PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.11, n.2, 2023
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2023/pmo1113

Olimpíadas de Matemática: Aritmética e resoluções de problemas

Manoel Rodrigues de A. Neto   Wállace M. de Sousa

Resumo

Desde a antiguidade, a Matemática sempre foi desafiadora, e muitas pessoas resolviam problemas matemáticos por prazer e diversão. Com o surgimento das olimpíadas de matemática, esses desafios transformaram-se em grandes competições que se espalharam por todo o mundo, sendo aprimoradas com o passar do tempo, e tal prazer e interesse pelas olimpíadas faz com que continuem surgindo novas competições até os dias atuais. Este trabalho aborda alguns conceitos relacionados à Aritmética e questões acerca dos conteúdos mencionados selecionadas de algumas olimpíadas de nível universitário, com suas devidas soluções, criando assim um material de apoio para quem deseja participar destas competições.

Palavras-chave: olimpíadas de matemática; aritmética; resolução de problemas.

Abstract

Since ancient times, Mathematics has always been challenging, and many people solve mathematical problems for pleasure and fun. With the advent of the mathematical olympiads, these challenges turned into great competitions that spread throughout the world, being improved over time, and that pleasure and interest for the olympiads makes it possible that new competitions continue to emerge until the present day. This work addresses some concepts related to Arithmetic and questions about the mentioned contents selected from some academical level olympiads, with their appropriate solutions, thus creating a support material for those who want to participate in these competitions.

Keywords: mathematical olympiads; arithmetic; problem solving.

1. Introdução

As competições matemáticas acontecem desde o século XVI, quando eram realizados desafios entre os matemáticos da época, com apostas de dinheiro, reputação e cátedras em universidades. Muitos deles dedicavam-se bastante para ter algum prestígio ou reconhecimento da sociedade [4].

Já no final do século XIX, no ano de 1894, surgiu a primeira competição com características das olimpíadas de Matemática que temos atualmente. Essas competições aconteceram na Hungria e eram chamadas de *Eotvos*, que era o sobrenome do presidente da Hungria naquele ano. Com o passar dos anos, competições similares foram se espalhando pelo leste europeu, e, em 1934, surgiu

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

a primeira olimpíada de matemática, que pode ser classificada como "moderna", na cidade de Leningrado, na extinta União Soviética, onde hoje a cidade tem o nome de São Petersburgo [1].

Todas essas competições ao longo dos anos, culminaram com a organização da primeira Olimpíada Internacional de Matemática (IMO), realizada na cidade de Bucareste na Romênia, no ano de 1959. A IMO é a olimpíada de Matemática mais antiga que ocorre atualmente, com participação de mais de 100 países do mundo todo.

A primeira olimpíada de matemática que surgiu no Brasil foi realizada no Estado de São Paulo em 1977. Estamos falando da Olimpíada Paulista de Matemática, que foi criada pela Academia Paulista de Ciência [1].

Este trabalho tem como principal objetivo criar um material de estudo e incentivo à participação de estudantes nas diversas Olimpíadas de Matemática Universitária, podendo ser aproveitado também para os alunos que estejam concluindo o ensino básico, possibilitando o aumento do acesso a esses conhecimentos e competições.

2. Tópicos de aritmética

Nesta seção, iremos abordar a aritmética dos restos com foco nos seguintes teoremas: Teorema de Euler, Teorema de Wilson e Pequeno Teorema de Fermat. Além disso, discutimos um resultado interessante acerca dos números de Fibonacci, a saber: existe uma regularidade quanto à repetição de seus últimos dígitos. Esses conceitos serão utilizados na resolução de problemas da seção seguinte. Esperamos que o leitor já tenha conhecimento de outros conteúdos de aritmética que também serão utilizados nessas soluções, como, por exemplo: Princípio de Indução Matemática, binômio de Newton, divisibilidade e números primos.

2.1. Aritmética dos Restos

Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b \mod m$. Se a relação $a \equiv b \mod m$ não for verdadeira, então diremos que a e b não são congruentes módulo m, e a notação usada para este caso é $a \not\equiv b \mod m$.

Por exemplo, $37 \equiv 12 \mod 5$, pois os restos da divisão de 37 e de 12 por 5 são iguais a 2. Por outro lado, $37 \not\equiv 11 \mod 12$, pois o resto da divisão de 37 por 12 é 1 e de 11 por 12 é 11.

Proposição 1. *Suponha que* $a, b, m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que* $a \equiv b \mod m$ *se, e somente se,* $m \mid (b - a)$.

Demonstração. Suponhamos que $a \equiv b \mod m$. Pelo algoritmo da divisão Euclidiana existem inteiros q_1, q_2 e r, tais que

$$a = m \cdot q_1 + r \quad \text{e} \quad b = m \cdot q_2 + r \text{ , onde } 0 \leqslant r < m.$$

Daí, temos que

$$\begin{aligned} b - a &= m \cdot q_2 + r - m \cdot q_1 - r \\ &= m(q_2 - q_1). \end{aligned}$$

Logo, $m \mid (b - a)$.

Reciprocamente, suponhamos que $m \mid (b-a)$. Neste caso, existe $q_1 \in \mathbb{Z}$ tal que $b-a = m \cdot q_1$. Portanto, $b = m \cdot q_1 + a$. Por outro lado, sejam q_2 e r o quociente e o resto da divisão de a por m, respectivamente. Assim, $a = m \cdot q_2 + r$, com $q_2, r \in \mathbb{Z}$ e $0 \leqslant r < m$. Disso, segue que

$$\begin{aligned} b &= m \cdot q_1 + a \\ &= m \cdot q_1 + m \cdot q_2 + r \\ &= m(q_1 + q_2) + r, \end{aligned}$$

ou seja,

$$b = m(q_1 + q_2) + r, \text{ onde } 0 \leqslant r < m.$$

Pela unicidade na divisão euclidiana, podemos concluir que r é também o resto da divisão de b por m. Assim, temos que $a \equiv b \mod m$. □

Proposição 2. *Seja* $m \in \mathbb{N}$. *Para quaisquer* $a, b, c \in \mathbb{Z}$, *temos:*

(i) $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, *então* $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

Demonstração. *(i)* Note que se $m \mid 0$, então $m \mid (a-a)$ e, consequentemente, $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, então que $m \mid a-b$. Assim, $a - b = mq$ para algum número inteiro q. Multiplicando por -1 essa igualdade, obtemos $b - a = m(-q)$, que significa que $m \mid b-a$. Portanto, $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $m \mid (b-a)$ e $m \mid (c-b)$. Agora, temos que $m \mid [(b-a)+(c-b)]$, ou seja, $m \mid c-a$. Logo, $a \equiv c \mod m$. □

Proposição 3. *Sejam* $a, b, c, d, m, r \in \mathbb{Z}$, *com* $m > 1$.

