## NOTA DE AULA

# Uma outra condição necessária e suficiente para que um inteiro seja regular módulo n

por José Morgado

Instituto de Matemática; Universidade Federal de Pernambuco, Brasil

1. Num artigo anterior, introduzimos a definição de *inteiro regular módulo $n$*: um inteiro $a$ diz-se regular módulo $n$, se existe algum inteiro $x$ tal que

$$a^2 x \equiv a \pmod{n}.$$

Mostrámos ([1], teorema 2) que $a$ é regular módulo $n$, se e só se o máximo divisor comum $(a,n)$, de $a$ e $n$, é divisor unitário de $n$, quer dizer, $(a,n)$ é primo com o quociente $\frac{n}{(a,n)}$. Em símbolos,

$$(1) \qquad (a,n) \mid^* n.$$

Num outro artigo ([2], teorema 2), mostrámos que $a$ é regular módulo $n$, se e só se

$$(2) \qquad a^{1+\varphi(n)} \equiv a \pmod{n}$$

onde $\varphi(n)$ designa, como de costume, o número de inteiros positivos primos com $n$ e que não excedem $n$.

Nesta nota vamos dar uma outra condição para que um inteiro seja regular módulo $n$, em termos de um certo semigrupo gerado por esse inteiro.

2. Designemos por $S$ o semigrupo formado pelo conjunto $\{0,1,2,\cdots,n-1\}$ munido da operação de produto módulo $n$. Seja $b$ um inteiro qualquer e seja $a$ o elemento de $S$ tal que $b \equiv a \pmod{n}$. Então é imediato que $b$ é regular módulo $n$, se e só se $a$ é regular módulo $n$. Além disso, se $y$ é um inteiro tal que

$$a^2 y \equiv a \pmod{n},$$

então existe evidentemente um elemento $x$ em $S$ tal que, no semigrupo $S$, se tem $a^2 x = a$. Um tal elemento $x$ é justamente o resto da divisão de $y$ por $n$.

Por isso, nesta nota, limitamo-nos a considerar os inteiros pertencentes ao semigrupo $S$.

Vamos estabelecer o seguinte

TEOREMA: *Seja* a ∈ S; *então* a *é regular módulo* n, *se e só se o subsemigrupo de* S *gerado por* a *é um grupo.*

DEM.: Com efeito, suponhamos que $a$ é regular módulo $n$ e seja $A$ o subsemigrupo gerado por $a$. Então de (2) resulta que a igualdade

$$a^{1+\varphi(n)} = a$$

é válida no semigrupo $S$ e, portanto, $a^{\varphi(n)}$ é elemento neutro de $A$ (tendo-se, evidentemente, $a^{\varphi(n)} = 1$, se e só se $a$ é primo com $n$).

Todo elemento de $A$ é da forma $a^t$ com $1 \leq t \leq \varphi(n)$; na verdade, se $t'$ é um inteiro maior que $\varphi(n)$ e não divisível por $\varphi(n)$, então tem-se $a^{t'} = a^t$, onde $t$ é o resto da divisão de $t'$ por $\varphi(n)$ e, se $t'$ é divisível por $\varphi(n)$, então tem-se $a^{t'} = a^{\varphi(n)}$.