Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
v. 23, n. 2, dez. 2023
Artigo de Iniciação Científica

Congruências numéricas: cinco problemas resolvidos propostos para olimpíadas internacionais de matemática

Numerical congruences: five solved problems proposed for international mathematics olympiads

Juan López Linares
Faculdade de Zootecnia e Engenharia de Alimentos
Universidade de São Paulo
jlopez@usp.br

Alexys Bruno-Alfonso
Faculdade de Ciências de Bauru
UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho"
alexys.bruno-alfonso@unesp.br

Grazielle Feliciani Barbosa
Universidade Federal de São Carlos
grazielle.barbosa@ufscar.br

Resumo

As congruências numéricas, também chamadas de Aritmética do relógio ou dos restos, são um assunto usualmente omitido nos programas de Ensino Médio no Brasil. Neste artigo são discutidos cinco problemas propostos para a Olimpíada Internacional de Matemática. Os problemas investigam a divisibilidade por 7 dos números $2^n - 1$ e $2^n + 1$, uma equação diofantina não linear, uma sequência em que cada número é encontrado pela soma dos dígitos do anterior, números com três últimos dígitos iguais e uma recorrência com quadrados perfeitos. São utilizadas congruências módulo 2, 3, 5, 7, 8, 9, 125 e 1000 e a fórmula do binômio de Newton.

Palavras-chave: Olimpíadas internacionais de matemática. Congruências numéricas. Ensino médio. Ensino universitário. Binômio de Newton.

Abstract

Numerical congruences, also called clock or remainder arithmetic, are a subject usually omitted in high school programs in Brazil. In this article five problems proposed for the International Mathematical Olympiad are discussed. The problems investigate the divisibility by 7 of the numbers $2^n - 1$ and $2^n + 1$, a non-linear Diophantine equation, a sequence where each number is found by summing the digits of the previous one, numbers with three last digits equals and a recurrence with perfect squares. Congruences modulo 2, 3, 5, 7, 8, 9, 125 and 1000 and Newton's binomial formula are used.

Keywords: International mathematical olympiads. Numerical congruences. High school. University education. Newton's binomial.

Artigo recebido em mar. 2023 e aceito em jul. 2023

1 Introdução

As congruências numéricas, também chamadas de Aritmética do relógio ou dos restos, são um assunto usualmente omitido nos programas de Ensino Médio no Brasil. Porém, ele entra no programa das Olimpíadas de Matemática em nível nacional e internacional.

A divisão inteira (com resto), atualmente chamada euclidiana, foi sistematizada por volta de 300 AC, em Alexandria, num conjunto de livros que se tornaria um dos marcos mais importantes da Matemática: Os Elementos de Euclides. Carl Friedrich Gauss foi o grande introdutor das congruências em 1801, no livro Disquisitiones Arithmeticae (GAUSS, 1965).

Congruências numéricas aparecem com muita frequência nos problemas da IMO relacionadas a diversos assuntos. Neste artigo discutem-se cinco problemas, que utilizam conhecimentos diferentes, mas sem a pretensão de esgotar o tema.

Embora úteis e proveitosas, as resoluções apresentadas nos fóruns de problemas da Olimpíada Internacional de Matemática (IMO) não detalham muitas transições, as quais ficam para o leitor. Os autores parecem supor que todos têm conhecimentos matemáticos suficientemente avançados. Adicionalmente, essas resoluções encontram-se frequentemente em inglês.

A apresentação visa que o material possa ser lido e compreendido por estudantes de língua portuguesa (e talvez espanhola) que preparam-se para as fases finais das olimpíadas nacionais ou internacionais. Espera-se também que esta abordagem sirva de apoio aos professores do Ensino Médio que aventuram-se em tópicos mais avançados. Em comparação com outras soluções disponíveis, as apresentadas no artigo utilizam argumentos menos rebuscados e um número menor de transições a serem preenchidas pelo leitor.

Na preparação para uma Olimpíada Internacional de Matemática cada delegação (menos o país sede) pode enviar problemas para formar a base de dados inicial, chamada lista longa (LongList, LL). Os mesmos não podem ter sido utilizados em competições anteriores, nem publicados e devem abranger vários tópicos de Matemática pré-universitária. O país sede da competição cria um Comitê de Seleção que escolhe os melhores problemas da LL para formar a lista curta (ShortList, SL). Os professores líderes, um por equipe, recebem a SL no primeiro dia da reunião e escolhem, por maioria simples, os seis problemas da SL que serão usados na IMO. As duas listas são mantidas em segredo até a IMO do próximo ano.

2 Definições, conceitos básicos e exemplos

Teorema 1 (Divisão Euclidiana)**.** *Dados $a \in \mathbb{Z}$ e $m \in \mathbb{N}$, existem q (quociente) e r (resto) inteiros únicos tais que:*

$$a = qm + r,\ 0 \leq r < m.$$

A demonstração da existência e unicidade de q e r pode ser encontrada, por exemplo, na página 46 de Hefez (2016).

Exemplo 2. *A divisão de* 7 *e* -7 *por* 3 *pode ser escrita como:* $7 = 2 \cdot 3 + 1$ *e* $-7 = -3 \cdot 3 + 2$.

Definição 3 (Divisibilidade)**.** *Quando o resto de uma divisão euclidiana de $a \in \mathbb{Z}$ por $m \in \mathbb{N}$ é zero ($\exists q \in \mathbb{Z}$ tal que $a = qm$) é dito que m divide a e denota-se:*

$$m \mid a.$$

Quando m não divide a escreve-se:

$$m \nmid a.$$

Exemplo 4. *Tem-se que* $7 \mid 21$ *pois* $21 = 3 \cdot 7$. *Por outro lado,* $7 \nmid 22$ *pois* $22 = 3 \cdot 7 + 1$.