(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* $ac \equiv bd \mod m$.

(iii) Se $ar \equiv br \mod m$ *e* $\mathrm{mdc}(r, m) = 1$, *então* $a \equiv b \mod m$.

Demonstração. *(i)* Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $m \mid (b-a)$ e $m \mid (d-c)$. Daí, temos que $m \mid [(b-a)+(d-c)]$, ou seja, $m \mid [(b+d)-(a+c)]$. E assim, $a + c \equiv b + d \mod m$.

(ii) Analogamente ao item *(i)*, m divide qualquer combinação linear entre $b-a$ e $d-c$. Então temos que $m \mid [d(b-a)+a(d-c)]$, mas $d(b-a)+a(d-c) = bd - ad + ad - ac = bd - ac$. Assim, $m \mid (bd - ac)$, mostrando que $ac \equiv bd \mod m$.

(iii) Se $ar \equiv br \mod m$, então $m \mid (br - ar)$, ou seja, $m \mid r(b-a)$. Como $\mathrm{mdc}(r, m) = 1$, segue que $m \mid (b-a)$. Logo, $b \equiv a \mod m$. □

Corolário 1. *Para todos* $n \in \mathbb{N}, a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$, *se* $a \equiv b \mod m$, *então tem-se que* $a^n \equiv b^n \mod m$.

Demonstração. Vamos demonstrar este corolário usando o Princípio de Indução Matemática. Considere a seguinte sentença aberta

$$p(n): \ a \equiv b \mod m \implies a^n \equiv b^n \mod m.$$

Para $n = 0$, temos

$$a^0 - b^0 = 1 - 1 = 0 = 0 \cdot m \Longrightarrow m \mid (a^0 - b^0) \Longrightarrow a^0 \equiv b^0 \mod m.$$

Então, a sentença aberta $p(n)$ é válida para $n = 0$. Agora, suponhamos que $p(n)$ vale para algum $n \in \mathbb{N}$, ou seja,

$$\text{Hipótese de indução: } a \equiv b \mod m \implies a^n \equiv b^n \mod m.$$

Vamos mostrar que $p(n+1)$ também vale, ou seja,

$$\text{Tese: } a \equiv b \mod m \implies a^{n+1} \equiv b^{n+1} \mod m.$$

Como $a \equiv b \mod m$ e, por hipótese de indução, $a^n \equiv b^n \mod m$, pela Proposição 3, temos que

$$a \cdot a^n \equiv b \cdot b^n \mod m \Longrightarrow a^{n+1} \equiv b^{n+1} \mod m,$$

como queríamos demonstrar. Logo, pelo Princípio de Indução Matemática, a sentença $p(n)$ é válida para todo $n \in \mathbb{N}$. □

Exemplo 1. Encontre o resto da divisão de 7^{10} por 51.

Solução: Note que

$$7^2 = 49 \equiv -2 \mod 51$$

Elevando ambos os membros a 5,

$$(7^2)^5 \equiv (-2)^5 \mod 51 \Longrightarrow 7^{10} \equiv -32 \mod 51.$$

Mas como $-32 = -51 + 19$,

$$7^{10} \equiv -51 + 19 \mod 51 \Longrightarrow 7^{10} \equiv 19 \mod 51.$$

Logo, o resto da divisão de 7^{10} por 51 é igual a 19.

Exemplo 2. Prove que $11 \mid (2^{1000} - 1)$.

Solução: Pela Proposição 1, basta provar que $2^{1000} \equiv 1 \mod 11$. Agora, observemos que

$$2^5 = 32 \equiv -1 \mod 11.$$

Elevando ambos os membros a 200, obtemos

$$(2^5)^{200} \equiv (-1)^{200} \mod 11 \Longrightarrow 2^{1000} \equiv 1 \mod 11.$$

E isto é suficiente para concluirmos que $11 \mid 2^{1000} - 1$.

2.2. Números de Fibonacci

Leonardo de Pisa, conhecido como Leonardo Fibonacci, nasceu na Itália por volta de 1175. Em sua obra intitulada *Liber Abacci*, ou livro do ábaco, está presente o problema dos coelhos, o qual daria origem a uma das sequências mais famosas da humanidade, conhecida como sequência de Fibonacci [2].

Cada termo da sequência de Fibonacci é definido, a partir do terceiro termo, como sendo a soma dos dois termos anteriores, com os dois primeiros termos iguais a 1. Assim, os primeiros números desta sequência são:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$$

Definição 1. A sequência de Fibonacci (F_n) é definida por $F_{n+2} = F_{n+1} + F_n$, para $n \geqslant 1$, onde $F_1 = 1$ e $F_2 = 1$.

Dentre as várias propriedades que tal sequência possui, temos a periodicidade. Os números de Fibonacci apresentam uma regularidade quanto à repetição de seus últimos dígitos. O dígito das unidades repete-se com uma periodicidade de 60, ou seja, a sequência formada pelos algarismos das unidades do números de Fibonacci repete-se a cada 60 números. Essa curiosidade foi descoberta em 1774 pelo matemático franco-italiano Joseph Louis Lagrange [7].

Por exemplo, os números $F_7 = 13$, $F_{67} = 44945570212853$ e $F_{127} = 155576970220531065681649693$ exemplificam a periodicidade dos dígitos das unidades desta sequência.

Proposição 4. $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ *para* m *e* n *naturais.*

A demonstração da Proposição 4 pode ser encontrada em [2], na página 25.

Proposição 5. $F_{n+60} \equiv F_n \mod 10$ *para todo* n *inteiro positivo.*

Demonstração. Faremos a demonstração usando o Princípio de Indução Matemática. Considere a seguinte sentença aberta

$$p(n): \ F_{n+60} \equiv F_n \mod 10.$$

Primeiramente, observe que $F_{61} \equiv F_1 \mod 10$, pois $F_{61} - F_1 = 2504730781961 - 1$. Logo, $p(1)$ é verdadeira. Agora, vamos supor que $p(n)$ seja verdadeira para algum $n \in \mathbb{N}$, ou seja,

$$\text{Hipótese de indução} \ : \ F_{n+60} \equiv F_n \mod 10.$$

Vamos mostrar que $p(n+1)$ também é verdadeira, ou seja,

$$\text{Tese} \ : \ F_{n+61} \equiv F_{n+1} \mod 10.$$

Por hipótese de indução, temos que $F_{n+60} \equiv F_n \mod 10$. Somando F_{n+59} à congruência anterior, temos $F_{n+59} + F_{n+60} \equiv F_n + F_{n+59} \mod 10$.

