Material Teórico - Módulo Aritmética dos Restos

O Teorema de Euler

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

16 de outubro de 2023

PORTAL DA MATEMÁTICA
OBMEP

Nas aulas anteriores, provamos e apresentamos algumas aplicações do Pequeno Teorema de Fermat. Neste material, apresentaremos uma generalização desse resultado, conhecida como o Teorema de Euler[1]. Antes, porém, apresentaremos um exemplo em cuja solução podemos perceber a ideia da demonstração do Teorema de Euler.

Exemplo 1. *Prove que* $13^6 \equiv 1 \pmod 9$.

Solução. Podemos mostrar que $13^6 \equiv 1 \pmod 9$ da seguinte maneira:

$$\begin{aligned} 13 \equiv 4 \pmod 9 &\implies 13^2 \equiv 4^2 \pmod 9 \\ &\implies 13^2 \equiv 16 \equiv -2 \pmod 9 \\ &\implies \left(13^2\right)^3 \equiv (-2)^3 \pmod 9 \\ &\implies 13^6 \equiv -8 \equiv 1 \pmod 9. \end{aligned}$$

Entretanto, para compreender a ideia da demonstração do Teorema de Euler, vamos apresentar uma solução diferente. Pra começar, vamos calcular os resíduos dos produtos $i \cdot 13$ na divisão por 9, em que $\text{mdc}\,(i,9) = 1$ e $1 \leq i \leq 9$. Temos

$$\begin{aligned} 1 \cdot 13 &= 13 \equiv 4 \pmod 9 \\ 2 \cdot 13 &= 26 \equiv 8 \pmod 9 \\ 4 \cdot 13 &= 52 \equiv 7 \pmod 9 \\ 5 \cdot 13 &= 65 \equiv 2 \pmod 9 \\ 7 \cdot 13 &= 91 \equiv 1 \pmod 9 \\ 8 \cdot 13 &= 104 \equiv 5 \pmod 9 \end{aligned}$$

Multiplicando membro a membro as seis congruências acima, obtemos

$$1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \cdot 13^6 \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \pmod 9.$$

Agora, uma vez que $\text{mdc}\,(1,9) = \text{mdc}\,(2,9) = \text{mdc}\,(4,9) = \text{mdc}\,(5,9) = \text{mdc}\,(7,9) = \text{mdc}\,(8,9) = 1$, concluímos que $\text{mdc}\,(1{\cdot}2{\cdot}4{\cdot}5{\cdot}7{\cdot}8,9) = 1$. Logo, podemos cancelar $1,{\cdot}2{\cdot}4{\cdot}5{\cdot}7{\cdot}8$ na última congruência acima, obtendo $13^6 \equiv 1 \pmod 9$. □

[1]Leonhard Euler (lê-se *Óiler*), que viveu ao longo do século XVIII, foi um dos mais importantes matemáticos da história.

Na segunda solução apresentada acima, o expoente de 13 em $13^6 \equiv 1 \pmod 9$ é igual à *quantidade de números* $i \in \{1,2,\ldots,9\}$ *tais que* $\text{mdc}\,(i,9) = 1$.

Mais geralmente, a **função ϕ de Euler** é definida, para cada inteiro positivo n, como a quantidade de inteiros positivos menores do que ou iguais a n e relativamante primos com n. Utilizamos a notação $\phi(n)$ para denotar essa quantidade.

Assim, $\phi(9) = 6$ (pois os inteiros positivos menores ou iguais a 9 e primos com 9 são 1, 2, 4, 5, 7, 8, num total de 6 inteiros) e $13^{\phi(9)} \equiv 1 \pmod 9$.

Perceba, ainda, que, se n é primo, então $\phi(n) = n - 1$. Realmente, sendo n primo, temos que $n > 1$ e todos os inteiros de 1 a $n - 1$ são primos com n.

Se os inteiros r_1, r_2, ..., $r_{\phi(n)}$ forem todos relativamente primos com n e satisfizerem $r_i \not\equiv r_j \pmod n$ sempre que $i \neq j$, diremos que o conjunto $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ é um **sistema reduzido de resíduos** módulo n.

Um exemplo de sistema reduzido de resíduos, módulo n, é o conjunto $\{j \in \mathbb{Z};\ 1 \leq j \leq n \text{ e } \text{mdc}\,(j,n) = 1\}$. Por outro lado, para obter um sistema reduzido de resíduos módulo n a partir de um sistema completo de resíduos, basta retirar, do sistema completo, os elementos que não são relativamente primos com n.

Os próximos três resultados mostram como calcular $\phi(n)$, em que n é um inteiro positivo qualquer.