Definição 5 (M.D.C.)**.** *Sejam* $a, b \in \mathbb{Z}$. *Por simplicidade, o máximo (maior) divisor comum (M.D.C.) entre os números* a *e* b *será denotado por:*

$$(a, b).$$

Exemplo 6. *Para os números* $6 = 2 \cdot 3$, $8 = 2^3$ *e* $9 = 3^2$ *vale que* $(6, 8) = 2$, $(6, 9) = 3$ *e* $(8, 9) = 1$.

Definição 7 (Primos entre si ou Coprimos)**.** *Sejam* $a, b \in \mathbb{Z}$. *Os números* a *e* b *serão chamados Primos entre si ou Coprimos quando:*

$$(a, b) = 1.$$

Exemplo 8. *Os números* $9 = 3^2$ *e* $10 = 2 \cdot 5$ *não são primos. Porém, como* $(9, 10) = 1$ *são classificados como primos entre si ou coprimos.*

Definição 9 (Números congruentes)**.** *É dito que* $a, b \in \mathbb{Z}$ *são congruentes módulo* $m \in \mathbb{N}$ *quando deixam o mesmo resto na divisão euclidiana por* m *e escreve-se:*

$$a \equiv b \mod m.$$

No caso em que o resto é diferente é dito que os números não são congruentes e escreve-se:

$$a \not\equiv b \mod m.$$

Exemplo 10. *Relativo ao resto da divisão por* 3 *escreve-se:* $7 \equiv 1 \mod 3$, $-7 \equiv 2 \mod 3$ *e* $7 \not\equiv 0 \mod 3$.

Segue da Definição 9 que a congruência é uma relação de equivalência pois são válidas as três propriedades enunciadas nas próximas linhas.

Proposição 11. *Seja* $m \in \mathbb{N}$. *Para* $a, b, c \in \mathbb{Z}$ *vale:*
i) $a \equiv a \mod m$ *(reflexividade),*
ii) Se $a \equiv b \mod m$, *então* $b \equiv a \mod m$ *(simetria),*
iii) Se $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$ *(transitividade).*

Para determinar a congruência entre dois números nem sempre é preciso calcular a divisão euclidiana. Pode ser utilizado o resultado enunciado a seguir.

Proposição 12. *Sejam* $a, b \in \mathbb{Z}$. *Tem-se* $a \equiv b \mod m$ *se, e somente se,* m *divide* $a - b$.

Demonstração. Sejam $a = qm + r$ com $0 \leq r < m$ e $b = q'm + r'$ com $0 \leq r < m$. Suponha-se primeiro que $a \equiv b \mod m$. Pela Definição 9, tem-se $r = r'$ e

$$a - b = qm + r - (q'm + r') = (q - q')m + (r - r') = dm.$$

Como $q - q' = d \in \mathbb{Z}$, segue que $m \mid a - b$. Reciprocamente, se $m \mid a - b$ existe $d \in \mathbb{Z}$ tal que:

$$a - b = dm = qm + r - (q'm + r') = (q - q')m + (r - r').$$

Pela restrição $\mid r - r' \mid < m$ deve-se ter $r = r'$. Novamente, da Definição 9, encontra-se:

$$a \equiv b \mod m.$$

□

Exemplo 13. *Vale que:*

$$75 \equiv 5 \mod 7 \Leftrightarrow 75 - 5 = 70 = 10 \cdot 7 \ (7 \mid 75 - 5),$$

$$-15 \equiv 6 \mod 7 \Leftrightarrow -15 - 6 = -21 = -3 \cdot 7 \ (7 \mid -15 - 6).$$

Proposição 14. *Sejam $a, b, c, d, m \in \mathbb{N}$.*
i) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.
ii) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $ac \equiv bd \mod m$.

Demonstração. Por hipótese tem-se $a \equiv b \mod m$ e $c \equiv d \mod m$. Ou seja, pela Proposição 12, tem-se $m \mid b - a$ e $m \mid d - c$.

i) Nota-se que o anterior implica que $m \mid (b - a) + (d - c)$. Portanto, $m \mid (b + d) - (a + c)$. Utilizando novamente a Proposição 12 obtêm-se que $a + c \equiv b + d \mod m$.

ii) Como $m \mid (b - a)$, então $m \mid d(b - a)$. Analogamente, de $m \mid (d - c)$, então $m \mid a(d - c)$. Segue, $m \mid d(b - a) + a(d - c) = bd - ac$. Mais uma vez, da Proposição 12, resulta $ac \equiv bd \mod m$. □

Exemplo 15. *Vale que:*
i) Se $19 \equiv 13 \mod 6$ e $11 \equiv 5 \mod 6$, então $30 \equiv 18 \mod 6$.
ii) Se $-4 \equiv 2 \mod 3$ e $1 \equiv 4 \mod 3$, então $-4 \equiv 8 \mod 3$.

