, numa divisão inteira, se multiplica o dividendo e o divisor por um mesmo número natural?

É provável que o aluno já não se lembre da resposta; mas é talvez melhor assim, porque pode então *redescobri-la. Sejam* a, $b \in \mathbb{N}$ e

$$a = bq + r \quad , \quad \text{com } q, r \in \mathbb{N}_0 \quad \text{e} \quad r < b$$

Multiplicando por qualquer $k \in \mathbb{N}$, virá então:

$$ak = (bk)q + rk \quad , \quad rk < bk$$

Conclusão: *o quociente não muda e o resto vem multiplicado por* k.

E agora:

Que propriedade pode resultar daqui para o m. d. c. ?

Multiplicando a e b por k, os sucessivos restos, no algoritmo de Euclides vêm todos multiplicados por k e, portanto, o mesmo acontece ao m. d. c. *Conclusão:*

$$\text{m. d. c. } (a, b) = D \Rightarrow \text{m. d. c. } (ak, bk) = kD$$

(Traduzir em linguagem comum)

Suponhamos, agora, que k é um divisor comum de a e de b, e seja

$$a = a'k \quad , \quad b = b'k \quad , \quad \text{m. d. c. } (a', b') = D'$$

Então, pela propriedade anterior:

$$\text{m. d. c. } (a'k,\ b'k) = kD'$$

Conclusão:

Se $k \dashv a$ e $k \dashv b$, então $k \dashv \text{m. d. c. } (a, b)$ e

$$\text{m. d. c. } (a, b) = D \Rightarrow \text{m. d. c. } (a/k\ ,\ b/k) = D/k$$

(Traduzir tudo isto em linguagem comum)

Por outro lado, como (1)

$$k \dashv \text{m. d. c. } (a, b) \Rightarrow k \dashv a \wedge k \dashv b$$

segue-se a *propriedade característica do m.d.c.:*

$$k \dashv a \wedge k \dashv b \Leftrightarrow k \dashv \text{m. d. c. } (a, b)$$

Recorde-se, agora, a DEFINIÇÃO:

Diz-se que a é *primo com* b , sse m. d. c. (a, b) = 1

---

(1) É conveniente mostrar que a relação $\dashv$ definida em IN é uma relação de ordem parcial lata. É costume usar o sinal | como abreviatura de 'divide'. Mas, tratando-se de uma relação que não é simétrica, parece-nos preferível o sinal que adoptamos. Neste caso, o sinal H significará 'o múltiplo de' (relação: inversa da primeira).

Posto isto, apresente-se a seguinte hipótese em IN:

$$k \dashv ab \wedge k \text{ é primo com } a$$

e procure-se levar o aluno a uma conclusão. Que quer dizer 'k é primo com a '? Resposta:

$$\text{m. d. c. } (a, k) = 1$$

Que se conclui daqui para o produto ab? Resposta:

$$\text{m. d. c. } (ab, kb) = b \quad \textit{(porquê?)}$$

Mas olhe-se de novo para a hipótese: $k \dashv ab$. Ora $k \dashv kb$. Logo $k \dashv b$ *(porquê?)*.

RECAPITULANDO:

$$k \dashv ab \wedge k \text{ é primo com } a \Rightarrow k \dashv b$$

Traduzindo em linguagem comum:

> Se um número divide um produto de dois factores e é primo com um deles, então divide o outro factor.

Este é o importante TEOREMA DE EUCLIDES, que nos vai servir de base para o estudo a seguir.

2.º CENTRO DE INTERESSE: *Redescobrir o teorema da decomposição de um número em factores primos.*

Muitas vezes, interessa decompor um número natural em factores tão pequenos quanto possível, mas todos diferentes de 1. Por exemplo:

$$20 = 2 \times 10 = 2 \times 2 \times 5$$

$$90 = 2 \times 45 = 2 \times 9 \times 5 = 2 \times 3 \times 3 \times 5, \text{ etc.}$$

Verificou-se então o seguinte: acaba-se por chegar sempre a factores que *já não se podem decompor mais,* e a última decomposição assim obtida é sempre a mesma *qualquer que seja o modo como se faz a decomposição.* Mas trata-se, por enquanto, de uma *verificação experimental.* Pergunta-se:

Será possível demonstrar rigorosamente estes factos, com toda a generalidade?

