Material Teórico - Módulo Aritmética dos Restos

Problemas com Congruências - Parte 2

Tópicos Adicionais

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

10 de julho de 2023

Neste material, continuamos a apresentar problemas cujas soluções envolvem aritmética modular.

Exemplo 1. *Considere a sequência dos números primos,* $p_1 = 2 < p_2 = 3 < p_3 = 5 < \ldots$. *Se*

$$k_n = \prod_{i=1}^{n} p_i = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n,$$

mostre que $k_n - 1$ *e* $k_n + 1$ *não são quadrados perfeitos,* $\forall n > 1$.

Solução. Iniciamos recordando que um quadrado perfeito é congruente a 0 ou a 1 módulo 3. De fato, se m é um inteiro qualquer, então

$$\begin{aligned}
&m \equiv 0 \,(\mathrm{mod}\, 3) \Longrightarrow m^2 \equiv 0^2 \equiv 0 \,(\mathrm{mod}\, 3);\\
&m \equiv 1 \,(\mathrm{mod}\, 3) \Longrightarrow m^2 \equiv 1^2 \equiv 1 \,(\mathrm{mod}\, 3);\\
&m \equiv 2 \,(\mathrm{mod}\, 3) \Longrightarrow m^2 \equiv 2^2 \equiv 4 \equiv 1 \,(\mathrm{mod}\, 3).
\end{aligned}$$

Para simplificar a notação, vamos denotar $k = k_n$. Veja que $p_1 = 2$ e $p_2 = 3$, logo, $k \equiv 0 \,(\mathrm{mod}\, 3)$. Desse modo, $k - 1 \equiv -1 \equiv 2 \,(\mathrm{mod}\, 3)$ e, assim, $k - 1$ não pode ser quadrado perfeito. Veja que não podemos utilizar o mesmo raciocínio para mostrar que $k + 1$ não é quadrado perfeito, pois $k + 1 \equiv 1 \,(\mathrm{mod}\, 3)$; por outro lado, esse fato também não implica que $k + 1$ é quadrado perfeito. O único fato que podemos concluir a partir de $k + 1 \equiv 1 \,(\mathrm{mod}\, 3)$ é o de que a técnica anterior não funciona nesse caso. Entretanto, quando analisamos a divisibilidade por 4, para m inteiro, temos

$$\begin{aligned}
&m \equiv 0 \,(\mathrm{mod}\, 4) \Longrightarrow m^2 \equiv 0^2 \equiv 0 \,(\mathrm{mod}\, 4);\\
&m \equiv 1 \,(\mathrm{mod}\, 4) \Longrightarrow m^2 \equiv 1^2 \equiv 1 \,(\mathrm{mod}\, 3);\\
&m \equiv 2 \,(\mathrm{mod}\, 4) \Longrightarrow m^2 \equiv 2^2 \equiv 4 \equiv 0 \,(\mathrm{mod}\, 3);\\
&m \equiv 3 \,(\mathrm{mod}\, 4) \Longrightarrow m^2 \equiv 3^2 \equiv 9 \equiv 1 \,(\mathrm{mod}\, 3).
\end{aligned}$$

Assim, concluímos que um quadrado perfeito é congruente a 0 ou a 1 módulo 4. Agora, note que k é divisível por 2 (pois

$p_1 = 2$) e não é divisível por 4, pois há apenas um fator 2 em sua fatoração; logo, $k \equiv 2 \pmod 4$. Portanto,

$$k \equiv 2 \pmod 4 \Longrightarrow k+1 \equiv 3 \pmod 4.$$

Assim, concluímos que $k+1$ também não é quadrado perfeito. □

Exemplo 2. *A equação diofantina $15x^2 - 7y^2 = 9$ possui soluções inteiras? Em caso afirmativo, encontre essas soluções.*