Proposição 2. *Se $n = p^k$, em que p é primo, então*

$$\phi(n) = p^{k-1}(p-1).$$

Prova. Para calcular $\phi(p^k)$, temos de calcular a quantidade de inteiros pertencentes ao conjunto $\{1,2,\ldots,p^k\}$ e que são relativamente primos com $n = p^k$.

Os únicos inteiros desse conjunto que *não são* relativamente primos com p^k são os múltiplos de p, isto é, os números p, $2p$, $3p$, ..., $p^k = p^{k-1} \cdot p$.

Portanto, a quantidade de múltiplos de p pertencentes a $\{1,2,\ldots,p^k\}$ é igual a p^{k-1}, de modo que $\phi(n) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

O próximo resultado, também devido a Euler, traz uma importante propriedade da função ϕ.

Teorema 3 (Euler). *Sejam m e n inteiros positivos tais que* $\text{mdc}\,(m,n) = 1$. *Então, $\phi(mn) = \phi(m)\phi(n)$.*

Prova. Vamos organizar os mn números inteiros de 1 a mn em uma tabela de m linhas e n colunas, do seguinte modo.

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\
\vdots & \vdots & \vdots & & \vdots \\
r & m+r & 2m+r & \dots & (n-1)m+r \\
\vdots & \vdots & \vdots & & \vdots \\
m & 2m & 3m & \dots & nm
\end{array}$$

Se $r \in \{1,2,\dots,m\}$ for tal que $\text{mdc}\,(r,m) = d > 1$, então todos os números da linha r têm mdc d com m; realmente, um número típico da linha r é da forma $km+r$, e $\text{mdc}\,(km+r,m) = d > 1$. Portanto, nenhum dos números dessa linha é relativamente primo com m.

Assim, para contar a quantidade inteiros positivos menores do que mn e que são relativamente primos com mn, basta contarmos a quantidade de inteiros relativamente primos com n em cada linha r com $\text{mdc}\,(r,m) = 1$.

Veja que a quantidade de linhas r tais que $\text{mdc}\,(r,m) = 1$ é $\phi(m)$. Mas todos os termos pertencentes a cada uma dessas linhas são relativamente primos com m, pois $\text{mdc}\,(km + r,m) = \text{mdc}\,(r,m) = 1$.

Assim, se mostrarmos que, em cada uma dessas linhas, há $\phi(n)$ números relativamente primos com n, então teremos mostrado que $\phi(mn) = \phi(m)\phi(n)$.

Para o que falta, note que os elementos de cada linha formam um sistema completo de resíduos módulo n. De fato, para $0 \le j,k \le n-1$, temos que $km + r \equiv jm + r\,(\text{mod}\,n)$ implica $km \equiv jm\,(\text{mod}\,n)$ e, como $\text{mdc}\,(m,n) = 1$, podemos cancelar m na última congruência para obter $k \equiv j\,(\text{mod}\,n)$,

logo, $k = j$. Assim, extraindo de cada um desses sistemas completos de resíduos um sistema reduzido, concluímos que cada uma dessas linhas contém exatamente $\phi(n)$ números relativamente primos com n. □

Teorema 4 (Euler). *Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, em que $p_1 < p_2 < \dots < p_r$ são primos e α_1, α_2, ..., α_r são inteiros positivos. Então*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right).$$

Prova. Como mdc $\left(p_i^{\alpha_i}, p_j^{\alpha_j}\right) = 1$ se $i \neq j$, podemos aplicar algumas vezes o teorema anterior para obter

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}\right) \\
&= \phi\left(p_1^{\alpha_1}\right)\phi\left(p_2^{\alpha_2}\right)\dots\phi\left(p_r^{\alpha_r}\right) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1)\dots p_r^{\alpha_r - 1}(p_r - 1) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\dots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

Exemplo 5. *Calcule $\phi(400)$.*

Solução. Fatorando 400, obtemos $400 = 2^4 \cdot 5^2$, logo,

$$\begin{aligned}
\phi(400) &= 400\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \\
&= 400 \cdot \frac{1}{2} \cdot \frac{4}{5} \\
&= 160.
\end{aligned}$$

□

Exemplo 6. *Prove que, se n é um inteiro positivo composto, então*

$$\phi(n) \leq n - \sqrt{n}.$$

Solução. Escrevemos $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Como n é composto, pelo menos um dos primos que aparecem em sua decomposição, digamos p_i, é menor ou igual a $\sqrt{n}$. Portanto, utilizando o teorema 4, obtemos

$$\begin{aligned}
\phi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right) \\
&\leq n \cdot 1^{r-1}\left(1 - \frac{1}{p_i}\right) \\
&\leq n\left(1 - \frac{1}{\sqrt{n}}\right) \\
&= n - \sqrt{n}.
\end{aligned}$$

□

Chegamos finalmente à generalização, devida a Euler, do Pequeno Teorema de Fermat.

