ANO XXXIII — N.os 125-128 GAZETA DE MATEMÁTICA JANEIRO/DEZ. — 1972

EDITOR: *Gazeta de Matemática, Lda.* ADMINISTRADOR: *A. Sá da Costa*

REDACTORES: *J. Gaspar Teixeira, J. Morgado e J. da Silva Paulo*

Composto na Tipografia Matemática, Lda. — Rua Diário de Notícias, 134 - 1.º - Esq. — Telef. 36 94 49 — LISBOA

NOTA DE AULA

Inteiros regulares módulo n

por José Morgado

Instituto de Matemática, Universidade Federal de Pernambuco, Brasil

Introdução

Recordemos que um elemento a de um anel A se diz *regular* (segundo VON NEUMANN), se existe em A algum elemento x tal que $axa = a$.

Parece então natural dizer que um inteiro a é *regular módulo* n, se existe algum inteiro x para o qual é válida a congruência

$$(1) \qquad a^2 x \equiv a \pmod{n}.$$

Resulta imediatamente da definição que os múltiplos de n e os inteiros primos com n são regulares módulo n, qualquer que seja o inteiro n. Geralmente, porém, há outros inteiros regulares módulo n. Assim, por exemplo, para $n = 12$, os inteiros regulares módulo n são aqueles que são congruentes com algum dos inteiros 0, 1, 3, 4, 5, 7, 8, 9, 11.

O objectivo desta nota é precisamente estudar o conjunto dos inteiros regulares módulo n.

Em toda esta nota, n designará um inteiro maior que 0.

1. Condições de regularidade.

Se a e b são inteiros, representaremos por (a, b) o máximo divisor comum positivo de a e b.

TEOREMA 1. *É condição necessária e suficiente para que o inteiro* a *seja regular módulo* n, *que se tenha*

$$(a, n) = (a^2, n).$$

DEM. Com efeito, suponhamos que a é regular módulo n. Então, da solubilidade da congruência (1), resulta que $(a^2, n) \mid a$. Logo, tem-se $(a^2, n) \mid (a, n)$ e, como, por outro lado, $(a, n) \mid (a^2, n)$, resulta que $(a, n) = (a^2, n)$.

Inversamente, se $(a, n) = (a^2, n)$, então existem inteiros u e v tais que

$$(a, n) = a^2 u + nv.$$

Designando por q o quociente de a por (a, n), tem-se

$$a = (a, n) q = a^2 uq + nvq,$$

o que mostra que a congruência (1) tem, pelo menos, a solução $x \equiv u\,q \pmod{n}$.

COROLÁRIO. *Se* a *é regular módulo* n, *então tem-se* $(a^m, n) = (a, n)$, *qualquer que seja o inteiro* $m > 1$.

Diz-se que o inteiro positivo d é um *divisor unitário* de n (em símbolos, $d \mid^* n$), se d é um divisor de n que é primo com o divisor complementar, i. e., $d \mid n$ e

$$\left(d, \frac{n}{d}\right) = 1.$$

É claro que, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde os p_i são primos distintos, então o número de divisores unitários de n é igual a 2^k, número de partes do conjunto $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots \cdots, p_k^{\alpha_k}\}$.

É também imediato que, se n_1 e n_2 são inteiros primos entre si, $d_1 \mid^* n_1$ e $d_2 \mid^* n_2$, então $d_1 d_2 \mid^* n_1 n_2$; inversamente, se $d \mid^* n_1 n_2$, com $(n_1, n_2) = 1$, então existem d_1 e d_2 tais que

$$d = d_1 d_2, \quad d_1 \mid^* n_1 \quad \text{e} \quad d_2 \mid^* n_2;$$

basta tomar $d_1 = (d, n_1)$ e $d_2 = (d, n_2)$.