Mas, por definição,

$$F_{n+59} + F_{n+60} = F_{n+61}$$

e, usando a Proposição 4 em F_{n+59}, obtemos

$$F_{n+59} = F_n F_{60} + F_{n-1} F_{59}$$

Assim,

$$F_{n+61} \equiv F_n + F_n F_{60} + F_{n-1} F_{59} \mod 10.$$

Note que $F_{59} \equiv 1 \mod 10$ e $F_{60} \equiv 0 \mod 10$, pois $F_{59} = 956722026041$ e $F_{60} = 1548008755920$. Então,

$$F_{n+61} \equiv F_n + F_n \cdot 0 + F_{n-1} \cdot 1 \equiv F_n + F_{n-1} \mod 10$$

e, finalmente, usando a definição da sequência de Fibonacci, $F_{n+61} \equiv F_{n+1} \mod 10$. Logo, pelo Princípio de Indução Matemática, $F_{n+60} \equiv F_n \mod 10$ para todo n inteiro positivo. □

2.3. Teorema de Euler

Proposição 6. *Sejam* $a, m \in \mathbb{Z}$, *com* $m > 1$. *A congruência* $aX \equiv 1 \mod m$ *possui solução se, e somente se,* $\mathrm{mdc}(a, m) = 1$. *Além disso, se* $x_0 \in \mathbb{Z}$ *é uma solução, então* x *é uma solução da congruência se, e somente se,* $x \equiv x_0 \mod m$.

A demonstração da Proposição 6 encontra-se em [3], na página 194.

Um *sistema reduzido* de resíduos módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que

a) $\mathrm{mdc}(r_i, m) = 1$, para todo $i = 1, \ldots, s$;

b) $r_i \not\equiv r_j \mod m$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $\mathrm{mdc}(n, m) = 1$, existe i tal que $n \equiv r_i \mod m$.

Proposição 7. *Seja* $r_1, \cdots, r_{\varphi(m)}$ *um sistema reduzido de resíduos módulo* m *e seja* $a \in \mathbb{Z}$ *tal que* $\mathrm{mdc}(a, m) = 1$. *Então,* $ar_1, \cdots, ar_{\varphi(m)}$ *é um sistema reduzido de resíduos módulo* m.

A demonstração da Proposição 7 pode ser encontrada em [3], na página 197.

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma importante função $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, chamada função 'fi de Euler'.

Exemplo 3.
- $\varphi(9) = 6$, pois de 1 até 8 temos seis números que são primos com 9, ou seja o mdc entre 9 e cada um deles é igual a 1. São eles $\{1, 2, 4, 5, 7, 8\}$.
- $\varphi(13) = 12$, pois de 1 até 12 todos os números são primos com 13, e isso se dá justamente por 13 ser um número primo.

Observação 1. Pela definição, temos que $\varphi(m) \leqslant m-1$, para todo $m \geqslant 2$. Além disso, $\varphi(m) = m-1$ se, e somente se, m é um número primo. De fato, m é primo se, e somente se, $1, 2, \cdots, m-1$ são coprimos com m, o que é equivalente a dizer que $\varphi(m) = m - 1$.

Teorema 1 (Euler)**.** *Sejam* $m, a \in \mathbb{Z}$ *com* $m > 1$ *e* $\mathrm{mdc}(a, m) = 1$. *Então,*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Demonstração. Seja $r_1, \cdots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição 7, $ar_1, \cdots, ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m e, portanto,

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \mod m$$

pela definição de sistema reduzido de resíduos. Consequentemente,

$$a^{\varphi(m)} r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \mod m,$$

ou seja,

$$a^{\varphi(m)} (r_1 \cdot r_2 \cdots r_{\varphi(m)}) \equiv (r_1 \cdot r_2 \cdots r_{\varphi(m)}) \mod m.$$

Como $\mathrm{mdc}(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$, segue que

$$a^{\varphi(m)} \equiv 1 \mod m$$

pelo item (iii) da Proposição 3. □

Exemplo 4. Determine o resto da divisão de 4^{50} por 9.

Solução: Como o $\mathrm{mdc}(4, 9) = 1$, pelo Teorema 1,

$$4^{\varphi(9)} \equiv 1 \mod 9.$$

Mas $\varphi(9) = 6$, então

$$4^6 \equiv 1 \mod 9 \Longrightarrow 4^{48} \equiv 1^8 \mod 9.$$

Multiplicando ambos os membros por 4^2,

$$4^{50} \equiv 16 \mod 9 \Longrightarrow 4^{50} \equiv 7 \mod 9.$$

Portanto, 7 é o resto da divisão de 4^{50} por 9.

Proposição 8. *Sejam* $m, m' \in \mathbb{N}$ *tais que* $\mathrm{mdc}(m, m') = 1$*. Então*

$$\varphi(mm') = \varphi(m)\varphi(m').$$

Demonstração da Proposição 8 na referência [3], página 199.

Proposição 9. *Se* p *é um número primo e* r*, um número natural, então tem-se que*

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

Demonstração. De 1 até p^r, temos p^r números naturais. Temos que excluir, desses, os números que não são primos com p^r, ou seja, todos os múltiplos de p, que são precisamente $p, 2p, \ldots, p^{r-1}p$, cujo número é p^{r-1}. Portanto, $\varphi(p^r) = p^r - p^{r-1}$, provando o resultado. □

Teorema 2. *Seja* $m > 1$ *e seja* $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *a decomposição de* m *em fatores primos. Então,*

$$\varphi(m) = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$

Demonstração. O resultado decorre imediatamente das Proposições 8, 9. □

2.4. Pequeno Teorema de Fermat e Teorema de Wilson

Lema 1. *Sejam* $a \in \mathbb{Z}$ *e* p *um número primo tais que* $\mathrm{mdc}(a, p) = 1$. *Tem-se que*

$$a^{p-1} \equiv 1 \mod p.$$

Demonstração. Como $a, p \in \mathbb{Z}$ e o $\mathrm{mdc}(a, p) = 1$, pelo Teorema 1

$$a^{\varphi(p)} \equiv 1 \mod p.$$

Mas p é um número primo, então $\varphi(p) = p - 1$. Daí, $a^{p-1} \equiv 1 \mod p$, como gostaríamos. □

Teorema 3 (Pequeno Teorema de Fermat)**.** *Dado um número primo* p *e qualquer* $a \in \mathbb{Z}$, *tem-se que*

$$a^p \equiv a \mod p$$

Demonstração. Se $\mathrm{mdc}(a, p) = 1$, então o resultado segue do Lema 1, multiplicando por a ambos os membros da congruência $a^{p-1} \equiv 1 \mod p$. No caso em que $\mathrm{mdc}(a, p) \neq 1$, segue-se que $p \mid a$, e, consequentemente, $p \mid (a^p - a)$, o que ainda garante que $a^p \equiv a \mod p$. □

Exemplo 5. Determine o resto da divisão de 13^{111} por 11.