Teorema 7 (Euler). *Sejam n um número inteiro positivo e a um inteiro tal que* $\operatorname{mdc}(a,n) = 1$. *Então,*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Prova. Seja $\{r_1, r_2, \dots, r_{\phi(n)}\}$ o sistema reduzido de resíduos módulo n formado pelos inteiros pertencentes a $\{0, 1, \dots, n-1\}$ e que são relativamente primos com n.

Afirmamos que o conjunto $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ também é um sistema reduzido de resíduos módulo n. Realmente, por um lado,

$$\operatorname{mdc}(a,n) = 1 \text{ e } \operatorname{mdc}(r_i,n) = 1 \Longrightarrow \operatorname{mdc}(ar_i,n) = 1.$$

Por outro, para todos $i,j \in \{1, 2, \dots, \phi(n)\}$, utilizando novamente o fato de que a e n são relativamente primos, temos que

$$ar_i \equiv ar_j \pmod{n} \Longrightarrow r_i \equiv r_j \pmod{n} \Longrightarrow i = j,$$

já que $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ é um sistema reduzido de resíduos módulo n.

Assim, temos que cada elemento ar_j é congruente a algum r_{i_j}, de forma tal que $\{i_1,i_2,\ldots,i_{\phi(n)}\}$ forma uma permutação de $\{1,2,\ldots,\phi(n)\}$. Desse modo, multiplicando membro a membro das congruências

$$\begin{aligned} ar_1 &\equiv r_{i_1} \pmod n,\\ ar_2 &\equiv r_{i_2} \pmod n,\\ &\vdots\\ ar_{\phi(n)} &\equiv r_{i_{\phi(n)}} \pmod n, \end{aligned}$$

obtemos

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \pmod n.$$

Daí, segue que

$$a^{\phi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \pmod n.$$

Por fim, como $\text{mdc}\,(r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)},n) = 1$, podemos cancelar esse número nos dois lados da última congruência acima para obter $a^{\phi(n)} \equiv 1 \pmod n$. □

Exemplo 8. *Encontre o resto na divisão de* 13^{9999} *por* 1000.

Solução. Como $\text{mdc}\,(13,1000) = 1$, pelo Teorema de Euler, temos que $13^{\phi(1000)} \equiv 1 \pmod{1000}$. Mas observe que $1000 = 2^3 \cdot 5^3$, logo, utilizando o teorema 4, obtemos

$$\begin{aligned} \phi(1000) &= 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\\ &= 1000 \cdot \frac{1}{2} \cdot \frac{4}{5}\\ &= 400. \end{aligned}$$

Assim, $13^{400} \equiv 1 \pmod{1000}$, o que implica $\left(13^{400}\right)^{25} \equiv 1^{25} \pmod{1000}$ ou, ainda,

$$13^{10000} \equiv 1 \pmod{1000}.$$

Por outro lado, perceba que $1001 = 7 \cdot 11 \cdot 13 = 13 \cdot 77$ e que $1001 \equiv 1 \pmod{1000}$. Desse modo, obtemos

$$\begin{aligned} 13^{9999} &\equiv 13^{9999} \cdot 1 \pmod{1000} \\ &\equiv 13^{9999} \cdot 1001 \pmod{1000} \\ &\equiv 13^{9999} \cdot 13 \cdot 77 \pmod{1000} \\ &\equiv 13^{1000} \cdot 77 \pmod{1000} \\ &\equiv 1 \cdot 77 \pmod{1000} \\ &\equiv 77 \pmod{1000}. \end{aligned}$$

□

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores apresentem outros exemplos como o exemplo 1 antes de apresentar a demonstração do Teorema de Euler, pois isso facilitará a compreensão da ideia da demonstração do teorema. Além disso, assim como observamos para o Pequeno Teorema de Fermat, fica claro no examplo 1 que certos problemas podem ser facilmente resolvidos apenas aplicando as propriedades de congruências, sem utilizar o Teorema de Euler. Entretanto, o teorema facilita a resolução de outros problemas e possui uma abrangência bem maior do que a do Pequeno Teorema de Fermat, como era de se esperar.

Sugestões de Leitura Complementar

1. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*. Rio de Janeiro, SBM, 2022.

2. J. P. O. Santos. *Introdução à Teoria dos Números*. Rio de Janeiro, IMPA, 2000.