Corolário 16. *Sejam $n, \lambda \in \mathbb{Z}$ e $m \in \mathbb{N}$. Somar um múltiplo de m não muda uma congruência módulo m:*

$$n + \lambda m \equiv n \mod m.$$

Demonstração. Seja a divisão euclidiana $n = qm + r$ com $0 \leq r < m$. Tem-se:

$$n + \lambda m = (qm + r) + \lambda m = (q + \lambda)m + r.$$

Ou seja, n e $n + \lambda m$ deixam o mesmo resto na divisão por m e, consequentemente, vale:

$$n + \lambda m \equiv n \mod m.$$

□

Exemplo 17. *Para todo $\lambda \in \mathbb{Z}$ vale que:*

$$7 + 3\lambda \equiv 7 \mod 3.$$

Corolário 18. *Sejam $a, b \in \mathbb{Z}$ e $m, n \in \mathbb{N}$. Se $a \equiv b \mod m$, então para todo n vale:*

$$a^n \equiv b^n \mod m.$$

Demonstração. A demostração é feita por indução e a utilização do item ii) da Proposição 14. □

Exemplo 19. *Como $23 \equiv 2 \mod 3$ vale que $23^6 \equiv 2^6 \mod 3$.*

A seguir mostra-se que vale a lei do cancelamento para a soma.

Proposição 20 (Cancelamento na soma)**.** *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. Se $a + c \equiv b + c \mod m$, então $a \equiv b \mod m$.*

Demonstração. Da hipótese, segue que $m \mid (b+c)-(a+c)$. Ou seja, $m \mid b-a$. □

Exemplo 21. *Como* $27 = 23 + \not{4} \equiv 2 + \not{4} = 6 \mod 3$, *então* $23 \equiv 2 \mod 3$.

Será visto a seguir que a lei do cancelamento para o produto vale somente quando c e m são primos entre si.

Proposição 22. *Sejam* $a, b, c, m \in \mathbb{Z}$ *com* $m > 1$. *Se* $ac \equiv bc \mod m$, *então* $a \equiv b \mod \left(\frac{m}{(c,m)}\right)$.

Demonstração. Da hipótese segue que $m \mid (bc)-(ac) = (b-a)c$. O máximo divisor comum de c e m divide ambos. Pode ser escrito:

$$\frac{m}{(c,m)} \;\Big|\; (b-a)\frac{c}{(c,m)} .$$

Como os números inteiros $\frac{c}{(c,m)}$ e $\frac{m}{(c,m)}$ são coprimos somente resta a possibilidade de:

$$\frac{m}{(c,m)} \mid (b-a) \Leftrightarrow a \equiv b \mod \left(\frac{m}{(c,m)}\right).$$

□

Exemplo 23. *De* $12 \cdot 18 - 12 \cdot 10 = 216 - 120 = 96$ *e* $16 \mid 96$ *tem-se que* $12 \cdot 18 \equiv 12 \cdot 10 \mod 16$. *Não é possível cancelar o número* 12 *pois* $18 \not\equiv 10 \mod 16$. *Porém, como* $(12, 16) = 4$, *então vale que:*

$$18 \equiv 10 \mod 4.$$

Corolário 24. *Sejam* $a, b, c, m \in \mathbb{Z}$ *com* $m > 1$ *e* $(c, m) = 1$. *Se* $ac \equiv bc \mod m$, *então* $a \equiv b \mod m$.

Demonstração. Segue diretamente da Proposição 22 e a hipótese $(c, m) = 1$. □

Exemplo 25. *Como* $(3, 4) = 1$, *então vale que:*

$$18 = 6 \cdot \not{3} \equiv 2 \cdot \not{3} = 6 \mod 4 \Leftrightarrow 6 \equiv 2 \mod 4.$$

Proposição 26 (Congruências módulo 9 e 3)**.** *Um número inteiro a, representado na base decimal como* $(a_n a_{n-1} \ldots a_1 a_0)_{10}$, *é congruente com a soma dos seus dígitos* a_i, $0 \leq i \leq n$, *módulo* 9 *e* 3. *Ou seja,*

$$a \equiv a_n + a_{n-1} + \ldots + a_1 + a_0 \mod 9,$$
$$a \equiv a_n + a_{n-1} + \ldots + a_1 + a_0 \mod 3.$$

Demonstração. Sabe-se que:

$$10 \equiv 1 \mod 9,$$
$$10 \equiv 1 \mod 3$$

e para todo $n \in \mathbb{N}$, pelo Corolário 18, tem-se:

$$10^n \equiv 1^n = 1 \equiv 1 \mod 9,$$
$$10^n \equiv 1^n = 1 \equiv 1 \mod 3.$$

Lembrando o significado da representação decimal:

$$a = (a_n a_{n-1} \dots a_1 a_0)_{10} = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10 a_1 + a_0.$$

Segue das equações anteriores, da Proposição 14 e o Corolário 18 que:

$$a = (a_n a_{n-1} \dots a_1 a_0)_{10} \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \mod 9,$$

$$a = (a_n a_{n-1} \dots a_1 a_0)_{10} \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \mod 3.$$

□

Exemplo 27. *Vale que:*

$$5849476 \equiv 5 + 8 + 4 + 9 + 1 + 7 + 6 = 43 \equiv 4 + 3 = 7 \mod 9,$$

$$5849476 \equiv 5 + 8 + 4 + 9 + 1 + 7 + 6 = 43 \equiv 4 + 3 = 7 \equiv 1 \mod 3.$$

Segue uma propriedade importante sobre quadrados perfeitos e sua relação com a divisão euclidiana por 3.

