Material Teórico - Módulo Aritmética dos Restos

O Teorema de Euler - Parte 2

Tópicos Adicionais

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

20 de novembro de 2023

Neste material, apresentaremos algumas aplicações do Teorema de Euler.

Exemplo 1. *Encontre os dois últimos algarismos da representação decimal de* $7^{7^{1000}}$.

Solução. Iniciamos observando que os dois últimos algarismos de um natural correspondem ao resto de sua divisão por 100. Então, com vistas ao uso do Teorema de Euler módulo 100, calculemos o valor de $\phi(100)$: como $100 = 2^2 \cdot 5^2$, temos

$$\begin{aligned}\phi(100) &= 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\\ &= 100\cdot\frac{1}{2}\cdot\frac{4}{5}\\ &= 40.\end{aligned}$$

Como $\text{mdc}\,(7{,}100) = 1$, utilizamos o Teorema de Euler para obter

$$7^{\phi(100)} \equiv 1 \pmod{100} \Longrightarrow 7^{40} \equiv 1 \pmod{100}.$$

Agora, vamos encontrar o resto da divisão de 7^{1000} — que é o expoente da potência $7^{7^{1000}}$ — por 40. Uma vez que $40 = 2^3 \cdot 5$, temos

$$\begin{aligned}\phi(40) &= 40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\\ &= 40\cdot\frac{1}{2}\cdot\frac{4}{5}\\ &= 16.\end{aligned}$$

Daí, mais uma vez utilizamos o Teorema de Euler, agora para obter

$$7^{\phi(40)} \equiv 1 \pmod{40} \Longrightarrow 7^{16} \equiv 1 \pmod{40}.$$

Mas perceba que $1000 = 16 \cdot 62 + 8$. Além disso, $7^2 = 49 \equiv 9 \pmod{40}$, o que acarreta

$$7^4 \equiv \left(7^2\right)^2 \equiv 9^2 = 81 \equiv 1 \pmod{40}.$$

Elevando ao quadrado os dois membros da última congruência, obtemos

$$7^8 \equiv \left(7^4\right)^2 \equiv 1^2 = 1 \,(\mathrm{mod}\, 40).$$

Juntando as informações acima, obtemos

$$\begin{aligned} 7^{1000} &= 7^{16\cdot 62+8} \,(\mathrm{mod}\, 40) \\ &\equiv \left(7^{16}\right)^{62} \cdot 7^8 \,(\mathrm{mod}\, 40) \\ &\equiv 1^{62} \cdot 1 \,(\mathrm{mod}\, 40) \\ &\equiv 1 \,(\mathrm{mod}\, 40). \end{aligned}$$

Desse modo, podemos escrever $7^{1000} = 40k + 1$, para algum k inteiro positivo. Então, lembrando da informação de que $7^{40} \equiv 1 \,(\mathrm{mod}\, 100)$, obtida no início da solução, chegamos a

$$\begin{aligned} 7^{7^{1000}} &= 7^{40k+1} \\ &= \left(7^{40}\right)^k \cdot 7 \\ &\equiv 1^k \cdot 7 \,(\mathrm{mod}\, 100) \\ &\equiv 7 \,(\mathrm{mod}\, 100). \end{aligned}$$

Portanto, os dois últimos algarismos de $7^{7^{1000}}$ são 07. □

Exemplo 2 (AIME). *Encontre o resto da divisão de* $6^{83} + 8^{83}$ *por* 49*.*

Solução. Como $\mathrm{mdc}\,(6,49) = \mathrm{mdc}\,(8,49) = 1$, podemos aplicar o teorema de Euler para obter $6^{\phi(49)} \equiv 1 \,(\mathrm{mod}\, 49)$ e $8^{\phi(49)} \equiv 1 \,(\mathrm{mod}\, 49)$.

Agora, observe que $\phi(49) = \phi\left(7^2\right) = 7(7-1) = 42$, logo, $6^{42} \equiv 1 \,(\mathrm{mod}\, 49)$ e $8^{42} \equiv 1 \,(\mathrm{mod}\, 49)$. Então,

$$\begin{aligned} 6^{42} \equiv 1 \,(\mathrm{mod}\, 49) &\Longrightarrow \left(6^{42}\right)^2 \equiv 1^2 \,(\mathrm{mod}\, 49) \\ &\Longrightarrow 6^{84} \equiv 1 \,(\mathrm{mod}\, 49) \end{aligned}$$

e

$$\begin{aligned} 8^{42} \equiv 1 \,(\mathrm{mod}\, 49) &\Longrightarrow \left(8^{42}\right)^2 \equiv 1^2 \,(\mathrm{mod}\, 49) \\ &\Longrightarrow 8^{84} \equiv 1 \,(\mathrm{mod}\, 49). \end{aligned}$$

