Material Teórico - Módulo Aritmética dos Restos

Problemas com Congruências - Parte 1

Tópicos Adicionais

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

21 de junho de 2023

Neste material, apresentamos alguns problemas cujas soluções envolvem aritmética modular. Iniciamos com o seguinte exemplo.

Exemplo 1. *Encontre o resto na divisão de* 11^{2023} *por* 9.

Solução. Temos que

$$\begin{aligned} 11 \equiv 2 \,(\mathrm{mod}\, 9) &\Longrightarrow 11^3 \equiv 2^3 \,(\mathrm{mod}\, 9) \\ &\Longrightarrow 11^3 \equiv 8 \equiv -1 \,(\mathrm{mod}\, 9). \end{aligned}$$

Mas

$$\begin{array}{r|l} 2\,0\,2\,3 & 3 \\ \cline{2-2} 2\,2 & 6\,7\,4 \\ 1\,3 & \\ 1 & \end{array}$$

Logo,

$$\begin{aligned} \left(11^3\right)^{674} \equiv (-1)^{674} \,(\mathrm{mod}\, 9) &\Longrightarrow 11^{2022} \equiv 1 \,(\mathrm{mod}\, 9) \\ &\Longrightarrow 11^{2022} \cdot 11 \equiv 1 \cdot 11 \,(\mathrm{mod}\, 9) \\ &\Longrightarrow 11^{2023} \equiv 11 \equiv 2 \,(\mathrm{mod}\, 9). \end{aligned}$$

Portanto, na divisão de 11^{2023} por 9, o resto é igual a 2. □

Exemplo 2. *Prove que, se* n *é um número natural, então* $11^{n+2} + 12^{2n+1}$ *é divisível por* 133.

Solução. Observe que

$$\begin{aligned} 11^{n+2} + 12^{2n+1} &= 11^n \cdot 11^2 + 12^{2n} \cdot 12^1 \\ &= 121 \cdot 11^n + 12 \cdot \left(12^2\right)^n \\ &= 121 \cdot 11^n + 12 \cdot 144^n. \end{aligned}$$

Agora, perceba que

$$11 \equiv 144 \,(\mathrm{mod}\, 133) \Longrightarrow 11^n \equiv 144^n \,(\mathrm{mod}\, 133)$$

e

$$121 \equiv -12 \,(\mathrm{mod}\, 133).$$

Portanto, multiplicando membro a membro as duas últimas conguências, obtemos

$$121 \cdot 11^n \equiv -12 \cdot 144^n \,(\mathrm{mod}\, 133),$$

de sorte que 133 divide $121 \cdot 11^n + 12 \cdot 144^n$. □

Exemplo 3. *Encontre o menor número natural n tal que $63^{2022} \cdot 65^{2023} + n$ seja divisível por 8.*

Solução. Temos que

$$63 \equiv -1 \,(\mathrm{mod}\, 8) \Longrightarrow 63^{2022} \equiv (-1)^{2022} \equiv 1 \,(\mathrm{mod}\, 8)$$

e

$$65 \equiv 1 \,(\mathrm{mod}\, 8) \Longrightarrow 65^{2023} \equiv 1^{2023} \equiv 1 \,(\mathrm{mod}\, 8).$$

Logo,

$$63^{2022} \cdot 65^{2023} \equiv 1 \cdot 1 \equiv 1 \,(\mathrm{mod}\, 8).$$

Portanto, o menor número natural n tal que $63^{2022} \cdot 65^{2023} + n$ é divisível por 8 é $n = 7$. □

Exemplo 4. *Mostre que $2^{70} + 3^{70}$ é divisível por 13.*

Solução 1. Temos que

$$\begin{aligned} 2^4 = 16 \equiv 3 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(2^4\right)^3 \equiv 3^3 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 2^{12} \equiv 27 \equiv 1 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow \left(2^{12}\right)^5 \equiv 1^5 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 2^{60} \equiv 1 \,(\mathrm{mod}\, 13) \end{aligned}$$

e

$$\begin{aligned} 2^4 = 16 \equiv 3 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(2^4\right)^2 \equiv 3^2 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 2^8 \equiv 9 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 2^8 \cdot 2^2 \equiv 9 \cdot 2^2 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 2^{10} \equiv 36 \equiv 10 \,(\mathrm{mod}\, 13). \end{aligned}$$

Juntando as informações obtidas acima, concluímos que

$$2^{70} = 2^{60} \cdot 2^{10} \equiv 1 \cdot 10 \equiv 10 \,(\mathrm{mod}\, 13).$$