Proposição 28 ($n^2 \not\equiv 2 \mod 3$)**.** *Seja $n \in \mathbb{Z}$.*
a) Se $n^2 \equiv 0 \mod 3$, então $n \equiv 0 \mod 3$,
b) Se $n^2 \equiv 1 \mod 3$, então $n \equiv 1 \mod 3$ ou $n \equiv 2 \mod 3$.
Ou seja, nenhum quadrado perfeito deixa resto 2 na divisão por 3 ($n^2 \not\equiv 2 \mod 3$).

Demonstração. Qualquer número $n \in \mathbb{Z}$ é de uma das três formas:
i) $n = 3k$ com $k \in \mathbb{Z}$ ou $n \equiv 0 \mod 3$,
ii) $n = 3k + 1$ com $k \in \mathbb{Z}$ ou $n \equiv 1 \mod 3$,
iii) $n = 3k + 2$ com $k \in \mathbb{Z}$ ou $n \equiv 2 \mod 3$.
Porém, somente existem duas possibilidades na divisão de um quadrado perfeito por 3:
i) $n^2 = (3k)^2 = 3(3k^2) = 3l$ com $l \in \mathbb{Z}$ ou $n^2 \equiv 0 \mod 3$,
ii) $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 = 3l + 1$ com $l \in \mathbb{Z}$ ou $n^2 \equiv 1 \mod 3$,
iii) $n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1 = 3l + 1$ com $l \in \mathbb{Z}$ ou $n^2 \equiv 1 \mod 3$. □

3 Problemas resolvidos

3.1 Divisibilidade por sete, congruência módulo três. IMO 1964 P1.

Problema 1. *(a) Encontrar todos os números naturais n tais que o número $2^n - 1$ seja divisível por 7. (b) Provar que, para todos os números naturais n, o número $2^n + 1$ não é divisível por 7.*

A IMO 1964 foi realizada na cidade de Moscou, Rússia. Problema 1 da competição, proposto pela delegação da antiga Checoslováquia (DJUKIC *et al*, 2011).

3.1.1 Resolução do Problema 1

Seja $k \in \mathbb{Z}$ com $k \geq 0$. O número natural n pode ser representado, considerando a divisão euclidiana por 3, na forma:

$$n = 3k + r, \ r \in \{0, 1, 2\}.$$

Com o anterior, a potência de 2 pode ser escrita como:

$$2^n = 2^{3k+r} = \left(2^3\right)^k \cdot 2^r = 8^k \cdot 2^r.$$

Relativo à divisão por 7 pode ser escrito para todo k que:

$$2^n = 8^k \cdot 2^r \equiv 1^k \cdot 2^r \equiv 2^r \mod 7.$$

Ou seja,

$$2^n \equiv \begin{cases} 1, & \text{se } r = 0 \\ 2, & \text{se } r = 1, \\ 4, & \text{se } r = 2 \end{cases} \mod 7.$$

Segue que:

$$2^n - 1 \equiv \begin{cases} 0, & \text{se } r = 0 \\ 1, & \text{se } r = 1, \\ 3, & \text{se } r = 2 \end{cases} \mod 7.$$

Isto é, $2^n - 1$ é divisível por 7 quando n é múltiplo de 3 ($r = 0 \Leftrightarrow n \equiv 0 \mod 3$).
Analogamente,

$$2^n + 1 \equiv \begin{cases} 2, & \text{se } r = 0 \\ 3, & \text{se } r = 1, \\ 5, & \text{se } r = 2 \end{cases} \mod 7.$$

Isso significa que 7 nunca divide $2^n + 1$. Os únicos restos possíveis são 2, 3 e 5.

3.2 Equação diofantina não linear, congruência módulo três. IMO 1967 LL P38.

Problema 2. *Existe um número inteiro tal que seu cubo é igual a $3n^2 + 3n + 7$, onde n também é inteiro?*

A IMO 1967 foi realizada na antiga Iugoslávia. Problema 38 da LL, proposto pela delegação da Polônia (DJUKIC *et al*, 2011).

3.2.1 Resolução do Problema 2

Procuram-se $m, n \in \mathbb{Z}$ tais que:

$$m^3 = 3n^2 + 3n + 7. \tag{1}$$

Do lado direito de (1) nota-se:

$$3n^2 + 3n + 7 \equiv 1 \mod 3. \tag{2}$$

Combinando (1) e (2) deve-se ter:

$$m^3 \equiv 1 \mod 3. \tag{3}$$

Dado $k \in \mathbb{Z}$, em relação à divisão por 3, um inteiro m pode ser classificado como: i) $m = 3k$, ii) $m = 3k + 1$, iii) $m = 3k + 2$.

Portanto,

i) $m^3 = (3k)^3 = 3(9k^3) \equiv 0 \mod 3$,

ii) $m^3 = (3k + 1)^3 = 3(9k^3 + 9k^2 + 3k) + 1 \equiv 1 \mod 3$,

iii) $m^3 = (3k + 2)^3 = 3(9k^3 + 18k^2 + 12k) + 8 \equiv 2 \mod 3$.