Por fim, veja que $6 \cdot (-8) = 8 \cdot (-6) = -48 \equiv 1 \pmod{49}$. Desse modo,

$$\begin{aligned} 6^{83} + 8^{83} &\equiv 6^{83} \cdot 6 \cdot (-8) + 8^{83} \cdot 8 \cdot (-6) \pmod{49} \\ &\equiv -8 \cdot 6^{84} - 6 \cdot 8^{84} \pmod{49} \\ &\equiv -8 \cdot 1 - 6 \cdot 1 \pmod{49} \\ &\equiv -14 \pmod{49} \\ &\equiv 35 \pmod{49}. \end{aligned}$$

Portanto, o resto da divisão de $6^{83} + 8^{83}$ por 49 é 35. □

Exemplo 3. *Mostre que existem infinitos múltiplos de* 2009 *da forma*

$$200\ldots09.$$

Solução. Escrevendo $2\underbrace{00\ldots09}_{k}$ como

$$2\underbrace{00\ldots00}_{k}+9 = 2 \cdot 10^k + 9,$$

vemos que basta encontrar infinitos $k \in \mathbb{N}$ tais que 2009 divide $2 \cdot 10^k + 9$. Mas

$$\begin{aligned} 2009 \mid (2 \cdot 10^k + 9) &\iff 2 \cdot 10^k + 9 \equiv 0 \pmod{2009} \\ &\iff 2 \cdot 10^k + 9 \equiv 2009 \pmod{2009} \\ &\iff 2 \cdot 10^k \equiv 2 \cdot 10^3 \pmod{2009} \\ &\iff 2 \cdot 10^3 \cdot 10^{k-3} \equiv 2 \cdot 10^3 \pmod{2009} \\ &\iff 10^{k-3} \equiv 1 \pmod{2009}. \end{aligned}$$

(Observe que foi possível "cancelar" $2 \cdot 10^3$ na penúltima congruência porque $\text{mdc}\left(2 \cdot 10^3, 2009\right) = 1$.)

Agora, uma vez que $\text{mdc}\,(10, 2009) = 1$, o Teorena de Euler garante que

$$10^{\phi(2009)} \equiv 1 \pmod{2009},$$

o que implica

$$10^{n\phi(2009)} \equiv 1 \pmod{2009}, \forall n \in \mathbb{N}.$$

Portanto, se tomarmos $k_n = n\phi(2009) + 3$, teremos que $10^{k_n-3} \equiv 1 \pmod{2009}$, e $2 \cdot 10^{k_n} + 9$ será um múltiplo de 2009. □

Exemplo 4 (Argentina). *Prove que, para cada número natural n, existe uma potência de 2 tal que, dentre os n últimos algarismos (à direita) da representação dessa potência na base decimal, a quantidade de algarismos iguais a zero é maior do que $2n/3$.*

Solução. Note que, se um número inteiro m maior do que 10^n deixa um resto que possui menos de $n/3$ algarismos quando dividido por 10^n, então, dentre os n últimos algarismos de m, a quantidade de algarismos iguais a zero é maior do que $n - n/3 = 2n/3$. Essa é a ideia central para resolver este problema.

Agora, como mdc $(2,5^n) = 1$ para todo n inteiro positivo, segue do Teorema de Euler que

$$\begin{aligned} 2^{\phi(5^n)} \equiv 1 \pmod{5^n} &\Longrightarrow 2^{\phi(5^n)} \cdot 2^n \equiv 1 \cdot 2^n \pmod{5^n} \\ &\Longrightarrow 2^{\phi(5^n)+n} \equiv 2^n \pmod{5^n}. \end{aligned}$$

Uma vez que 2^n claramente divide $2^{\phi(n)+n} - 2^n$, concluímos que também vale $2^{\phi(5^n)+n} \equiv 2^n \pmod{2^n}$. Mas, como mdc $(2^n,5^n) = 1$, concluímos que $2^{\phi(5^n)+n} \equiv 2^n \pmod{2^n \cdot 5^n}$, ou seja, $2^{\phi(5^n)+n} \equiv 2^n \pmod{10^n}$.

Finalmente, observe que

$$2^n = \left(2^3\right)^{n/3} = 8^{n/3} < 10^{n/3},$$

logo, a quantidade de algarismos de 2^n é menor do que $n/3$. Portanto, dentre os últimos n algarismos de $2^{\phi(5^n)+n}$, a quantidade de algarismos iguais a zero é maior do que $2n/3$. □

Exemplo 5 (IMO[1]). *Prove que existem a sequência $a_n = 2^n - 3$ $(n > 1)$ contém infinitos termos dois a dois primos entre si.*

[1] Olimpíada Internacional de Matemática.