Também temos que

$$\begin{aligned} 3^3 = 27 \equiv 1 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(3^3\right)^{23} \equiv 1^{23} \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{69} \equiv 1 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{69} \cdot 3 \equiv 1 \cdot 3 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{70} \equiv 3 \,(\mathrm{mod}\, 13). \end{aligned}$$

Portanto, obtemos

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 13 \equiv 0 \,(\mathrm{mod}\, 13),$$

ou seja, $2^{70} + 3^{70}$ é divisível por 13. □

Solução 2. Observando que $4 \equiv -9 \,(\mathrm{mod}\, 13)$, temos que

$$\begin{aligned} 2^{70} + 3^{70} &= (2^2)^{35} + (3^2)^{35} \\ &= 4^{35} + 9^{35} \\ &\equiv (-9)^{35} + 9^{35} \,(\mathrm{mod}\, 13). \\ &\equiv -9^{35} + 9^{35} \equiv 0 \,(\mathrm{mod}\, 13). \end{aligned}$$

□

Exemplo 5. *É possível escrever* 10000 *como soma de dois cubos perfeitos?*

Solução. Inicialmente, veja que

$$\begin{aligned} 10 \equiv 3 \,(\mathrm{mod}\, 7) &\Longrightarrow 10^2 \equiv 3^2 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^2 \equiv 9 \equiv 2 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^2 \cdot 10 \equiv 2 \cdot 10 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^3 \equiv 20 \equiv -1 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^3 \cdot 10 \equiv (-1) \cdot 10 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^4 \equiv -10 \equiv 4 \,(\mathrm{mod}\, 7) \end{aligned}$$

Por outro lado, se n é um número natural qualquer, afirmamos que $n^3 \equiv 0 \,(\mathrm{mod}\, 7)$ ou $n^3 \equiv 1 \,(\mathrm{mod}\, 7)$ ou $n^3 \equiv -1 \,(\mathrm{mod}\, 7)$.

De fato, temos que

$$n \equiv 0 \pmod 7 \Longrightarrow n^3 \equiv 0^3 \equiv 0 \pmod 7$$
$$n \equiv 1 \pmod 7 \Longrightarrow n^3 \equiv 1^3 \equiv 1 \pmod 7$$
$$n \equiv 2 \pmod 7 \Longrightarrow n^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7$$
$$n \equiv 3 \pmod 7 \Longrightarrow n^3 \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$$
$$n \equiv 4 \pmod 7 \Longrightarrow n^3 \equiv 4^3 \equiv 64 \equiv 1 \pmod 7$$
$$n \equiv 5 \pmod 7 \Longrightarrow n^3 \equiv 5^3 \equiv (-2)^3 \equiv -8 \equiv -1 \pmod 7$$
$$n \equiv 6 \pmod 7 \Longrightarrow n^3 \equiv 6^3 \equiv (-1)^3 \equiv -1 \pmod 7$$

Agora, suponha que $10000 = a^3 + b^3$, em que a e b são números naturais. Combinando os possíveis valores para a^3 e b^3 módulo 7, obtemos que, módulo 7,

$$a^3 + b^3 \equiv 0 + 0,0 + 1,0 + (-1),1 + 1,1 + (-1) \text{ ou } (-1) + (-1),$$

isto é,

$$a^3 + b^3 \equiv 0,1,-1,2 \text{ ou } -2 \pmod 7.$$

Conforme vimos acima, $10000 = 10^4 \equiv 4 \equiv -3 \pmod 7$, de sorte que deveríamos ter

$$-3 \equiv 0,1,-1,2 \text{ ou } -2 \pmod 7.$$

Uma vez que isso é impossível, concluímos que 10000 não pode ser escrito como uma soma de cubos perfeitos. □

Observação 6. *Não podemos ultilizar o mesmo raciocínio empregado na solução do exemplo 5 para concluir que* 100 *não pode ser escrito como soma de dois cubos. De fato, como*

$$100 = 10^2 \equiv 3^2 \equiv 2 \pmod 7$$

ao supormos que $100 = a^3 + b^3$*, não chegamos a uma contradição (como naquele exemplo), tendo em vista que* $a^3 + b^3$ *pode ser congruente a* 2*, módulo* 7*.*

Contudo, isso também não significa que 100 *possa ser escrito como soma de dois cubos perfeitos. De fato, é fácil*

verificar (faça isso!) que 100 *não pode ser escrito desse modo (os cubos perfeitos menores que* 100 *são* 0, 1, 8, 27 *e* 64*, e não há dois deles que somem* 100*).*