Os factores indecomponíveis a que se chega (a que poderíamos chamar os *átomos* da decomposição) têm o nome de *números primos* (1). Portanto, um número natural *a* diz-se *primo,* sse é diferente de 1 e não pode decompor-se num produto:

$$a = m \times n \quad , \quad \text{com} \quad m \neq 1 \quad \text{e} \quad n \neq 1$$

É claro que esta definição equivale à seguinte:

DEFINIÇÃO. Diz-se que um número *a* é *primo,* sse é diferente de 1 e só é divisível por 1 e por a.

---

(1) Etimologicamente, 'número primo' significa 'número primeiro' (ou 'número primitivo').

Simbolicamente (no universo IN):

$$a \text{ é primo} \underset{\cdot}{\Leftrightarrow} a \neq 1 \wedge (x \dashv a \underset{x}{\Rightarrow} x = 1 \vee x = a)$$

Um número diz-se *composto* (ou *decomponível*), sse é diferente de 1 e não é primo.

Seja *a* um número composto. Então existem $m \neq 1$ e $n \neq 1$, tais que

$a = m \times n$, sendo portanto $m < a$ e $n < a$ *(porquê?)*

Se m *e* n *são primos, o número* a *está decomposto em factores primos*. Se não, um pelo menos dos números *m, n* não é primo; seja por exemplo m; então existem $m' \neq 1$ e $n' \neq 1$, tais que $m = m' \times n'$; portanto:

$$a = m' \times n' \times n \qquad (m' < m \ , \ n' < m)$$

Se os números m', n', n são primos, o número *a* está *decomposto em factores primos*. Se não, um pelo menos dos factores é decomponível como no caso anterior. E assim sucessivamente. Enquanto houver um factor que não seja primo, o processo continuará. Pergunta-se agora:

Este processo poderá não ter fim? O que aconteceria se o processo não mais terminasse? A resposta é, naturalmente:

Nesse caso, as sucessivas decomposições davam origem a uma infinidade de números cada vez mais pequenos, o que já sabemos que é impossível. Logo:

O número acaba sempre por ficar decomposto em factores primos.

Agora resta só um ponto a esclarecer:

Se fizermos a decomposição de um número a em factores primos por caminhos diferentes, os resultados poderão ser diferentes?

Suponhamos que se obteve, por dois processos:

$$a = p_1 p_2 \cdots p_m \quad , \quad a = q_1 q_2 \cdots q_n$$

sendo $p_1, \ldots, p_m, q_1, \ldots q_n$ números primos. Então

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \tag{2}$$

Suponhamos, por exemplo, $m \leqslant n$ e vejamos se p_1 é igual a algum dos factores do 2.º membro. Se $p_1 \neq q_1$, então p_1 é primo com q_1 *(porquê?)* e como divide o produto de q_1 por $q_2 \ldots q_n$, então divide $q_2 \ldots q_n$. Se $p_1 \neq q_2$, então p_1 é primo com q_2 e, portanto, divide $q_3 \ldots q_n$. E assim sucessivamente, até chegar q_n. *Logo* p_1 *tem de ser igual a um dos números* $q_1, \ldots, q_n$. Como o produto é comutativo, podemos, por comodidade, supor escolhida a ordem dos factores de modo que seja $p_1 = q_1$. Então de (2) vem:

$$p_2 \cdots p_m = q_2 \cdots q_n$$

Raciocinando de modo análogo, concluímos que p_2 é igual a um dos factores do 2.º membro e podemos supor escolhida a ordem dos factores de modo que seja $p_2 = q_2$. Procedendo assim sucessivamente, conclui-se que

$$p_1 = q_1 \quad , \quad p_2 = q_2 \quad , \quad \cdots \quad , \quad p_m = q_m$$

Ora $m \leqslant n$, por hipótese. Poderá ser $m < n$? Não, porque, nesse caso,

dividindo ambos os membros do (2) por $p_1 \ldots p_m$ obtínhamos $1 = q_{m+1} \ldots q_n$, o que é impossível *(porquê?)*. Em conclusão:

TEOREMA. *Um número composto admite sempre uma e uma só decomposição em factores primos (à parte a ordem destes).*

(Normalmente os factores são escritos por ordem crescente de grandeza, em sentido lato.)