O conceito de divisor unitário intervem na formulação do seguinte

TEOREMA 2. *É condição necessária e suficiente para que o inteiro* a *seja regular módulo* n, *que se tenha*

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

DEM. Na verdade, suponhamos que a é regular módulo n. Pretendemos mostrar que

$$\left((a, n), \frac{n}{(a, n)}\right) = 1.$$

Imaginemos que se tinha

$$\left((a, n), \frac{n}{(a, n)}\right) = d > 1$$

e seja $p^k \mid^* d$. Então, de $p^k \mid (a, n)$ e $p^k \mid \frac{n}{(a, n)}$, resultaria $p^{2k} \mid n$.

Por outro lado, de $p^k \mid a$, resultaria $p^{2k} \mid a^2$. Ter-se-ia, portanto,

$$p^{2k} \mid (a^2, n).$$

Mas, pelo teorema anterior, $(a^2, n) = (a, n)$ e, por consequência, $p^{2k} \mid n$ e $p^{2k} \mid a$ e, como $p^k \mid \frac{n}{(a, n)}$, resultaria que $p^{3k} \mid n$.

De $p^{2k} \mid a$, resultaria $p^{4k} \mid a^2$, donde $p^{3k} \mid (a^2, n)$, i. e., $p^{3k} \mid (a, n)$ e, como $p^k \mid \frac{n}{(a, n)}$, concluir-se-ia que $p^{4k} \mid n$.

Ter-se-ia então $p^{2k} \mid \frac{n}{(a, n)}$ e $p^{2k} \mid (a, n)$, i. e., $p^{2k} \mid d$, o que contradiz a hipótese de ser p^k um divisor unitário de d.

Esta contradição mostra que $d = 1$, como se pretendia.

Inversamente, suponhamos que $(a, n) \mid^* n$.

Se fosse $(a^2, n) \neq (a, n)$, como $(a, n) \mid (a^2, n)$, ter-se-ia $(a^2, n) = (a, n)\,r$, onde $r > 1$. Designando por p um divisor primo de r, de $p \mid (a^2, n)$, resultaria $p \mid a^2$ e $p \mid n$, donde $p \mid a$ e $p \mid n$, donde $p^2 \mid (a^2, n)$ e, como $(a^2, n) \mid n$, ter-se-ia também $p \mid \frac{n}{(a, n)}$, visto que $r \mid \frac{n}{(a, n)}$, contrariamente à hipótese de ser (a, n) um divisor unitário de n.

Logo, $(a^2, n) = (a, n)$ e, por consequência, a é regular módulo n.

COROLÁRIO 1. *É condição necessária e suficiente para que todo inteiro seja regular módulo* n, *que* n *seja livre de quadrados.*

DEM. Com efeito, se n é livre de quadrados, i. e., se $n = 1$ ou $n = p_1 p_2 \cdots p_k$, onde os p_i são primos distintos, então todo divisor de n é evidentemente um divisor unitário de n, tendo-se, por consequência, $(a, n) |^* n$ para todo a, i. e., todo inteiro a é regular módulo n.

Inversamente, se $(a, n) |^* n$ para todo inteiro a, então necessariamente n é livre de quadrados, visto que, se para algum primo p se tivesse $p^2 | n$, então (p, n) não seria divisor unitário de n e, portanto, p não seria regular módulo n.

COROLÁRIO 2. *Se* $n > 1$, *é condição necessária e suficiente para que somente os inteiros primos com* n *e os múltiplos de* n *sejam regulares módulo* n, *que* n *tenha um único divisor primo.*

DEM. De facto, se n tivesse mais que um divisor primo, então n teria pelo menos um divisor unitário d diferente de 1 e diferente de n e d seria regular módulo n.

Se, pelo contrário, n tem um só divisor primo, os únicos divisores unitários de n são 1 e n e, portanto, os inteiros regulares módulo n são os primos com n e os múltiplos de n.

2. O semigrupo dos inteiros regulares módulo n.

Pode ter-se $a^2 x \equiv a \pmod{n}$, sem que x seja regular módulo n; assim, por exemplo, tem-se $8^2 \cdot 2 \equiv 8 \pmod{12}$ e, no entanto, 2 não é regular módulo 12, mas tem-se também $8^2 \cdot 8 \equiv 8 \pmod{12}$ e 8 é regular módulo 12.

