CENTRO DE MATEMÁTICA
UNIVERSIDADE DO PORTO

Parecer Sobre a Pretensa Demonstração de Carlos Correia de Matos

O argumento apresentado por Carlos Correia de Matos nas páginas 13 e 14 (posteriormente repetido nas páginas 15 e 19, aqui numa série de equivalências escritas de um modo formalmente incorreto) do documento complementar que se encontra na página relativa à sua petição não é válido. Há nele uma confusão persistente entre números e polinómios. Logo no Passo 0 é afirmado que $x^n + y^n$ é divisível por $x + y$ se e só se n é ímpar. Isto é verdade no anel dos polinómios de duas variáveis, mas falso quando x e y são inteiros, como no argumento em causa. Neste caso, apenas o "se" é verdadeiro, podendo ser dada uma infinidade de contra-exemplos para o "só se", como no caso em que $x = y$, pois que $2x$ divide $2x^n$ para todo o n, seja n ímpar ou par.

Porém, o erro mais sério encontra-se no Passo 2, onde Carlos Correia de Matos usa um facto que é válido no anel dos polinómios: se $x - z'$ divide $x^n - z^n$ então z' é raiz do polinómio $x^n - z^n$, mas esquecendo-se que aqui está a lidar com números, mais exatamente com uma pretensa solução da equação de Fermat, e não com polinómios. E, tratando-se de números inteiros, esta sua inferência está errada. De facto, não faz sequer sentido, pois sendo z', x e z números inteiros, a frase «z' é raiz do polinómio $x^n - z^n$» carece de qualquer significado. Carlos Correia de Matos usa isto para concluir que $z' = z$. Poderia acontecer que, apesar do raciocínio estar errado, a sua conclusão fosse válida por uma outra qualquer razão. Acontece que mesmo isso não é verdade, podendo ser dada uma infinidade de contra-exemplos. Deixo aqui três: $6 - 5$ divide $6^n - 2^n$, para todo $n \in \mathbb{N}$, e no entanto $5 \neq 2$; também $7 - 5$ divide $7^n - 3^n$, para todo $n \in \mathbb{N}$, e $5 \neq 3$; finalmente, $91 - 2$ divide $91^n - 90^n$ sempre que n é da forma $11 + 88k$ ($k \in \mathbb{N}_0$), e no entanto $2 \neq 90$.

De facto, é mesmo possível ver que uma abordagem no contexto em que é feita a de Carlos Correia de Matos está condenada ao fracasso. Isto porque se usam aí apenas propriedades básicas de anéis comutativos e acontece que há anéis comutativos nos quais a equação de Fermat admite soluções não-triviais, como o anel $\mathbb{Z}[\sqrt{3}\,i]$, no qual se verifica (sendo $n \in \mathbb{N}$):

$$\left(1+\sqrt{3}\,i\right)^n + \left(1-\sqrt{3}\,i\right)^n = 2^n, \qquad \text{para todo } n \equiv \pm 1 \pmod 6.$$

É claro que a existência destas soluções invalida qualquer abordagem de carácter algébrico elementar.

Porto, 3 de junho de 2020

António José de Oliveira Machiavelo