

O TEOREMA CHINÊS DOS RESTOS

FERNANDO FERREIRA

Sejam n e m números naturais diferentes de 1, co-primos entre si. Considere-se a seguinte função:

$$\begin{aligned}\gamma: \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [k]_{mn} &\rightsquigarrow ([k]_m, [k]_n)\end{aligned}$$

Esta definição está correta pois os valores não dependem dos representantes tomados. Além disso, a função é injetiva. Com efeito, se $\gamma([k]_{mn}) = \gamma([r]_{mn})$ vem, simultaneamente, $[k]_m = [r]_m$ e $[k]_n = [r]_n$, i.e., $m \mid (k - r)$ e $n \mid (k - r)$. Dado que $m \perp n$, tem-se $mn \mid (k - r)$ e, portanto, $[k]_{mn} = [r]_{mn}$. Visto que o conjunto de partida e o conjunto de chegada têm a mesma cardinalidade (ambos têm a cardinalidade mn), a função γ é uma bijeção. É mesmo um isomorfismo de anéis, como é fácil de verificar.

O facto de γ ser um isomorfismo de anéis é uma forma (algébrica) de formular o teorema chinês dos restos. É, porém, comum formular o teorema da seguinte forma:

Teorema chinês dos restos. *Sejam m e n números naturais diferentes de 1, com $m \perp n$. Dados $a, b \in \mathbb{Z}$, existe $x \in \mathbb{Z}$ tal que*

$$\begin{aligned}x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}\end{aligned}$$

Além disso, x é único módulo mn .

Demonstração. Dado que a função γ é sobrejetiva, existe $x \in \mathbb{Z}$ tal que $\gamma([x]_{mn}) = ([a]_m, [b]_n)$. Logo, $([x]_m, [x]_n) = ([a]_m, [b]_n)$. Isto quer dizer que $x \equiv a \pmod{m}$ e $x \equiv b \pmod{n}$, como se queria. A parte da unicidade é deixada ao leitor. \square

A restrição da função γ ao grupo de unidades $(\mathbb{Z}/mn\mathbb{Z})^*$ toma valores em $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ pois o valor duma unidade (por um morfismo de anéis) é uma unidade. Além disso, a função restrita

$$\begin{aligned}\gamma \uparrow: (\mathbb{Z}/mn\mathbb{Z})^* &\rightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \\ [k]_{mn} &\rightsquigarrow ([k]_m, [k]_n)\end{aligned}$$

é uma bijeção. É injetiva porque é a restrição da injeção γ ; é sobrejetiva porque γ é um isomorfismo de anéis (e, portanto, a imagem inversa duma unidade é uma unidade). Assim, $\gamma \uparrow$ é um isomorfismo de grupos e, em particular, a cardinalidade de $(\mathbb{Z}/mn\mathbb{Z})^*$ é igual à cardinalidade do produto cartesiano $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Tem-se, pois, a igualdade $\varphi(mn) = \varphi(m)\varphi(n)$, por definição da função de Euler (desde que $m \perp n$). Esta igualdade permite obter uma fórmula elegante para $\varphi(n)$:

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right)$$

Para deduzir esta fórmula, seja $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_s^{r_s}$ a fatorização de n em primos distintos (com todos os expoentes r_1, r_2, \dots, r_s não nulos). Vem

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_s^{r_s}) \\ &= \varphi(p_1^{r_1}) \cdot \varphi(p_2^{r_2}) \cdot \dots \cdot \varphi(p_s^{r_s}) \\ &= (p_1^{r_1} - p_1^{r_1-1}) \cdot (p_2^{r_2} - p_2^{r_2-1}) \cdot \dots \cdot (p_s^{r_s} - p_s^{r_s-1}) \\ &= p_1^{r_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{r_2} \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_s^{r_s} \left(1 - \frac{1}{p_s}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_s}\right) \\ &= n \prod_{\substack{p|n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right)\end{aligned}$$

rasccunho