TEOREMA 3. *Se o inteiro* a *é regular módulo* n, *então existe pelo menos uma solução* x *da congruência* $a^2 x \equiv a \pmod{n}$ *que também é regular módulo* n.

DEM. Seja y um inteiro tal que $a^2 y \equiv a \pmod{n}$. Então, como

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

vê-se que $a y^2$ é uma solução daquela congruência. Além disso, tem-se

$$(a y^2)^2 \cdot a = a^2 y \cdot y^5 a \equiv a^2 y^5 = a^2 y \cdot y^2 \equiv a y^2 \pmod{n},$$

o que mostra que $a y^2$ é regular módulo n, como se pretendia.

Designemos por $R(n)$ o conjunto dos inteiros regulares módulo n, compreendidos no intervalo fechado $[0, n-1]$. É imediato que tal conjunto constitui um semigrupo com respeito ao produto módulo n. A este semigrupo chamaremos *semigrupo dos inteiros regulares módulo* n.

É claro que todo inteiro regular módulo n é congruente com um e um só elemento de $R(n)$.

Assim, pelo Teorema 3, a equação $a^2 x = a$ onde $a \in R(n)$, tem pelo menos uma solução no semigrupo $R(n)$. Na realidade, o número de soluções em $R(n)$ é precisamente igual a $(a^2, n) = (a, n)$, visto que, se x é uma solução da congruência $a^2 x \equiv a \pmod{n}$, então o conjunto das soluções módulo n é

$$\left\{ x, x + \frac{n}{(a,d)}, x + \frac{2n}{(a,d)}, \cdots, x + \frac{((a,d)-1)n}{(a,d)} \right\}$$

e dois quaisquer destes inteiros são incongruentes módulo n.

TEOREMA 4. *Para todo* $a \in R(n)$, *o subsemigrupo gerado por* a *é um grupo.*

DEM. Com efeito, como o subsemigrupo gerado por a é finito, existem inteiros positivos u e $v \neq u$ tais que $a^u = a^v$.

Vamos provar que existe um inteiro $r>1$ tal que $a^r = a$.

Seja s o menor inteiro positivo para o qual existe algum inteiro $r > s$ tal que $a^r = a^s$. Seja $d = (a, n)$, i. e., $a = a_1 d$ e $n = n_1 d$, com $(a_1, n_1) = 1$.

Então, no anel Z dos inteiros, tem-se

$$(2) \qquad a_1^r d^s - a_1^s d^r = k n$$

para algum inteiro k.

Trata-se de provar que $s = 1$.

Na verdade, se fosse $s > 1$, de (2) resultaria

$$a_1^r d^{r-1} - a_1^s d^{s-1} = k n_1,$$

donde se concluiria que $a_1 d \mid k n_1$. Mas, como $d \mid^* n$, ter-se-ia $(a_1 d, n) = 1$ e, por consequência, $k = k_1 a_1 d$ para algum inteiro k_1.

Daqui resultaria

$$a_1^{r-1} d^{r-1} - a_1^{s-1} d^{s-1} = k_1 a_1 d n_1 = k_1 a_1 n$$

no anel Z, donde

$$a^{r-1} = a^{s-1} \text{ em } R(n),$$

contràriamente à hipótese feita sobre s. Logo $s = 1$.

Designando por r precisamente o menor inteiro maior que 1 para o qual se tem $a^r = a$, então é imediato que, para todo inteiro m, a^m é igual, em $R(n)$, a um dos elementos

$$a, a^2, a^3, \cdots, a^{r-1}$$

e que estes elementos são todos distintos. É também imediato que o conjunto destes elementos constitui um grupo (isomorfo ao grupo aditivo dos inteiros módulo $r-1$), sendo a^{r-1} o elemento neutro e sendo o inverso de a^i, $1 \leq i < r-1$, o elemento a^{r-1-i}, no caso de ser $r > 2$; para $r = 2$, o grupo contém sòmente o elemento a.

3. Uma função aritmética multiplicativa

Seja $\rho(n)$ o número de elementos do semigrupo $R(n)$.