É claro que a demonstração anterior (aliás a seguida no ensino tradicional) tem carácter parcialmente intuitivo. Uma demonstração rigorosa só poderia ser dada no 7.º ano, pelo método de indução matemática; mas não vale a pena fazê-lo.

Convém ainda recordar o processo usual, para decompor um número em factores primos, e apontar o teorema segundo o qual o conjunto dos números primos é infinito (pode omitir-se a demonstração).

Designemos por p_n o número primo de ordem *n*, para cada $n \in \mathbb{N}$. Fica, assim, definida a *sucessão dos números primos:*

$$p_1 = 2 \ , \ p_2 = 3 \ , \ p_3 = 5 \ , \ \ldots$$

O teorema anterior equivale a dizer o seguinte:

Para cada número composto a, *existe sempre uma e uma só sucessão* x_n *de números inteiros absolutos tal que*

$$a = 2^{x_1} \times 3^{x_2} \times 5^{x_3} \times 7^{x_4} \times 11^{x_5} \times \ldots \times p_n^{x_n} \ldots$$

sendo $x_n = 0$ *a partir de certa ordem.*

Por exemplo, se $a = 20$, tem-se $x_1 = 2$, $x_2 = 0$, $x_3 = 1$, $x_n = 0$ para $n > 3$.

Deste modo, como se vê, a sucessão dos números primos desempenha, no *semigrupo multiplicativo* IN, um papel análogo ao de uma *base de um espaço vectorial de dimensão infinita*. Então os expoentes $x_1, x_2, \ldots, x_n, \ldots$ da decomposição em factores primos são comparáveis às *componentes* de um vector nessa base; *multiplicar* dois elementos de IN equivale a *somar* ordenadamente as respectivas componentes.

Isto mostra bem como é diferente a estrutura dos semigrupos $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$; uma caracterização axiomática do segundo é, com certeza, muito mais complicada que a do primeiro (1).

12. A determinação do m. m. c. a partir do m. d. c. ou a determinação de ambos por decomposição em factores primos podem também ser assuntos a recordar no 6.º ano (há 40 anos, estes assuntos faziam parte do programa do ensino primário!). *O que deve inteiramente abolir são clássicos problemas-cliché, sem interesse algum, a que acabou por se reduzir quase todo o ensino da aritmética racional no* 3.º *ciclo, desvirtuando-se por completo a sua finalidade.*

Mas a inclusão destes assuntos, mesmo abreviadamente, como atrás se indica, no moderno 6.º ano, levanta o eterno problema do tempo: para o tratar de maneira satisfatória, há que eliminar uma outra parte do programa. Propomos que esta parte a suprimir seja a *introdução à geometria analítica no espaço.*

Não nos parece grave dispensar, no ensino liceal, o estudo da geometria analítica no espaço. Pelo contrário, o teorema da decomposição em factores primos é essencial para poder *justificar a intro-*

---

(1) O semigrupo $(\mathbb{N}, +)$ admite um único automorfismo: a identidade. O semigrupo $(\mathbb{N}, \cdot)$ admite uma infinidade de automorfismos, determinados por todas as aplicações biunívocas do conjunto dos números primos sobre si mesmo.

dução dos números irracionais e deve, por esse e outros motivos, fazer parte da cultura geral que compete ao ensino secundário. O aluno a quem se consegue despertar o espírito crítico e a curiosidade intelectual, de acordo com as finalidades do ensino, sente vivamente a necessidade de uma tal justificação e mostra-se insatisfeito quando não a encontra.

Poderiam ser apresentados vários exemplos, em prova desta afirmação. Não devem ser precisos milagres, para convencer os incrédulos... Entre outros casos, é de assinalar a tentativa do aluno Fernando Saraiva de uma turma-piloto do Liceu de Oeiras, para demonstrar o seguinte

TEOREMA: *Sendo* a *e* n *números naturais, se não existe nenhum número natural* x *tal que* $x^n = a$, *também não existe nenhum número fraccionário que verifique a mesma condição (isto é, não existe* $\sqrt[n]{a}$ *em* (Q).

Para isso, o referido aluno estabeleceu previamente um outro teorema e um corolário, de maneira bastante curiosa, revelando qualidades muito apreciáveis, que devem ser encorajadas. Mas os seus raciocínios omitem um ponto: admite implicitamente, em certa passagem, sem o mencionar, o seguinte facto essencial:

> Se um número primo divide um produto, divide pelo menos um dos factores do produto.