Solução: Como 11 é um número primo e o $\mathrm{mdc}(13, 11) = 1$, pelo Lema 1

$$13^{10} \equiv 1 \mod 11.$$

Elevando ambos os membros a 11, temos

$$13^{110} \equiv 1^{11} \mod 11.$$

Por fim, multiplicando ambos os membros por 13,

$$13^{111} \equiv 13 \mod 11 \Longrightarrow 13^{111} \equiv 2 \mod 11.$$

Logo, o resto da divisão de 13^{111} por 11 é 2.

Teorema 4 (Teorema de Wilson)**.** *Se* p *é um número primo, então*

$$(p - 1)! \equiv -1 \mod p.$$

Demonstração. Note que para $p = 2$ e $p = 3$ o teorema é válido. Suponhamos então $p \geqslant 5$ primo. Para todo $i \in 1, \ldots, p-1$, pela Proposição 6, a congruência $iX \equiv 1 \mod p$ possui uma única solução módulo p; ou seja, dado $i \in 1, \ldots, p-1$ existe um único $j \in 1, \ldots, p-1$ tal que $ij \equiv 1 \mod p$. Por outro lado, se $i \in 1, \ldots, p-1$ é tal que $i^2 \equiv 1 \mod p$, então $p \mid i^2 - 1$, o que equivale a $p \mid i - 1$ ou $p \mid i + 1$, o que só pode ocorrer se $i = 1$ ou $i = p - 1$. Logo,

$$2 \cdots (p-2) \equiv 1 \mod p,$$

e, portanto,

$$\begin{aligned} 1 \cdot 2 \cdots (p-2)(p-1) &\equiv p - 1 \mod p \\ &\equiv -1 \mod p. \end{aligned}$$

Ou seja,

$$(p - 1)! \equiv -1 \mod p,$$

como gostaríamos. □

Exemplo 6. Qual o resto da divisão de $\dfrac{13!}{7}$ por 7?

Solução: Temos que

$$\begin{aligned}\frac{13!}{7} &= \frac{13\cdot 12\cdot 11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{7}\\ &= 13\cdot 12\cdot 11\cdot 10\cdot 9\cdot 8\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1.\end{aligned}$$

Por outro lado,

$$\begin{aligned}(13\cdot 12\cdot 11\cdot 10\cdot 9\cdot 8)(6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1) &\equiv (6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1)(6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1) \mod 7\\ &\equiv 6!\cdot 6! \mod 7\end{aligned}$$

Pelo Teorema de Wilson,

$$\frac{13!}{7} \equiv (-1)\cdot(-1) \mod 7 \Longrightarrow \frac{13!}{7} \equiv 1 \mod 7$$

Então, o resto da divisão de $\dfrac{13!}{7}$ por 7 é 1.

3. Alguns Problemas de Olimpíadas de Matemática Universitária

Aqui são apresentadas resoluções de questões, ligadas à aritmética, de algumas olimpíadas de matemática universitária. Foram selecionadas as questões mais recentes, sendo todas de 2017 até os dias atuais, apresentadas em ordem cronológica, e, também, exclusivamente questões que disponibilizavam apenas o gabarito mas sem nenhuma solução.

1) (GN 2017 - 1ª fase - Q 07) Quantos valores inteiros de x no intervalo $[1, 100]$ fazem com que o determinante da seguinte matriz seja múltiplo de 3?

$$\begin{pmatrix} x^2 & 1 & 7\\ 2 & 3 & 4\\ 7 & 5 & (x+2)\end{pmatrix}$$

(a) 0 **(b)** 34 **(c)** 67 **(d)** 100

Solução: Vamos definir a matriz em questão por M_x e, inicialmente, iremos calcular o determinante dessa matriz em função de x. Pela regra de Sarrus temos que:

$$\begin{aligned}\det M_x &= (3x^3+6x^2)+28+70-147-20x^2-(2x+4)\\ &= 3x^3-14x^2-2x-53.\end{aligned}$$

Assim,

$$\det M_x \equiv x^2+x+1 \mod 3.$$

Agora vamos determinar para quais valores x a expressão x^2+x+1 será múltiplo de 3, ou seja, será congruente a 0 módulo 3. Notemos que:

- se $x \equiv 0 \mod 3$, então $x^2+x+1 \equiv 1 \mod 3$;
- se $x \equiv 1 \mod 3$, então $x^2+x+1 \equiv 0 \mod 3$;

• se $x \equiv 2 \mod 3$, então $x^2 + x + 1 \equiv 1 \mod 3$.

Portanto, os únicos valores de $x \in [1, 100]$ tais que $\det M_x \equiv 0 \mod 3$ são aqueles que satisfazem $x_n = 1 + 3n$, para algum $n \in \mathbb{Z}_{\geq 0}$. Agora, basta notar que $x_n \in [1, 100]$ se, e somente se, $n \in \{0, 1, 2, ..., 33\}$. Concluímos que existem 34 valores inteiros de x no intervalo $[1, 100]$ tais que $\det M_x \equiv 0 \mod 3$. A resposta correta é o item (b).

2) (GN 2017 - 1ª fase - Q 10) Para cada par de números inteiros m, n denotemos por $\mathrm{mdc}(m, n)$ o máximo divisor comum de m e n. Se $n \geq 2$, qual é o valor de $\sum_{j=1}^{n-1} \left\lfloor \frac{1}{\mathrm{mdc}(n, j)} \right\rfloor$?

(a) 1 **(b)** $\phi(n)$ **(c)** n **(d)** $\frac{n}{\phi(n)}$

Solução: Se n e j forem primos entre si, então $\mathrm{mdc}(n, j) = 1$ e isto implica $\left\lfloor \frac{1}{\mathrm{mdc}(n, j)} \right\rfloor = 1$. Por outro lado, se n e j tiverem fatores em comum em sua decomposição, então $\mathrm{mdc}(n, j) \geqslant 1$, o que implica $\left\lfloor \frac{1}{\mathrm{mdc}(n, j)} \right\rfloor = 0$. Assim, temos que no somatório só terão valor 1 as parcelas onde j for coprimo com n, no caso contrário, a parcela será nula. Por exemplo:

• Para $n = 2$, temos que

$$\sum_{j=1}^{1} \left\lfloor \frac{1}{\mathrm{mdc}(2, j)} \right\rfloor = \left\lfloor \frac{1}{1} \right\rfloor = 1 = \phi(2).$$

• Para $n = 3$, temos que

$$\sum_{j=1}^{2} \left\lfloor \frac{1}{\mathrm{mdc}(3, j)} \right\rfloor = \left\lfloor \frac{1}{1} \right\rfloor + \left\lfloor \frac{1}{1} \right\rfloor = 1 + 1 = 2 = \phi(3).$$

• Para $n = 4$, temos que

$$\sum_{j=1}^{3} \left\lfloor \frac{1}{\mathrm{mdc}(4, j)} \right\rfloor = \left\lfloor \frac{1}{1} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{1} \right\rfloor = 1 + 0 + 1 = 2 = \phi(4).$$

Dessa forma, concluímos que $\sum_{j=1}^{n-1} \left\lfloor \frac{1}{\mathrm{mdc}(n, j)} \right\rfloor = \phi(n)$. A resposta correta é o item (b).