Ou seja, a única possibilidade de satisfazer a congruência (3) é que para algum $k \in \mathbb{Z}$:

$$m = 3k + 1. \tag{4}$$

Substituindo (4) em (1) encontra-se:

$$3(9k^3 + 9k^2 + 3k) + 1 = 3n^2 + 3n + 7,$$

$$3(9k^3 + 9k^2 + 3k) = 3(n^2 + n + 2),$$

$$9k^3 + 9k^2 + 3k = n^2 + n + 2. \tag{5}$$

Do lado esquerdo de (5) tem-se:

$$9k^3 + 9k^2 + 3k \equiv 0 \mod 3. \tag{6}$$

Dado $l \in \mathbb{Z}$ para o lado direito de (5) vale:

i) $n = 3l \Rightarrow n^2 + n + 2 = 9l^2 + 3l + 2 \equiv 2 \mod 3$,

ii) $n = 3l + 1 \Rightarrow n^2 + n + 2 = (9l^2 + 6l + 1) + (3l + 1) + 2 = 9l^2 + 9l + 4 \equiv 1 \mod 3$,

iii) $n = 3l + 2 \Rightarrow n^2 + n + 2 = (9l^2 + 12l + 4) + (3l + 2) + 2 = 9l^2 + 15l + 8 \equiv 2 \mod 3$.

Ou seja, $n^2 + n + 2 \not\equiv 0 \mod 3$. Isto está em contradição com (5) e (6). Portanto, não existem soluções inteiras da equação (1).

3.3 Soma dos dígitos, congruência módulo nove. IMO 1975 P4.

Problema 3. *Seja A a soma dos dígitos do número 16^{16} e B a soma dos dígitos do número A. Encontrar a soma dos dígitos do número B sem calcular 16^{16}.*

A IMO 1975 foi realizada na cidade de Burgas, Bulgária. Problema 6 da SL e 4 da competição, proposto pela delegação da antiga União Soviética (DJUKIC *et al*, 2011).

3.3.1 Resolução do Problema 3

É solicitada a soma dos dígitos do número B, a qual denota-se por C. Cada elemento é encontrado pela soma dos dígitos do anterior na sequência $\left(16^{16}, A, B, C\right)$. Lembrando da Proposição 26 escreve-se:

$$16^{16} \equiv A \equiv B \equiv C \mod 9.$$

Ainda:

$$16^{16} = \left(2^4\right)^{16} = 2^{64}.$$

O resultado anterior sugere estudar a congruência módulo nove das potências de 2:

$$2^1 = 2 \equiv 2 \mod 9,$$

$$2^2 = 4 \equiv 4 \mod 9,$$

$$2^3 = 8 \equiv 8 \mod 9,$$

$$2^4 = 16 \equiv 7 \mod 9,$$

$$2^5 = 2^4 \cdot 2 \equiv 7 \cdot 2 = 14 \equiv 5 \mod 9,$$

$$2^6 = 2^5 \cdot 2 \equiv 5 \cdot 2 = 10 \equiv 1 \mod 9.$$

Como a menor potência de 2 que leva a uma congruência 1 é 6 escreve-se a divisão euclidiana do número 64 por 6:

$$64 = 10 \cdot 6 + 4.$$

Segue que:

$$16^{16} = 2^{64} = 2^{6 \cdot 10 + 4} = \left(2^6\right)^{10} \cdot 2^4,$$

$$16^{16} = \left(2^6\right)^{10} \cdot 2^4 \equiv 1^{10} \cdot 2^4 \equiv 2^4 \equiv 7 \mod 9.$$

Resumindo, tem-se que:

$$16^{16} \equiv A \equiv B \equiv C \equiv 7 \mod 9.$$

Por outro lado,

$$16^{16} < 100^{16} = \left(10^2\right)^{16} = 10^{32}.$$

Isto é, o número 16^{16} tem no máximo 32 dígitos, sendo todos menores ou iguais que 9. Portanto, $A \leq 32 \cdot 9 = 288$. Até 288 o número natural com maior soma dos seus dígitos é o 199. Segue que $B \leq 1 + 9 + 9 = 19$ e $C \leq 1 + 9 = 10$. Como o número C não pode ser superior a 10 e deve ser congruente a 7 módulo 9 tem-se que $C = 7$.

Com a ajuda de uma calculadora pode-se verificar:

$$16^{16} = 18446744073709551616.$$

Logo, $A = 88$, $B = 16$ e $C = 7$. Uma das belezas do uso de congruências consiste em poder lidar com números grandes sem apelar ao uso do computador.

3.4 Congruências módulo 2, 5, 8, 125 e 1000. IMO 1978 P1.

Problema 4. *Sejam $n > m \geq 1$ números naturais tais que os grupos dos três últimos dígitos nas representações decimais de 1978^m e 1978^n coincidem. Encontrar o par ordenado (m, n) para o qual $m + n$ é mínimo.*

A IMO 1978 foi realizada na cidade de Bucareste, capital da Romênia. O problema acima foi proposto pela delegação de Cuba e escolhido como o primeiro da competição (DJUKIC *et al*, 2011).

3.4.1 Resolução do Problema 4

Como os grupos dos três últimos dígitos nas representações decimais de 1978^m e 1978^n coincidem, a diferença deles é divisível por 1000. Isto é,

$$1000 \mid 1978^n - 1978^m = 1978^m \left(1978^{n-m} - 1\right). \tag{7}$$

Tem-se que $1000 = 8 \cdot 125 = 2^3 \cdot 5^3$, logo vale que:

$$8 \mid 1978^m \left(1978^{n-m} - 1\right), \tag{8}$$

$$125 \mid 1978^m \left(1978^{n-m} - 1\right). \tag{9}$$

Como $n > m$, $2 \mid 1978$ e $2 \mid 1978^{n-m}$, mas $2 \nmid (1978^{n-m} - 1)$, para satisfazer (8) deve-se ter que:

$$8 \mid 1978^m. \tag{10}$$

O resto na divisão por 8 de 1978 é 2:

$$1978 \equiv 2 \mod 8.$$

Adicionalmente,

$$1978^3 \equiv 2^3 \equiv 0 \mod 8.$$

Ou seja, deve-se ter que $m \geq 3$. Por outro lado, tem-se que:

$$\begin{gathered} 1978 \equiv 3 \mod 5, \\ 1978^2 \equiv 3^2 = 9 \equiv 4 \mod 5, \\ 1978^3 \equiv 3^3 \equiv 3 \cdot 4 = 12 \equiv 2 \mod 5, \\ 1978^4 \equiv 3^4 \equiv 3 \cdot 2 = 6 \equiv 1 \mod 5, \\ 1978^5 \equiv 3^5 \equiv 3 \cdot 1 = 3 \mod 5. \end{gathered} \tag{11}$$