Este teorema(1), consequência imediata do TEOREMA DE EUCLI-

(1) Mais precisamente, o aluno utiliza o chamado 'teorema de Gauss', caso particular deste aqui enunciado (cf. 'Compêndio de Aritmética Racional', do Dr. J. J. Gonçalves Calado).

DES, pode ser usado directamente para demonstrar o teorema anterior. Bastará fazê-lo num caso particular, para dar a ideia:

Seja $a = 5$ e $n = 3$. É claro que não existe nenhum número natural x tal que $x^3 = 5$ (*porquê?*). Suponhamos agora que existe um número fraccionário x tal que $x^3 = 5$. Esse número poderá ser representado por uma *fracção irredutível* m/n, isto é, tal que m e *n* sejam *primos entre si.* Tem-se então $(\frac{m}{n})^3 = 5$ ou seja

$$m^3 = 5n^3 \tag{1}$$

Mas, nesse caso, $5 \dashv m^3$ e portanto $5 \dashv m$ (*porquê?*). Existe pois um $k \in \mathbb{N}$ tal que $m = 5k$ e, assim, atendendo a (1),

$$5^3 k^3 = 5 n^3, \quad \text{donde:} \quad 5^2 k^2 = n^3$$

Então $5 \dashv n^3$ e portanto $5 \dashv n$. Ora já vimos que $5 \dashv m$. Mas isto é absurdo, porque tínhamos suposto que *m* e *n* são primos entre si.

Logo $\sim \exists\, x \in \mathbb{Q}^+ : x^3 = 5$; e, como também não existe nenhum $x < 0$ tal que $x^3 = 5$, conclui-se:

Não existe $\sqrt[3]{5}$ *em* $\mathbb{Q}$.

O referido teorema, caso particular do teorema de Euclides, pode apresentar-se com o seguinte aspecto:

O anel A_μ *das classes de congruência módulo* μ *não tem divisores de zero, sse* μ *é primo.*

A partir daqui, demonstra-se que:

A_μ *é um corpo, sse* μ *é primo.*

Com efeito, suponhamos que μ é primo e seja *a* um elemento qualquer de A_μ diferente de 0. Então, a aplicação

$$x \curvearrowright ax \text{ de } A_\mu \text{ em } A_\mu$$

é *injectiva* (*porquê?*) e, como A_μ é finito, a aplicação é *sobrejectiva*. Logo existe um elemento x de A_μ (e um só) tal que $ax = 1$,

q. e. d.

Como aplicação do TEOREMA DA DECOMPOSIÇÃO EM FACTORES PRIMOS convém ainda propor, aos alunos, o seguinte exercício:

Demonstrar que, se um número natural a *não é potência de expoente inteiro de* 10, *então* $\log_{10} a$ *é um número irracional.*

13. Vamos terminar este capítulo com mais uma observação. Várias vezes temos salientado, invocando o testemunho de grandes cientistas, que o processo da criação científica começa pela *intuição*; e temos insistido em que o ensino de qualquer assunto deve igualmente começar pela *fase intuitiva*. Mas a *fase racional,* que se lhe segue, é igualmente indispensável. Especialmente em matemática, nenhum resultado pode merecer inteira confiança, enquanto não for sancionado pela *razão,* isto é, demonstrado logicamente. Por isso, se é muito importante estimular no aluno a intuição e a imaginação criadora, não menos importante é desenvolver nele o espírito crítico, o hábito da análise lógica e do raciocínio rigoroso.

Numa tentativa de demonstração, tal como num cálculo, basta um pequeno lapso – a simples ausência de um elo quase imperceptível – para faslear o resultado. Por isso, todos os pormenores da

demonstração devem ser analisados, por assim dizer, *à lupa. De contrário, o aluno será capaz de aceitar como verdadeiras várias proposições falsas, após uma cadeia de raciocínios que lhe pareçam impecáveis.*

Note-se bem:

Esta situação é muito mais frequente do que possa parecer à primeira vista!

Um dos principais deveres do ensino é ensinar o aluno a pensar.

E todo o aluno deve ambicionar adquirir autonomia mental e espírito crítico suficiente, para não se deixar facilmente convencer com argumentos errados – e menos ainda com *argumentos de autoridade.*

Índice