3) (OBMU 2018 - 1ª fase - Q 23) Para quantos números primos p o número $p^3 - 4p + 9$ é um quadrado perfeito?

(a) 2 **(b)** 3 **(c)** 5 **(d)** 7

Solução: Queremos saber para quantos números primos p a expressão $p^3 - 4p + 9 = n^2$ para algum inteiro positivo n. Assim,

$$\begin{aligned} p^3 - 4p + 9 = n^2 &\implies n^2 - 9 \equiv 0 \mod p \\ &\implies p \mid (n-3) \text{ ou } p \mid (n+3) \\ &\implies n = q \cdot p + 3 \text{ ou } n = q \cdot p - 3, \text{ para algum inteiro } q \\ &\implies n^2 = (q \cdot p + 3)^2 \text{ ou } n^2 = (q \cdot p - 3)^2, \text{ para algum inteiro } q. \end{aligned} \tag{1}$$

Portanto, $p^3 - 4p + 9 = (q \cdot p + 3)^2$ ou $p^3 - 4p + 9 = (q \cdot p - 3)^2$ para algum inteiro q. Simplificando essas últimas expressões chegamos a

$$p(p - q^2) = 2(3q + 2) \text{ ou } p(p - q^2) = 2(-3q + 2),$$

respectivamente. Dessa forma, concluímos que $\left[p \mid 2 \text{ ou } p \mid (3q + 2)\right]$ ou $\left[p \mid 2 \text{ ou } p \mid (-3q + 2)\right]$, respectivamente. Notemos que $p \mid 2$ implica que $p = 2$ e, nesse caso, p é uma solução. Agora, suponhamos que p seja um primo ímpar e satisfaça a condição do enunciado da questão. Neste caso, existe um inteiro q (positivo) tal que $p \mid (3q + 2)$ ou $p \mid (-3q + 2)$. De qualquer forma, temos que $p \le 3q + 2$ e, por (1), que $n \ge q \cdot p - 3$. Assim,

(i) $p \le 3q + 2 \implies q \ge (p - 2)/3;$

(ii) $n \ge qp - 3 \underset{(i)}{\implies} n \ge (p(p - 2))/3 - 3 = (p^2 - 2p - 9)/3.$

Portanto,

$$\begin{aligned} n \ge \frac{p^2 - 2p - 9}{3} &\implies n^2 \ge \frac{p^4 - 4p^3 - 14p^2 + 36p + 81}{9} \\ &\implies p^3 - 4p + 9 \ge \frac{p^4 - 4p^3 - 14p^2 + 36p + 81}{9} \\ &\implies 0 \ge p^4 - 13p^3 - 14p^2 + 72p \\ &\implies 0 \ge p^3 - 13p^2 - 14p + 72, \end{aligned}$$

ou seja, $(p - 2)(p^2 - 11p - 16) \le 0$. Como $p > 2$, temos que

$$p^2 - 11p - 36 \le 0.$$

Resolvendo esta inequação, obtemos

$$\frac{11 - \sqrt{265}}{2} \leqslant p \leqslant \frac{11 + \sqrt{265}}{2}.$$

Notemos que os únicos valores para p primo são: $2, 3, 5, 7, 11$ e 13. Agora, basta verificar que, dentre esses números, aqueles que satisfazem $p^3 - 4p + 9 = n^2$ para algum inteiro n são: $2, 7$ e 11. Concluímos que existem apenas três números primos p tais que o número $p^3 - 4p + 9$ é um quadrado perfeito. A resposta correta é o item (b).

4) (OBMU 2019 - 1ª fase - Q 09) Para quantos valores de n inteiros positivos o determinante da matriz

$$\begin{pmatrix} 2^n & 3^n \\ 3^n & -2^n \end{pmatrix}$$

é divísivel por 7?

(a) 0 **(b)** 1 **(c)** 2 **(d)** 15

Solução: Vamos definir a matriz em questão por A_n e, inicialmente, iremos calcular o determinante de A_n em função de n.

$$\det A_n = -2^{2n} - 3^{2n} = -(4^n + 9^n).$$

Agora, utilizando a congruência modular e escrevendo os termos módulo 7, notemos que:

• como $4 \equiv 4 \mod 7$, então $4^n \equiv 4^n \mod 7$;

• como $9 \equiv 2 \mod 7$, então $9^n \equiv 2^n \mod 7$.

Disso, podemos concluir que

$$\det A_n \equiv -(4^n + 2^n) \mod 7,$$

ou seja,

$$\det A_n \equiv -2^n(2^n + 1) \mod 7.$$

Nosso objetivo é descobrir para quantos valores n vale a seguinte congruência

$$-2^n(2^n + 1) \equiv 0 \mod 7,$$

ou seja, para quantos valores n o inteiro 7 divide $2^n(2^n + 1)$. Como 7 não divide 2^n para qualquer inteiro n, então nosso objetivo é saber para quantos valores n o inteiro 7 divide $2^n + 1$.

Considere n um inteiro positivo. Pela Divisão Euclidiana, existem inteiros q e r, quociente e resto, tais que $n = 3q + r$ e $0 \leq r \leq 2$. Assim, $2^n + 1 = 2^{3q+r} + 1 = 8^q \cdot 2^r + 1$ onde $0 \leq r \leq 2$. Como $8 \equiv 1 \mod 7$, então

$$2^n + 1 \equiv 0 \mod 7 \iff \text{existe } r \in \{0, 1, 2\} \text{ tal que } 2^r + 1 \equiv 0 \mod 7.$$

Notemos que não existe $r \in \{0, 1, 2\}$ tal que 7 divida $2^r + 1$. A resposta correta é o item (a).

5) (OBMU 2019 - 1ª fase - Q 25) Considere a sequência definida por $a_1 = 0$, $a_2 = 1$ e, para $n \geq 3$,

$$a_n = (n-1)(a_{n-1} + a_{n-2})$$

Determine o resto na divisão de a_{2019} por 2019.