Entretanto, utilizando o mesmo raciocínio empregado no exemplo 5, é possível mostrar que qualquer potência de 10 *da forma* 10^{3n+1} *não pode ser escrita como soma de dois cubos perfeitos. Com efeito, temos*

$$\begin{aligned} 10^3 \equiv -1 \,(\mathrm{mod}\, 7) &\Longrightarrow \left(10^3\right)^n \equiv (-1)^n \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^{3n} \equiv (-1)^n \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^{3n} \cdot 10 \equiv (-1)^n \cdot 10 \,(\mathrm{mod}\, 7) \\ &\Longrightarrow 10^{3n+1} \equiv (-1)^n \cdot 3 \,(\mathrm{mod}\, 7). \end{aligned}$$

Se n *for par, obtemos*

$$10^{3n+1} \equiv (-1)^n \cdot 3 \equiv 3 \,(\mathrm{mod}\, 7)$$

e, se n *for ímpar,*

$$10^{3n+1} \equiv (-1)^n \cdot 3 \equiv -3 \,(\mathrm{mod}\, 7).$$

Como 3 *ou* -3 *não são possíveis congruências de* $a^3 + b^3$ *por* 7*, concluímos que não é possível escrever* 10^{3n+1} *como soma de dois cubos perfeitos.*

Exemplo 7. *Se* n *é um número natural ímpar, então a soma* $1^n + 2^n + \ldots + (n-2)^n + (n-1)^n$ *é um múltiplo de* n*.*

Solução. Sendo n ímpar, os inteiros de 1 a $n-1$ podem ser agrupados nos pares 1 e $n-1$, 2 e $n-2$, $\ldots$, $\frac{n-1}{2}$ e $n - \left(\frac{n-1}{2}\right) = \frac{n+1}{2}$. Por outro lado, também porque n é ímpar, temos $(-t)^n = -t^n$, para todo $t \in \mathbb{Z}$. Logo,

$$\begin{aligned} n-1 \equiv -1 \,(\mathrm{mod}\, n) &\Longrightarrow (n-1)^n \equiv (-1)^n \equiv -1^n \\ &\Longrightarrow (n-1)^n + 1^n \equiv 0 \,(\mathrm{mod}\, n), \end{aligned}$$

$$\begin{aligned} n-2 \equiv -2 \,(\mathrm{mod}\, n) &\Longrightarrow (n-2)^n \equiv (-2)^n \equiv -2^n \\ &\Longrightarrow (n-2)^n + 2^n \equiv 0 \,(\mathrm{mod}\, n) \end{aligned}$$

e, em geral,

$$n - j \equiv -j \,(\mathrm{mod}\, n) \Longrightarrow (n-j)^n \equiv (-j)^n \equiv -j^n$$
$$\Longrightarrow (n-j)^n + j^n \equiv 0 \,(\mathrm{mod}\, n).$$

Fazendo j variar de 1 a $\frac{n-1}{2}$, obtemos as congruências

$$\begin{array}{l} (n-1)^n + 1^n \equiv 0 \,(\mathrm{mod}\, n) \\ (n-2)^n + 2^n \equiv 0 \,(\mathrm{mod}\, n) \\ \ldots\ldots \\ \left(n - \frac{n-1}{2}\right)^n + \left(\frac{n-1}{2}\right)^n \equiv 0 \,(\mathrm{mod}\, n) \end{array} .$$

Somando-as membro a membro, chegamos a

$$1^n + 2^n + \ldots + \left(\frac{n-1}{2}\right)^n + \left(\frac{n+1}{2}\right)^n + \ldots +$$
$$+(n-2)^n + (n-1)^n \equiv 0 \,(\mathrm{mod}\, n).$$

□

Exemplo 8. *A soma de dois quadrados perfeitos ímpares pode ser um quadrado perfeito?*

Solução. Se n é um quadrado perfeito ímpar, então $n = m^2$, em que m também é ímpar, logo, $m \equiv 1$ ou $3 \,(\mathrm{mod}\, 4)$. Mas

$$m \equiv 1 \,(\mathrm{mod}\, 4) \Longrightarrow n = m^2 \equiv 1^2 \equiv 1 \,(\mathrm{mod}\, 4)$$

e

$$m \equiv 3 \,(\mathrm{mod}\, 4) \Longrightarrow n = m^2 \equiv 3^2 \equiv 9 \equiv 1 \,(\mathrm{mod}\, 4).$$

Assim, concluímos que qualquer quadrado perfeito ímpar é congruente a 1 módulo 4. Portanto, a soma de dois quadrados perfeitos ímpares é congruente a $1 + 1 = 2$ módulo 4.