As congruências anteriores mostram que os únicos restos permitidos na divisão por 5 de potências de 1978 são 1, 2, 3 e 4. Isto é, $5 \nmid 1978^m$ e consequentemente $125 \nmid 1978^m$. Segue que, para satisfazer (9), deve-se ter:

$$\begin{gathered} 125 \mid \left(1978^{n-m} - 1\right), \\ 1978^{n-m} \equiv 1 \mod 125. \end{gathered} \tag{12}$$

Em outras palavras, de (12) deve-se ter que o resto na divisão por 125 de 1978^{n-m} é 1, ou deve existir $q \in \mathbb{N}$ tal que:

$$1978^{n-m} = 125q + 1 = 5\,(25q) + 1.$$

Isso implica que dividir 1978^{n-m} por 5 deve deixar resto 1 também. Mas, de (11), a única possibilidade para que uma potência de 1978 deixe resto 1 na divisão por 5 é que esta seja múltiplo de 4. Em símbolos, deve existir $k \in \mathbb{N}$ tal que:

$$n - m = 4k. \tag{13}$$

Substituindo (13) em (12) procura-se encontrar o menor valor de k tal que:

$$1978^{4k} \equiv 1 \mod 125. \tag{14}$$

Ainda:

$$1978 \equiv 103 \equiv -22 \mod 125,$$

$$1978^4 \equiv (-22)^4 = 484^2 \equiv 109^2 \equiv (-16)^2 = 256 \equiv 6 \mod 125. \tag{15}$$

Isto é, de (14) e (15), tem-se:

$$1978^{4k} = \left(1978^4\right)^k \equiv 6^k \equiv 1 \mod 125, \tag{16}$$

$$6^k \equiv 1 \mod 125. \tag{17}$$

Em outras palavras, o problema foi reduzido a buscar o menor valor de k tal que uma potência de 6 deixe resto 1 na divisão por 125.

Utilizando o Binômio de Newton pode-se escrever:

$$6^k = (1+5)^k = \sum_{i=0}^{k} \binom{k}{i} 1^{k-i} 5^i = 1 + 5k + 25\binom{k}{2} + 125\binom{k}{3} + \ldots + 5^k. \tag{18}$$

Os casos $k = 1$ e $k = 2$ são trivialmente descartados de satisfazer (16). Para $k > 2$ a partir da quarta parcela na direita da equação (18) todos eles são múltiplos de 125. Segue que:

$$6^k \equiv 1 + 5k + 25\binom{k}{2} = 1 + 5k + 25\frac{k\,(k-1)}{2} \mod 125. \tag{19}$$

De (17) e (19) encontra-se:

$$0 \equiv 5k + 25\frac{k\,(k-1)}{2} \mod 125,$$

$$\frac{25k^2 - 15k}{2} = \frac{5k\,(5k-3)}{2} \equiv 0 \mod 125.$$

Como 2 e 125 são coprimos a congruência anterior é equivalente a:

$$5k\,(5k-3) \equiv 0 \mod 125. \tag{20}$$

Tem-se que 5 (e consequentemente 125) não divide $5k-3$. Segue que $125 \mid 5k$, $25 \mid k$, $100 \mid 4k$ e logo, de (13), $100 \mid n-m$. Com $m \geq 3$, encontrado partindo de (8), é concluído que o par ordenado (m, n) para o qual $m+n$ é mínimo é $(3, 103)$.

Utilizando um computador ou site, como https://www.wolframalpha.com, pode ser verificado que os números 1978^3 e 1978^{103} terminam com os dígitos 352.

3.5 Quadrados perfeitos módulo 3. IMO 2017 P1.

Problema 5. *Para cada inteiro $a_0 > 1$, define-se a sequência $a_0, a_1, a_2, \ldots$ tal que, para cada $n \geq 0$ vale:*

$$a_{n+1} = \begin{cases} \sqrt{a_n}, & \text{se } \sqrt{a_n} \text{ é inteiro,} \\ a_n + 3, & \text{caso contrário.} \end{cases}$$

Determine todos os valores de a_0 para os quais existe um número A tal que $a_n = A$ para infinitos valores de n.

A IMO 2017 foi realizada na Cidade do Rio de Janeiro, Brasil. Problema proposto por Stephan Wagner, África do Sul (THE PROBLEM...,, 2017).

3.5.1 Resolução do Problema 5

Convém observar que os primeiros termos da sequência para alguns valores de a_0:

$$(2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 37, 40, 43, \ldots),$$

$$(3, 6, 9, 3, 6, 9, 3, 6, 9, 3, 6, 9, 3, 6, \ldots),$$

$$(4, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 37, 40, 43, \ldots),$$

$$(5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 37, 40, 43, \ldots),$$

$$(6, 9, 3, 6, 9, 3, 6, 9, 3, 6, 9, 3, 6, \ldots),$$

$$(7, 10, 13, 16, 4, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 37, 40, 43, \ldots).$$

Quando $a_0 = 2$ e $a_0 = 5$ as sequências parecem ser crescentes, o que significaria que não existe um número A tal que $a_n = A$ para infinitos valores de n.