(a) 1 **(b)** 2017 **(c)** 2019 **(d)** 2018

Solução: Notemos que

$$\begin{aligned}
a_n &\equiv (n-1)(a_{n-1} + a_{n-2}) \mod n \\
&\equiv (-1)(a_{n-1} + a_{n-2}) \mod n \\
&\equiv (-1)\left[(n-2)(a_{n-2} + a_{n-3}) + a_{n-2}\right] \mod n \\
&\equiv (-1)\left[(n-1)a_{n-2} + (n-2)a_{n-3}\right] \mod n \\
&\equiv (-1)(-a_{n-2} - 2a_{n-3}) \mod n \\
&\equiv (-1)^2(a_{n-2} + 2a_{n-3}) \mod n \\
&\equiv (-1)^2\left[(n-3)(a_{n-3} + a_{n-4}) + 2a_{n-3}\right] \mod n \\
&\equiv (-1)^2\left[(n-1)a_{n-3} + (n-3)a_{n-4}\right] \mod n \\
&\equiv (-1)^2(-a_{n-3} - 3a_{n-4}) \mod n \\
&\equiv (-1)^3(a_{n-3} + 3a_{n-4}) \mod n \\
&\vdots \\
&\equiv (-1)^{n-2}\left[a_{n-(n-2)} + (n-2)a_{n-(n-1)}\right] \mod n \\
&\equiv (-1)^n\left[a_2 + (n-2)a_1\right] \mod n,
\end{aligned}$$

ou seja,

$$a_n \equiv (-1)^n\left[a_2 + (n-2)a_1\right] \mod n.$$

Substituindo $n = 2019$, $a_2 = 1$ e $a_1 = 0$ na última congruência acima obtemos

$$a_{2019} \equiv -1 \mod 2019,$$

ou seja, o resto da divisão de a_{2019} por 2019 é 2018. A resposta correta é o item (d).

6) (1ª CELL 2021 - Q 01) Seja

$$A = \begin{pmatrix} 1 & 2 & \cdots & 1000 \\ 1001 & 1002 & \cdots & 2000 \\ \vdots & \ddots & \vdots & \vdots \\ 999001 & 999002 & \cdots & 1000^2 \end{pmatrix}$$

Escolha qualquer entrada e a denote por x_1. Em seguida, apague a linha e coluna contendo x_1 para obtemos uma matriz 999×999. Então escolha qualquer entrada e a denote por x_2. Apague a linha e a coluna contendo x_2 para obter uma matriz 998×998. Realize essa operação 1000 vezes. Determine o valor da soma

$$x_1 + x_2 + \cdots + x_{1000}.$$

(a) 1000 **(b)** $\dfrac{1000^3 + 1000}{2}$ **(c)** 1000^2 **(d)** $\dfrac{1000^2 + 1000}{2}$ **(e)** $\dfrac{1001}{2}$

Solução: Primeiramente, iremos encontrar uma expressão geral para a_{ij}. Notemos que

$$a_{(i+1)j} = a_{ij} + 1000 \quad \text{e} \quad a_{i(j+1)} = a_{ij} + 1.$$

Assim, com i (ou j) fixo os elementos a_{ij} são progressões aritméticas de razão 1 (ou 1000). Como o elemento $a_{11} = 1$, temos que

$$a_{ij} = 1 + 1000 \cdot (i-1) + 1 \cdot (j-1)$$

$$a_{ij} = 1 + 1000 \cdot (i-1) + j - 1$$

$$a_{ij} = 1000 \cdot (i-1) + j.$$

Agora, notemos que, se $x_n = a_{i_n j_n}$ para todo $n = 1, ..., 1000$, então $1 \leq i_n, j_n \leq 1000$, com $i_n \neq i_m$ se $n \neq m$ e $j_n \neq j_m$ se $n \neq m$. Assim,

$$\begin{aligned}\sum_{n=1}^{1000} x_n = \sum_{n=1}^{1000}\left[1000 \cdot (i_n - 1) + j_n\right] &= \sum_{n=1}^{1000} 1000 \cdot (i_n - 1) + \sum_{n=1}^{1000} j_n \\ &= \sum_{i=1}^{1000} 1000 \cdot (i-1) + \sum_{j=1}^{1000} j.\end{aligned}$$

Por outro lado, usando a regra de soma dos termos de uma PA, temos que

$$\sum_{i=1}^{1000} 1000 \cdot (i-1) = \frac{1000\left[0 + 1000(1000-1)\right]}{2} = \frac{1000^3 - 1000^2}{2}$$

e

$$\sum_{j=1}^{1000} j = \frac{1000(1+1000)}{2} = \frac{1000^2+1000}{2}.$$

Portanto,

$$\sum_{n}^{1000} x_n = \frac{1000^3-1000^2}{2} + \frac{1000^2+1000}{2}$$
$$= \frac{1000^3+1000}{2}.$$

A resposta correta é o item (b).

7) (1ª CELL 2021 - Q 02) Quantos ternos racionais aparecem na expansão binomial de

$$(\sqrt[3]{2}+\sqrt{6})^{100}?$$

(a) 16 **(b)** 17 **(c)** 66 **(d)** 33 **(e)** 50

Solução: Usando a expansão do binômio de Newton, temos que

$$(\sqrt[3]{2}+\sqrt{6})^{100} = \sum_{n=0}^{100} \binom{100}{n} \cdot (\sqrt[3]{2})^n \cdot (\sqrt{6})^{100-n}$$
$$= \sum_{n=0}^{100} \binom{100}{n} \cdot (\sqrt[3]{2})^n \cdot \frac{6^{50}}{(\sqrt{6})^n}$$

Sabemos que:

- todos os termos da forma $\binom{100}{n}$ são inteiros e, portanto, racionais;
- $(\sqrt[3]{2})^n$ é racional se, e somente se, 3 divide n;
- $(\sqrt{6})^n$ é racional se, e somente se, 2 divide n;
- o produto de um número racional (não nulo) por um número irracional resulta em um número irracional.

Dessa forma, concluímos que

$$\binom{100}{n} \cdot (\sqrt[3]{2})^n \cdot (\sqrt{6})^{100-n} \text{ é racional se, e somente se, } 6 \mid n.$$

Como $n \in [0,100]$, basta determinar todos os múltiplos de 6 no intervalo $[0,100]$. Notemos que

$$n = 6k \in [0,100] \iff k \in \{0,1,...,16\}.$$

Portanto, existem 17 múltiplos de 6 no intervalo $[0,100]$. A resposta correta é o item (b).

8) (1ª CELL 2021 - Q 03) Seja $f : \{1,2,\cdots\} \longrightarrow \mathbb{R}$ uma função tal que $f(n)-f(n+1) = f(n)f(n+1)$ para todo $n \geq 1$. Sabendo que $f(2020) = 1/4040$, o valor de $f(1)$ é:

(a) $\frac{1}{2}$ **(b)** $\frac{1}{4040}$ **(c)** $\frac{1}{2021}$ **(d)** 1 **(e)** $\frac{1}{2020}$

Solução: Primeiramente, notemos que

$$f(n) - f(n+1) = f(n)f(n+1) \implies f(n+1) + f(n)f(n+1) = f(n),$$

ou seja,

$$f(n+1) = \frac{f(n)}{1+f(n)}$$

para todo $n \in \{1, 2, ...\}$. Deixamos para o leitor mostrar, por indução em n, que

$$f(n+1) = \frac{f(1)}{1+n \cdot f(1)}$$

é verdadeiro para todo $n \in \{1, 2, ...\}$. Agora, como $f(2020) = 1/4040$ segue que

$$\frac{1}{4040} = f(2019+1) = \frac{f(1)}{1+2019 \cdot f(1)},$$

ou seja,

$$\frac{1}{4040} = \frac{f(1)}{1+2019 \cdot f(1)}.$$

Assim, concluímos que $f(1) = 1/2021$. A resposta correta é o item (c).