Solução. Vamos admitir que essa equação possua soluções inteiras, isto é, suponhamos que exista um par de números inteiros (x,y) tal que $15x^2 - 7y^2 = 9$. Observe que $15 \equiv 0 \pmod 5$, $-7 \equiv -2 \pmod 5$ e $9 \equiv 4 \pmod 5$. Desse modo,

$$15x^2 - 7y^2 \equiv 0x^2 - 2y^2 \equiv -2y^2 \pmod 5$$

e, por outro lado,

$$15x^2 - 7y^2 = 9 \equiv 4 \pmod 5.$$

Logo,

$$-2y^2 \equiv 4 \pmod 5.$$

Como $\text{mdc}\,(2,5) = 1$, podemos "cancelar o 2" na última congruência para obter $-y^2 \equiv 2 \pmod 5$, ou, o que é o mesmo, $y^2 \equiv -2 \equiv 3 \pmod 5$. Por outro lado, se m é um inteiro qualquer, então

$$\begin{aligned}
&m \equiv 0 \pmod 5 \Longrightarrow m^2 \equiv 0^2 \equiv 0 \pmod 5;\\
&m \equiv 1 \pmod 5 \Longrightarrow m^2 \equiv 1^2 \equiv 1 \pmod 5;\\
&m \equiv 2 \pmod 5 \Longrightarrow m^2 \equiv 2^2 \equiv 4 \pmod 5;\\
&m \equiv 3 \pmod 5 \Longrightarrow m^2 \equiv 3^2 \equiv 9 \equiv 4 \pmod 5;\\
&m \equiv 4 \pmod 5 \Longrightarrow m^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod 5.
\end{aligned}$$

Assim, um quadrado perfeito só pode ser congruente a 0, 1 ou 4 módulo 5, portanto, nunca é congruente a 2 nem a 3. Daí, concluímos que a equação $15x^2 - 7y^2 = 9$ não possui soluções inteiras. □

Exemplo 3. *Mostre que a equação diofantina* $x^3+21y^2+5=0$ *não possui soluções inteiras.*

Solução. Para mostrar que a equação $x^3+21y^2+5=0$ não possui soluções inteiras, vamos utilizar congruências módulo 7. Iniciamos mostrando que um cubo perfeito é congruente a 0, 1 ou -1 módulo 7. De fato, se m é um inteiro qualquer, então

$$\begin{aligned}
&m \equiv 0 \pmod 7 \Longrightarrow m^3 \equiv 0^3 \equiv 0 \pmod 7;\\
&m \equiv 1 \pmod 7 \Longrightarrow m^3 \equiv 1^3 \equiv 1 \pmod 7;\\
&m \equiv 2 \pmod 7 \Longrightarrow m^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7;\\
&m \equiv 3 \pmod 7 \Longrightarrow m^3 \equiv 3^3 \equiv 27 \equiv -1 \pmod 7;\\
&m \equiv 4 \pmod 7 \Longrightarrow m^3 \equiv 4^3 \equiv 64 \equiv 1 \pmod 7;\\
&m \equiv 5 \pmod 7 \Longrightarrow m^3 \equiv 5^3 \equiv 125 \equiv -1 \pmod 7;\\
&m \equiv 6 \pmod 7 \Longrightarrow m^3 \equiv 6^3 \equiv 216 \equiv -1 \pmod 7.
\end{aligned}$$

Agora, suponha que exista um par de inteiros (x,y) tal que $x^3+21y^2+5=0$. Então, como $21 \equiv 0 \pmod 7$ e $5 \equiv -2 \pmod 7$, temos

$$\begin{aligned}
x^3+21y^2+5 \equiv 0 \pmod 7 &\Longrightarrow x^3+0y^2-2 \equiv 0 \pmod 7\\
&\Longrightarrow x^3-2 \equiv 0 \pmod 7\\
&\Longrightarrow x^3 \equiv 2 \pmod 7.
\end{aligned}$$

Como vimos antes, x^3 não pode ser congruente a 2 módulo 7. Portanto, temos uma contradição, o que implica a inexistência de soluções inteiras da equação $x^3+21y^2+5=0$. □

Observação 4. *O tipo de argumento utilizado nos exemplos 2 e 3 permite mostrar que certas equações diofantinas não possuem soluções inteiras. Contudo, ele não serve para mostrar que uma equação diofantina tem soluções inteiras. Por exemplo, perceba que a inexistência de soluções módulo* 5 *ou módulo* 7 *implica a inexistência de soluções inteiras, mas a recíproca não é verdadeira. De fato, uma equação pode*

ter soluções módulo m, para algum m inteiro, mas não possuir soluções inteiras. Por exemplo, $2x = 1$ possui soluções módulo 5 ($x \equiv 3$), mas não possui soluções inteiras.