Para cada divisor unitário d de n, seja E_d o subconjunto de $R(n)$ constituído pelos elementos a tais que $(a, n) = d$. Tem-se evidentemente

$$R(n) = \bigcup_{d \mid^* n} E_d \text{ e } E_d \cap E_{d'} = \emptyset, \text{ se } d \neq d'.$$

Ora $(a, n) = d$, se e só se a é da forma $k d$, onde $1 \leq k \leq \frac{n}{d}$ e $\left(k, \frac{n}{d}\right) = 1$.

Isto significa que o número de elementos em E_d é igual a $\varphi\left(\frac{n}{d}\right)$, onde φ designa o indicador de EULER.

Tem-se, portanto,

$$(3) \qquad \rho(n) = \sum_{d \mid^* n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid^* n} \varphi(d).$$

Vejamos agora que ρ é uma função multiplicativa, i. e., se $(m,n)=1$, então $\rho(mn) = \rho(m)\rho(n)$.

De (3) resulta que

$$\rho(m)\rho(n) = \Big(\sum_{d \mid^* m} \varphi(d)\Big)\Big(\sum_{d' \mid^* n} \varphi(d')\Big) =$$

$$= \sum_{\substack{d \mid^* m \\ d' \mid^* n}} \varphi(d)\varphi(d').$$

Mas φ é uma função multiplicativa e, como $(d, d') = 1$, tem-se

$$\rho(m)\rho(n) = \sum_{\substack{d \mid^* m \\ d' \mid^* n}} \varphi(d d').$$

Por outro lado, todo divisor unitário de mn se escreve univocamente como produto

de um divisor unitário de m por um divisor unitário de n e, por consequência, tem-se

$$\rho(mn) = \sum_{D \mid^* mn} \varphi(D) = \sum_{dd' \mid^* mn} \varphi(dd') = \sum_{\substack{d \mid^* m \\ d' \mid^* n}} \varphi(dd'),$$

como pretendíamos.

Ficou assim provado o seguinte

TEOREMA 5. *Se* $\rho(n)$ *designa o número de inteiros não negativos menores que* n *e regulares módulo* n, *então* ρ *é uma função multiplicativa e tem-se*

$$\rho(n) = \sum_{d \mid^* n} \varphi(d).$$

COROLÁRIO. *Se* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *onde os* p_i *são primos distintos, então*

$$\rho(n) = (1 + p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(1 + p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots \cdots (1 + p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Com efeito, como ρ é multiplicativa, tem-se $\rho(n) = \rho(p_1^{\alpha_1}) \cdots \rho(p_k^{\alpha_k})$ e, além disso,

$$\rho(p_i^{\alpha_i}) = \sum_{d \mid^* p_i^{\alpha_i}} \varphi(d) = \varphi(1) + \varphi(p_i^{\alpha_i}) = 1 + p_i^{\alpha_i} - p_i^{\alpha_i - 1}.$$

Recordemos que, se f e F são duas funções aritméticas tais que

$$F(n) = \sum_{d \mid^* n} f(d),$$

então tem-se (ver [4])

$$f(n) = \sum_{d \mid^* n} \mu^*(d) F\left(\frac{n}{d}\right),$$

onde a função μ^* (análogo unitário da função μ de MÖBIUS), é definida por $\mu^*(n) = (-1)^{\omega(n)}$, sendo $\omega(n)$ o número de primos distintos que dividem n.

Assim, do teorema anterior, resulta

$$\varphi(n) = \sum_{d \mid^* n} \mu^*(d) \rho\left(\frac{n}{d}\right).$$

BIBLIOGRAFIA

[1] A. H. CLIFFORD and G. B. PRESTON, *The Algebraic Theory of Semigroups*, vol. I, Mathematical Surveys, number 7, Providence, 1961.

[2] N. H. MCCOY, *The Theory of Numbers*, The Macmillan Company, New York, 1965.

[3] R. H. BRUCK, *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Berlin, 1958.

[4] E. COHEN, *Arithmetical functions associated with unitary divisors of an integer*, Math. Zeitschr., **74** (1960), pp. 66-80.