Quando $a_0 = 3$ e $a_0 = 6$ as sequências parecem ser periódicas, a configuração 3, 6, 9 repete. Neste caso pode-se tomar, por exemplo, $A = 3$ para satisfazer as condições do problema.

E quando $a_0 = 4$ e $a_0 = 7$ as sequências crescem até um quadrado perfeito, decrescem até 2 para depois crescer o tempo todo, o qual novamente significaria que não existe um número A tal que $a_n = A$ para infinitos valores de n.

Esses exemplos sugerem que devem-se separar os estudos em três casos, dependendo do resto deixado por a_0 na divisão por 3. Isto é:

i) $a_0 \equiv 0 \mod 3$ ou $a_0 = 3k$ com $k \in \mathbb{N}$,

ii) $a_0 \equiv 1 \mod 3$ ou $a_0 = 3k + 1$ com $k \in \mathbb{N}$,

iii) $a_0 \equiv 2 \mod 3$ ou $a_0 = 3k + 2$ com $k \in \mathbb{N}$.

O caso iii) é o mais simples de analisar. Dado que nenhum quadrado perfeito deixa resto 2 na divisão por 3 (Proposição 28), se $a_0 \equiv 2 \mod 3$, então $\sqrt{a_0}$ não é inteiro, $a_1 = a_0 + 3$ e $a_1 \equiv 2 \mod 3$. Pelo Corolário 16, $\forall n \in \mathbb{N}$ ter-se-á $a_n \equiv 2 \mod 3$. Portanto, $\sqrt{a_n}$ não é inteiro, $a_{n+1} = a_n + 3$ e $a_{n+1} \equiv 2 \mod 3$. Isto é, a sequência é crescente. Logo, não existe um número A tal que $a_n = A$ para infinitos valores de n.

Para os casos i) e ii) estudam-se as desigualdades:

$$b < b + 3 < b^2 < a_0 \leq (b + 3)^2. \tag{21}$$

Foca-se primeiro a desigualdade $b + 3 < b^2$ ou:

$$b^2 - b = b(b - 1) > 3. \tag{22}$$

A qual é verdadeira

$$\forall b \geq 3, b \in \mathbb{N}. \tag{23}$$

Pela definição, os termos da sequência a_n crescerão de três em três até encontrar um quadrado perfeito. Suponha-se que o quadrado perfeito mais próximo, e maior que a_0, seja $(b + 3)^2$, como em (21). Isto é, para um certo índice k ter-se-á $a_k = (b + 3)^2$ e o termo de ordem $k + 1$ será $a_{k+1} = b + 3$. Enquanto a desigualdade (22) for verdadeira os termos da sequência aumentarão até o próximo quadrado perfeito. Em outras palavras, para um certo $m \in \mathbb{N}$ ter-se-á $a_{k+1+m} = b^2$, e $a_{k+1+m+1} = b$. Logo, o processo se repete até a desigualdade (22) não ser mais verdadeira. Segue que o valor mínimo da sequência será menor ou igual a 3.

Agora foca-se no caso i) $a_0 \equiv 0 \mod 3$. Suponha-se que o quadrado perfeito mais próximo por cima de a_0 seja $(3l+3)^2$ com $l \in \mathbb{N}$:

$$3l < 3l+3 < (3l)^2 < a_0 \leq (3l+3)^2. \tag{24}$$

Isto é, para um certo índice k ter-se-á $a_k = (3l+3)^2$ e o termo de ordem $k+1$ será $a_{k+1} = 3l+3$. Trocando b por $3l$ em (23) encontra-se que, enquanto $3l \geq 3$ ou $l \geq 1$ for verdadeira, os termos da sequência aumentarão até o próximo quadrado perfeito e a seguir decrescerão.

Lembra-se também que se $a_k \equiv 0 \mod 3$, então $a_{k+1} = \sqrt{a_k} \equiv 0 \mod 3$ (Proposição 28). Segue que todos os termos da sequência serão múltiplos de 3 e o menor deles será 3 para $l = 1$. A partir de certo índice a configuração 3, 6, 9 repetirá infinitamente. Tomando $A \in \{3, 6, 9\}$ serão satisfeitas as condições do problema. Um exemplo é:

$$(27, 30, 33, 36, 6, 9, 3, 6, 9, 3, \ldots).$$

No caso ii) $a_0 \equiv 1 \mod 3$ ter-se-á duas possibilidades.

ii-1) Suponha-se que o quadrado perfeito mais próximo, e maior que a_0, seja para um certo índice k da forma $a_k = (3l+2)^2$. O termo de ordem $k+1$ será $a_{k+1} = 3l+2$ com $l \in \mathbb{N}$. Neste ponto o problema se reduz ao caso iii) visto anteriormente. A sequência crescerá ilimitadamente e não existirá um número A tal que $a_n = A$ para infinitos valores de n. Para este subcaso o valor mínimo da sequência deixa resto 2 na divisão por 3, mas não é 2. Um exemplo é:

$$(19, 22, 25, 5, 8, 11, 14, 17, \ldots).$$

ii-2) Suponha-se que o quadrado perfeito mais próximo, e maior que a_0, seja para um certo índice k da forma $a_k = (3l+1)^2$. O termo de ordem $k+1$ será $a_{k+1} = 3l+1$ com $l \in \mathbb{N}$. Neste subcaso enquanto $3l+1 > 3$ ou $l > 1$ for verdadeira os termos da sequência aumentarão até o próximo quadrado perfeito e a seguir decrescerão.