Exemplo 5. *Existem inteiros positivos m e n tais que $3^m + 7 = 2^n$?*

Solução. Inicialmente, veja que $2 \equiv -1 \pmod 3$, o que implica $2^n \equiv (-1)^n \pmod 3$. Logo, 2^n é congruente a 1 módulo 3 quando n é par e congruente a -1 módulo 3 quando n é ímpar. Mas $3^m \equiv 0 \pmod 3$ e $7 \equiv 1 \pmod 3$, o que acarreta $3^m + 7 \equiv 1 \pmod 3$. Portanto, se m e n são inteiros positivos tais que $3^m + 7 = 2^n$, então $2^n = 3^m + 7 \equiv 1 \pmod 3$, de onde concluímos que n é par. Seja, então, $k \in \mathbb{N}$ tal que $n = 2k$. Temos que

$$\begin{aligned} 3^m + 7 = 2^{2k} &\Longrightarrow 3^m + 7 = \left(2^2\right)^k \\ &\Longrightarrow 3^m + 7 = 4^k. \end{aligned}$$

Por outro lado, temos que $3 \equiv -1 \pmod 4$, logo, $3^m \equiv (-1)^m \pmod 4$. Daí, 3^m é congruente a 1 módulo 4 se m é par e congruente a -1 módulo 4 se m é ímpar. Mas $4^k \equiv 0 \pmod 4$ e $-7 \equiv 1 \pmod 4$, de modo que $3^m \equiv 4^k - 7 \equiv 1 \pmod 4$. Assim, concluímos que m também é par, digamos, $m = 2q$. Juntando as informações obtidas acima, garantimos a existência de naturais k e q tais que

$$3^{2q} + 7 = 2^{2k},$$

ou, o que é o mesmo,

$$\left(2^k\right)^2 - \left(3^q\right)^2 = 7.$$

Uma vez que o lado esquerdo da última equação é uma diferença de quadrados, podemos reescrevê-la como

$$\left(2^k + 3^q\right)\left(2^k - 3^q\right) = 7.$$

Desse modo, concluímos que $2^k + 3^q = 7$ e $2^k - 3^q = 1$, pois o único modo de escrever 7 como produto de dois números

inteiros positivos é $7 = 7 \cdot 1$. Somando as duas últimas equações, obtemos $2 \cdot 2^k = 8$, logo, $k = 2$ e $n = 2k = 4$. Subtraindo as duas equações, obtemos $2 \cdot 3^q = 6$, logo $q = 1$ e $m = 2q = 2$.

Portanto, a única solução inteira de $3^m + 7 = 2^n$ é o par $(m,n) = (2,4)$. □

Exemplo 6. *Prove que qualquer número inteiro positivo é congruente à soma de seus algarismos, módulo* 9 *e módulo* 3.

Solução. Seja $a_0a_1 \ldots a_n$ um número inteiro positivo; então, temos

$$a_0a_1 \ldots a_{n-1}a_n = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + \ldots + a_{n-1} \cdot 10 + a_n.$$

Como

$$\begin{aligned} 10^k - 1 &= 10^k - 1^k \\ &= (10-1)\left(10^{k-1} + 10^{k-2} + \ldots + 1\right) \\ &= 9\left(10^{k-1} + 10^{k-2} + \ldots + 1\right), \end{aligned}$$

temos $10^k \equiv 1 \pmod 9$. Desse modo, módulo 9, obtemos

$$\begin{aligned} a_0a_1 \ldots a_{n-1}a_n &\equiv a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + \ldots + a_{n-1} \cdot 10 + a_n \\ &\equiv a_0 \cdot 1 + a_1 \cdot 1 + \ldots + a_{n-1} \cdot 1 + a_n \\ &\equiv a_0 + a_1 + \ldots + a_{n-1} + a_n. \end{aligned}$$

Concluímos, assim, que qualquer inteiro positivo é congruente à soma de seus algarismos módulo 9. Por outro lado, uma vez que

$$a \equiv b \pmod 9 \Rightarrow 9 \mid (a-b) \Rightarrow 3 \mid (a-b) \Rightarrow a \equiv b \pmod 3,$$

segue que qualquer inteiro positivo é congruente à soma de seus algarismos módulo 3. □

Exemplo 7. *Foi calculada a soma dos algarismos da representação decimal do número* 2^{2023}*. Depois disso, foi calculada a soma dos algarismos do número resultante, e assim por diante, até o resultado da soma ser um único algarismo. Que algarismo é esse?*