9) (1ª CELL 2021 - Q 04) Considere a sequência a_n definida por $a_1 = 2$ e para todo $n \in \mathbb{N}$

$$a_{n+1} = (a_n)^2 + 6a_n + 6.$$

Determine o resto de a_{100} na divisão por 7.

(a) 0 **(b)** 1 **(c)** 2 **(d)** 3 **(e)** 4

Solução: Primeiramente, notemos que

- como $a_2 = 2^2 + 6 \cdot 2 + 6 = 22$, então $a_2 \equiv 1 \mod 7$;
- como $a_3 = (a_2)^2 + 6a_2 + 2$, então $a_3 \equiv 1^2 + 6 \cdot 1 + 6 \mod 7$, ou seja, $a_3 \equiv 6 \mod 7$;
- como $a_4 = (a_3)^2 + 6a_3 + 2$, então $a_4 \equiv 6^2 + 6 \cdot 6 + 6 \mod 7$, ou seja, $a_4 \equiv 1 \mod 7$.

Dessa maneira, conseguimos concluir a seguinte regra para todo $n > 1$:

$$a_n \equiv \begin{cases} 1 \mod 7, & \text{se n é par} \\ 6 \mod 7, & \text{se n é ímpar} \end{cases}$$

Logo, o resto de a_{100} na divisão por 7 é 1. A resposta correta é o item (b).

10) (1ª CELL 2021 - Q 05) Considere o número real, escrito em notação decimal,

$$r = 0,235831...$$

em que, a partir da terceira casa decimal após a vírgula, todo dígito é igual ao resto na divisão por 10 da soma dos dois dígitos anteriores. Podemos afirmar que

(a) $(10^{60} - 1) \cdot r$ é inteiro

(b) $(10^{25} - 1) \cdot r$ é inteiro

(c) $(10^{17} - 1) \cdot r$ é inteiro

(d) r é irracional algébrico

(e) r é irracional não algébrico

Solução: Considere (F_n) a sequência de Fibonacci e (a_n) a sequência formada pelos dígitos de r apos a vírgula, ou seja, $0 \leq a_n < 10$ para todo $n \in \mathbb{N}^*$ e $a_1 = 2$, $a_2 = 3$, $a_3 = 5$, ... Neste caso, temos que

$$F_{n+2} \equiv a_n \mod 10$$

para todo inteiro $n \geq 1$. Por outro lado, temos que

$$F_{(n+2)+60} \equiv F_{n+2} \mod 10$$

para todo inteiro $n \geq 1$. Segue que

$$a_{n+60} \equiv a_n \mod 10$$

para todo inteiro $n \geq 1$. Como $a_n < 10$ para todo $n \in \mathbb{N}^*$, segue que

$$a_{n+60} = a_n$$

para todo inteiro $n \geq 1$. Daí, a cada 60 termos, a sequência volta a se repetir. Se denotarmos por r_1 este período, então multiplicando r por 10^{60}, obtemos

$$10^{60} \cdot r = r_1 + r,$$

ou seja,

$$10^{60} \cdot r - r = r_1.$$

Logo $10^{60} \cdot r - r = (10^{60} - 1) \cdot r = r_1$ é inteiro. A resposta correta é o item (a).

11) (2ª CELL 2021 - Q 03) O resto da divisão de $2^{2021} + 3^{2021}$ por 17 é

(a) 12 **(b)** 13 **(c)** 14 **(d)** 15 **(e)** 16

Solução: Primeiramente, notemos que

- o Pequeno Teorema de Fermat implica que $2^{16} \equiv 1 \mod 17$. Assim, $(2^{16})^{126} \equiv 1^{126} \mod 17$, ou seja, $2^{2016} \equiv 1 \mod 17$. Além disso, temos que $2^5 \equiv 15 \mod 17$. Portanto,

$$2^{2021} \equiv 15 \mod 17;$$

- o Pequeno Teorema de Fermat implica que $3^{16} \equiv 1 \mod 17$. Assim, $(3^{16})^{126} \equiv 1^{126} \mod 17$, ou seja, $3^{2016} \equiv 1 \mod 17$. Além disso, temos que $3^5 \equiv 5 \mod 17$. Portanto,

$$3^{2021} \equiv 5 \mod 17.$$

Portanto,

$$\begin{aligned} 2^{2021}+3^{2021} &\equiv 15+5 \mod 17 \\ &\equiv 20 \mod 17 \\ &\equiv 3 \mod 17. \end{aligned}$$

O resto da divisão de $2^{2021}+3^{2021}$ por 17 é 3. Nenhuma das alternativas contém a resposta correta.

12) (2ª CELL 2021 - Q 15) Para n natural, seja A_n a matriz 2×2 com entradas $a_n, b_n, c_n, d_n \in \mathbb{Z}$ dada por

$$A_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}^n$$

(a n-ésima potência da matriz de entradas 2,1,-1,2). Para quantos valores de n dentre $1, 2, \ldots, 2021$ a entrada c_n é um múltiplo de 7?

(a) 250 **(b)** 251 **(c)** 252 **(d)** 253 **(e)** 254

Solução: Como queremos saber para quantos valores de n entre $1, 2, ..., 2021$ a entrada c_n é múltiplo de 7, então iremos calcular os coeficientes de A_n módulo 7. Notemos que

$$A_1 = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix},\ A_2 = \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix},\ A_3 = \begin{pmatrix} 2 & -4 \\ 4 & 2 \end{pmatrix},\ A_4 = \begin{pmatrix} 0 & -3 \\ 3 & 0 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} -3 & -6 \\ 6 & -3 \end{pmatrix},\ A_6 = \begin{pmatrix} -5 & -2 \\ 2 & -5 \end{pmatrix},\ A_7 = \begin{pmatrix} -5 & 1 \\ -1 & -5 \end{pmatrix},\ A_8 = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}.$$

Segue que

$$A_{8k} = \begin{pmatrix} (-2)^k & 0 \\ 0 & (-2)^k \end{pmatrix}$$

para todo k. Como

$$2021 = 8\cdot 252 + 5,$$

segue que existem pelo menos 252 valores para n tais que o termo c_n de A_n é múltiplo de 7. Para provar que existem apenas esses valores para n tal que c_n é múltiplo de 7, usaremos a seguinte informação, que pode ser provada por indução: para todo n, temos que $a_n = d_n$ e $c_n = -b_n$. Suponhamos que existe n tal que $c_n \equiv 0 \mod 7$. Portanto,

$$A_n = \begin{pmatrix} a_n & 0 \\ 0 & a_n \end{pmatrix}.$$

Agora, usando o algorítmo da divisão, considere $q, r \in \mathbb{N}\cup\{0\}$ tais que $n = 8q + r$, onde $0 \le r < 8$ (notemos que $n \ge 8$). Assim,

$$\begin{pmatrix} a_n & 0 \\ 0 & a_n \end{pmatrix} = A_n = A_{8q}\cdot A_r = \begin{pmatrix} (-2)^q & 0 \\ 0 & (-2)^q \end{pmatrix}\cdot A_r = (-2)^q\cdot A^r.$$

Se $r \neq 0$, segue que $(-2)^q \cdot c_r \equiv 0 \mod 7$, onde $c_r \in \{1, 4, 3, 6, 2, -1\}$ o que é absurdo. Logo, $r = 0$. A resposta correta é o item (c).