Se a raiz quadrada do próximo quadrado perfeito deixar resto 2 na divisão por 3, segue o caso iii). Um exemplo é:

$$(58, 61, 64, 8, 4, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 37, 40, 43, \ldots).$$

Se a raiz quadrada deixar resto 1 na divisão por 3 o processo será repetido. Porém, mesmo no caso em que todos os termos da sequência são congruentes a $1 \mod 3$, quando $l = 1$ para um certo índice h ter-se-á $a_h = 4$ e $a_{h+1} = 2$. A partir deste ponto retorna-se ao caso iii). A sequência crescerá ilimitadamente e não existirá um número A tal que $a_n = A$ para infinitos valores de n. Para este último subcaso o valor mínimo da sequência é 2. Um exemplo é:

$$(28, 31, 34, 37, 40, 43, 46, 49, 7, 10, 13, 16, 4, 2, 5, 8, \ldots).$$

A Figura 1 mostra o gráfico dos vinte primeiros elementos da sequência a_n quando $a_0 = 43$.

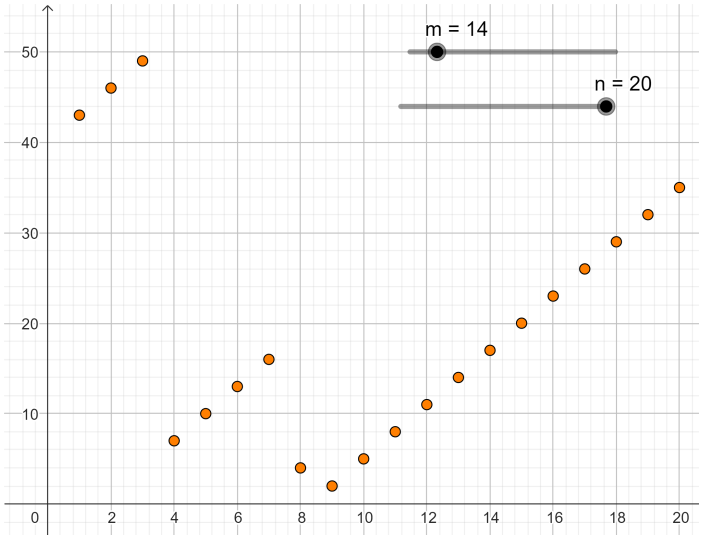

Figura 1: Gráfico da sequência a_n até $n = 20$. Com $m = 14$, caso $a_0 = 3m + 1 = 43 \equiv 1 \mod 3$.

Resumindo, somente existirá solução para o problema apresentado quando $a_0 \equiv 0 \mod 3$, onde $A \in \{3, 6, 9\}$.

4 Conclusões

Neste artigo foram discutidos detalhadamente cinco problemas propostos para a Olimpíada Internacional de Matemática. Os mesmos enfatizam o poder das congruências numéricas para lidar com números grandes e encontrar padrões e regularidades. O assunto é usualmente omitido nos programas de Ensino Médio no Brasil. Porém, ele entra no programa olímpico em nível nacional e internacional.

O Problema 1 (P1 da IMO de 1964, Moscou) solicitou encontrar os valores naturais de n tais que os número $2^n - 1$ e $2^n + 1$ fossem divisíveis por 7. O estudo das congruências módulo 3 e 7 resolveu o desafio.

No Problema 2 (P38 da LL da IMO de 1967, na antiga Iugoslávia) foi pedido para encontrar inteiros que resolvessem uma equação diofantina não linear. Analisando a congruência módulo 3 provou-se que tal solução não existe.

O Problema 3 (P4 da IMO de 1975, na Bulgária) utilizou a congruência módulo nove para estudar uma sequência $\left(16^{16}, A, B, C\right)$, cada número é encontrado pela soma dos dígitos do anterior.

No Problema 4 (P1 da IMO de 1978, na Romênia) pede-se para encontrar dois números naturais tais que os grupos dos três últimos dígitos nas representações decimais de 1978^m e 1978^n coincidam e a soma $m + n$ seja mínima. Foram usadas congruências módulo 2, 5, 8, 125 e 1000, assim como a fórmula do binômio de Newton.

O Problema 5 (P1 da IMO de 2017, no Brasil) solicitou escolher o valor inicial de uma sequência, definida de forma recorrente, de tal forma que exista algum número que repete-se infinitamente. A solução do mesmo levou ao estudo de congruências módulo 3 e de quadrados perfeitos.

5 Bibliografia

DJUKIC, D. *et al.* **The IMO compendium:** a collection of problems suggested for the International Mathematical Olympiads: 1959–2009. 2nd ed. New York: Springer, 2011.

GAUSS, C. F. **Disquisitiones arithmeticae.** Tradução de Arthur A. Clarke. New Haven: Yale University Press, 1965.

HEFEZ, A. **Aritmética.** 2. ed. Rio de Janeiro: SBM, 2016. (Coleção ProfMat, 8).

THE PROBLEM SELECTION COMMITTEE OF IMO 2017. **Shortlisted problems (with solutions).** Rio de Janeiro: [s. n.], 2017. Disponível em: http://www.imo-official.org/problems/IMO2017SL.pdf. Acesso em: 28 fev. 2023.