Solução. Veja que $a_2 = 1$, $a_3 = 5$ e $a_4 = 13$. Suponha que os termos a_{n_1}, a_{n_2}, a_{n_3}, ..., a_{n_k} sejam dois a primos entre si, isto é, $\text{mdc}\,(a_{n_i},a_{n_j}) = 1$, sempre que $1 \leq i,j \leq k$, com $i \neq j$. Defina

$$m = a_{n_1}a_{n_2}\ldots a_{n_k} \quad \text{e} \quad n_{k+1} = \phi\,(m)\,.$$

Veja que cada a_{n_i} é ímpar, logo, $\text{mdc}\,(2,a_{n_1}a_{n_2}\ldots a_{n_k}) = \text{mdc}\,(2,m) = 1$. Portanto, aplicando o Teorema de Euler, obtemos

$$\begin{aligned} 2^{\phi(m)} \equiv 1\,(\text{mod}\,m) &\Longrightarrow 2^{n_{k+1}} - 3 \equiv -2\,(\text{mod}\,m) \\ &\Longrightarrow a_{n_{k+1}} \equiv -2\,(\text{mod}\,m). \end{aligned}$$

Desse modo, existe q inteiro tal que

$$a_{n_{k+1}} = mq - 2.$$

Agora, vamos mostrar que $\text{mdc}\,\left(a_{n_{k+1}},a_{n_i}\right) = 1$, para todo $i \in \{1,2,\ldots,k\}$. De fato, seja $d = \text{mdc}\,\left(a_{n_{k+1}},a_{n_i}\right)$. Como a_{n_i} divide m, temos que d divide $a_{n_{k+1}}$ e mq, logo, d divide 2, pois $2 = mq - a_{n_{k+1}}$. Mas, uma vez que a_n é ímpar para todo n, concluímos que d não pode ser igual a 2. Logo, $d = 1$. □

Exemplo 6 (Olimpíada Balcânica). *Prove que, para cada número natural n dado, existe um número natural $m > n$ tal que a representação decimal de 5^m é obtida acrescentando certa quantidade de algarismos à esquerda da representação decimal de 5^n.*

Solução. Sendo k a quantidade de algarismos de 5^n, temos

$$10^{k-1} < 5^n < 10^k.$$

Desejamos encontrar $m > n$ tal que a representação decimal de 5^m é obtida acrescentando certa quantidade de algarismos à esquerda da representação decimal de 5^n, ou seja, tal que os últimos k algarismos das representações decimais de 5^m e 5^n sejam iguais. Isto é equivalente a $5^m - 5^n$ terminar em k zeros, isto é, a que 10^k divida $5^m - 5^n$.

Agora, veja que

$$\begin{aligned} 10^k \mid (5^m - 5^n) &\iff 5^m - 5^n = 10^k q,\ \exists\, q \in \mathbb{Z} \\ &\iff 5^n \left(5^{m-n} - 1\right) = 10^k q. \end{aligned}$$

Como $10^{k-1} < 5^n$ implica $n \geq k$, podemos dividir ambos os membros da última igualdade acima por 5^k para obter

$$5^{n-k} \left(5^{m-n} - 1\right) = 2^k q.$$

Por outro lado, como $\text{mdc}\,(5^{n-k}, 2^k) = 1$, temos que

$$5^{n-k} \left(5^{m-n} - 1\right) = 2^k q \Longrightarrow 2^k \mid \left(5^{m-n} - 1\right).$$

Reciprocamente,

$$\begin{aligned} 2^k \mid \left(5^{m-n} - 1\right) &\Longrightarrow 5^{m-n} - 1 = 2^k l,\ \exists\, l \in \mathbb{Z} \\ &\Longrightarrow 5^{n-k}(5^{m-n} - 1) = 2^k \cdot \underbrace{5^{n-k} l}_{q}. \end{aligned}$$

Desse modo,

$$\begin{aligned} 10^k \mid (5^m - 5^n) &\iff 2^k \mid (5^{m-n} - 1) \\ &\iff 5^{m-n} \equiv 1 \pmod{2^k}. \end{aligned}$$

Por fim, o Teorema de Euler garante que

$$5^{\phi\left(2^k\right)} \equiv 1 \pmod{2^k},$$

logo, basta tomar $m = n + \phi\left(2^k\right)$. □

Dicas para o Professor

Sugerimos que sejam utilizadas quatro sessões de 50min para expor o conteúdo deste material. Recomendamos fortemente que os alunos tentem encontrar soluções para os problemas apresentados neste material utilizando meios próprios.

Se, depois de certo tempo, os alunos não conseguirem apresentar uma solução para determinado problema, dê dicas antes de apresentar a solução completa. É possível que os alunos apresentem soluções que não fazem uso do Teorema de Euler, principalmente para os problemas 1 e 2.

Alguns dos exemplos aqui discutidos aparecem na referência [1]. Remetemos o leitor a ela para outros exemplos interessantes.

Sugestões de Leitura Complementar

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