Solução. Veja que $2^3 = 8 \equiv -1 \pmod 9$. Além disso,

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

logo, $2023 = 3 \cdot 674 + 1$. Então

$$\begin{aligned} 2^3 \equiv -1 \pmod 9 &\Longrightarrow \left(2^3\right)^{674} \equiv (-1)^{674} \pmod 9 \\ &\Longrightarrow 2^{3\cdot 674} \equiv 1 \pmod 9 \\ &\Longrightarrow 2^{3\cdot 674} \cdot 2 \equiv 1 \cdot 2 \pmod 9 \\ &\Longrightarrow 2^{3\cdot 674+1} \equiv 2 \pmod 9 \\ &\Longrightarrow 2^{2023} \equiv 2 \pmod 9. \end{aligned}$$

Agora, utilizando o resultado apresentado no exemplo 6, temos que 2^{2023} é congruente à soma dos algarismos de sua representação decimal módulo 9. Por sua vez, o resultado dessa soma também é congruente à soma de seus algarismos módulo 9, e assim por diante, até que o último algarismo restante também é congruente a 2^{2023}, módulo 9. Concluímos, portanto, que esse algarismo deve ser igual a 2. □

Encerramos este material com o problema abaixo, que fez parte da prova da Olimpíada Internacional de Matemática - IMO de 1975.

Exemplo 8. *Seja A a soma dos algarismos de 4444^{4444}, quando esse número é escrito em notação decimal. Seja B a soma dos algarismos de A. Encontre a soma dos algarismos de B.*

Solução. Vamos denotar por C a soma dos algarismos de B. Veja que

$$4444^{4444} < \left(10^4\right)^{4444} = 10^{4\cdot 4444} = 10^{17776}.$$

Desse modo, 4444^{4444} tem, no máximo, 17776 algarismos, logo, a soma de seus algarismos satisfaz

$$A \leq 17776 \cdot 9 = 159984.$$

Assim, A tem no máximo 6 algarismos e, se tiver exatamente 6 algarismos, o algarismo das centenas de milhar é igual a 1 e o das dezenas de milhar é no máximo 5. Portanto, o número inteiro entre 1 e 159984 cuja soma dos algarismos é a maior possível é 99999, logo, B, que é a soma dos algarismos de A, vale no máximo $5 \cdot 9 = 45$. Agora, note que 39 é o número entre 1 e 45 cuja soma dos algarismos é a maior possível. Portanto, a soma dos algarismos de B é, no máximo, $3 + 9 = 12$.

Por outro lado, pelo exemplo 6, sabemos que

$$4444^{4444} \equiv A \equiv B \equiv C \pmod 9.$$

Além disso, uma vez que

$$\begin{array}{r|l} 4\,4\,4\,4 & 9 \\ \cline{2-2} 8\,4 & 4\,9\,3 \\ 3\,4 & \\ 7 & \end{array}$$

temos

$$\begin{aligned} 4444 \equiv 7 \pmod 9 &\implies 4444^2 \equiv 7^2 \pmod 9 \\ &\implies 4444^2 \equiv 49 \equiv 4 \pmod 9 \\ &\implies 4444^2 \cdot 4444 \equiv 4 \cdot 7 \pmod 9 \\ &\implies 4444^3 \equiv 28 \equiv 1 \pmod 9. \end{aligned}$$

Uma vez que $4444 = 3 \cdot 1481 + 1$, obtemos

$$\begin{aligned} 4444^3 \equiv 1 \pmod 9 &\implies \left(4444^3\right)^{1481} \equiv 1^{1481} \pmod 9 \\ &\implies 4444^{3 \cdot 1481} \equiv 1 \pmod 9 \\ &\implies 4444^{3 \cdot 1481} \cdot 4444 \equiv 1 \cdot 4444 \pmod 9 \\ &\implies 4444^{3 \cdot 1481 + 1} \equiv 4444 \equiv 7 \pmod 9 \\ &\implies 4444^{4444} \equiv 7 \pmod 9. \end{aligned}$$

Daí, segue que $C \equiv 7 \pmod 9$. Como $1 \leq C \leq 12$, concluímos que $C = 7$. □

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, apresente alguns exemplos numéricos com a ideia do exemplo 6 antes de apresentar o resultado geral, pois isso facilita o entendimento. Além disso, apresente outros exemplos mais simples antes de propor o exemplo 8. Em relação à observação 4, é fundamental que os alunos entendam que o argumento utilizado nos exemplos 2 e 3 serve apenas para mostrar que não existe solução.

Sugestões de Leitura Complementar

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