Suponha, agora, que $n^2 = m_1^2 + m_2^2$, em que m_1 e m_2 são ímpares. Então n^2 é par e

$$n^2 \equiv m_1^2 + m_2^2 \equiv 1 + 1 \equiv 2 \,(\mathrm{mod}\, 4).$$

Por outro lado, uma vez que n^2 par implica n par, digamos, $n = 2k$, com $k \in \mathbb{N}$. Então,

$$n^2 = (2k)^2 = 4k^2 \equiv 0 \,(\mathrm{mod}\, 4),$$

o que é uma contradição.

Desse modo, concluímos que a soma de dois quadrados perfeitos ímpares não pode ser um quadrado perfeito. □

Exemplo 9. *Mostre que, se p e q são números primos maiores que 3, então $p^2 - q^2$ é divisível por 24.*

Solução. Sejam p e q números primos maiores que 3. Vamos escrever $p^2 - q^2 = (p + q)(p - q)$ e analisar as possíveis congruências de $p-q$ e $p+q$ módulo 4. Uma vez que p e q são primos maiores do que 3, temos que p e q são ímpares, logo, p e q são congruentes a 1 ou a 3 módulo 4. Consideremos os cruzamentos de tais possibilidades:

$$\begin{aligned} &p \equiv 1(\mathrm{mod}\, 4) \text{ e } q \equiv 1 \,(\mathrm{mod}\, 4) \Longrightarrow \\ &\Longrightarrow p + q \equiv 2 \,(\mathrm{mod}\, 4) \text{ e } p - q \equiv 0 \,(\mathrm{mod}\, 4) \\ &\Longrightarrow p + q = 2q_1 \text{ e } p - q = 4q_2 \\ &\Longrightarrow (p + q)(p - q) = 8q_1q_2. \end{aligned}$$

$$\begin{aligned} &p \equiv 3(\mathrm{mod}\, 4) \text{ e } q \equiv 1 \,(\mathrm{mod}\, 4) \Longrightarrow \\ &\Longrightarrow p + q \equiv 4 \equiv 0 \,(\mathrm{mod}\, 4) \text{ e } p - q \equiv 2 \,(\mathrm{mod}\, 4) \\ &\Longrightarrow p + q = 4q_1 \text{ e } p - q = 2q_2 \\ &\Longrightarrow (p + q)(p - q) = 8q_1q_2. \end{aligned}$$

De modo similar, é possível verificar que $(p+q)(p-q)$ também é múltiplo de 8 quando $p \equiv 3$ e $q \equiv 1$ módulo 4, assim como quando $p \equiv 3$ e $q \equiv 3$ módulo 4.

Portanto, concluímos que, em qualquer caso, $(p+q)(p-q)$ é múltiplo de 8, se p e q são primos maiores do que 3.

Por outro lado, como p e q são primos maiores que 3, analisando as classes de restos módulo 3, temos que $p \equiv 1$ e $q \equiv 2$ (ou vice-versa), p,$q \equiv 1$ ou p,$q \equiv 2 \,(\mathrm{mod}\, 3)$. Agora,

$$p \equiv 1, q \equiv 2 \,(\mathrm{mod}\, 3) \Longrightarrow p + q \equiv 1 + 2 \equiv 0 \,(\mathrm{mod}\, 3);$$

$$p,q \equiv 1 \,(\mathrm{mod}\, 3) \Longrightarrow p - q \equiv 1 - 1 \equiv 0 \,(\mathrm{mod}\, 3);$$

$$p,q \equiv 2 \,(\mathrm{mod}\, 3) \Longrightarrow p - q \equiv 2 - 2 \equiv 0 \,(\mathrm{mod}\, 3).$$

Então, em qualquer caso, $p + q$ ou $p - q$ é um múltiplo de 3, de sorte que $(p+q)(p-q) \equiv 0 \,(\mathrm{mod}\, 3)$, ou seja, $(p+q)(p-q)$ é múltiplo de 3.

Portanto, como $p^2 - q^2 = (p+q)(p-q)$ é múltiplo de 8 e de 3, concluímos que $p^2 - q^2$ é múltiplo de $\mathrm{mmc}\,(8,3) = 24$. □

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 e reservem uma parte da aula para que os alunos tentem encontrar soluções por seus próprios meios. Em particular, antes de apresentar exemplos mais elaborados, recomendamos fortemente que os professores proponham vários exemplos mais simples, como o exemplo 1. Desse modo, os alunos adquirirão habilidades que são fundamentais para resolver outros problemas que envolvem congruências.

As referências a seguir contêm problemas de variados graus de dificuldade envolvendo congruências.

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.

2. D. Fomim, S. Genkin e I. Itenberg. *Círculos Matemáticos: A Experiência Russa.* Rio de Janeiro, IMPA 2012.

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