13) (3ª CELL 2022 - Q 03) Seja a um inteiro positivo tal que

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{25} = \frac{a}{25!}.$$

Encontre o resto de a na divisão por 13.

(a) 1 **(b)** 2 **(c)** 3 **(d)** 7 **(e)** 12

Solução: Primeiramente, notemos que

$$\sum_{n=1}^{25} \frac{1}{n} = \frac{a}{25!} \implies \sum_{n=1}^{25} \frac{25!}{n} = a \implies \sum_{n=1}^{12} \frac{25!}{n} + \frac{25!}{13} + \sum_{n=14}^{25} \frac{25!}{n} = a.$$

Além disso, temos que

- $\sum_{n=1}^{12} \frac{25!}{n} \equiv 0 \mod 13$;
- $\sum_{n=14}^{25} \frac{25!}{n} \equiv 0 \mod 13$;
- $14 \cdot 15 \cdots 25 \equiv 1 \cdot 2 \cdots 12 \mod 13$.

Portanto,

$$\begin{aligned} a &\equiv \sum_{n=1}^{25} \frac{25!}{n} \mod 13 \\ &\equiv \sum_{n=1}^{12} \frac{25!}{n} + \frac{25!}{13} + \sum_{n=14}^{25} \frac{25!}{n} \mod 13 \\ &\equiv \frac{25!}{13} \mod 13 \\ &\equiv 12! \cdot (14 \cdot 15 \cdots 25) \mod 13 \\ &\equiv 12! \cdot 12! \mod 13, \end{aligned}$$

ou seja,

$$a \equiv (12!)^2 \mod 13.$$

Por outro lado, o Teorema de Wilson implica que

$$12! \equiv -1 \mod 13.$$

Portanto,

$$a \equiv 1 \mod 13.$$

Concluímos que o resto de a por 13 é 1. A resposta correta é o item (a).

14) (3ª CELL 2022 - Q 15) Considere a matriz

$$A = \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}$$

Qual o menor inteiro $n > 0$ para o qual $A^n \equiv A \mod 11$? Aqui, dadas duas matrizes 2×2 X e Y com entradas inteiras, escrevemos $X \equiv Y \mod 11$ se cada entrada de X é congruente módulo 11 à entrada de Y na mesma posição.

(a) 11 **(b)** 16 **(c)** 121 **(d)** 110 **(e)** 120

Solução: Como queremos saber quando duas matrizes são equivalentes módulo 11, então iremos calcular as matrizes A^n com os coeficientes módulo 11. Notemos que

$$A^2 \equiv \begin{pmatrix} 4 & -2 \\ 2 & 4 \end{pmatrix} \mod 11 \qquad \text{e} \qquad A^3 \equiv \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \mod 11.$$

Seja n um inteiro positivo. Então, pela Divisão de Euclides, existem $q, r \in \mathbb{Z}$ com $0 \leq r < 3$ tais que $n = 3q + r$. Assim,

$$\begin{aligned} A^n &\equiv A^{3q}A^r \mod 11 \\ &\equiv 4^q A^r \mod 11. \end{aligned}$$

Nosso objetivo é encontrar o menor inteiro $q \geq 1$ tal que $4^q A^r \equiv A \mod 11$ para algum $0 \leq r < 3$. Agora, deixamos para o leitor a verificação dos seguintes fatos:

- Se $r = 0$. Nesse caso, não existe $q \geq 1$ tal que $4^q I_2 \equiv A \mod 11$, onde I_2 é a matriz identidade de ordem 2.
- Se $r = 1$. Nesse caso, o menor inteiro $q \geq 1$ tal que $4^q A \equiv A \mod 11$ é $q = 5$. Assim, $n = 3 \cdot 5 + 1 = 16$ é o menor valor para $r = 1$.
- Se $r = 2$. Nesse caso, não existe inteiro $q \geq 1$ tal que $4^q A^2 \equiv A \mod 11$.

Assim, 16 é o menor inteiro n tal que $A^n \equiv A \mod 11$. A resposta correta é o item (b).

15) (OMpD 2022 - 1ª fase - Q 01) Qual o resto da divisão de $11^{3333} + 33^{1111}$ por 7?

(a) 0 **(b)** 1 **(c)** 3 **(d)** 5 **(e)** 6

Solução: Primeiramente, notemos que

- como $11^3 \equiv 1 \mod 7$, então $(11^3)^{1111} \equiv 1^{1111} \mod 7$, ou seja,
$$11^{3333} \equiv 1 \mod 7;$$
- o Pequeno Teorema de Fermat implica que $33^6 \equiv 1 \mod 7$. Assim, $(33^6)^{185} \equiv 1^{185} \mod 7$, ou seja, $33^{1110} \equiv 1 \mod 7$. Isso implica que $33^{1111} \equiv 33 \mod 7$, ou seja,
$$33^{1111} \equiv 5 \mod 7.$$

Portanto,

$$\begin{aligned} 11^{3333} + 33^{1111} &\equiv 1 + 5 \mod 7 \\ &\equiv 6 \mod 7. \end{aligned}$$

O resto da divisão de $11^{3333} + 33^{1111}$ por 7 é 6. A resposta correta é o item (e).

Considerações Finais

As olimpíadas de Matemática são de extrema importância para despertar o interesse pelo estudo da Matemática, incentivando os alunos e revelando talentos na área. A motivação desse trabalho foi a falta de material publicado e disponível para estudo, tratando-se de olimpíadas de Matemática de nível universitário. Desenvolvemos soluções de problemas olímpicos envolvendo conteúdos de aritmética, que foram extraídos de competições universitárias de Matemática, sendo selecionadas apenas as questões que não têm nenhuma solução publicada nas páginas oficiais das competições. Além disso, os problemas foram retirados de competições realizadas apenas nos últimos 6 anos, o que aumentou a dificuldade na seleção dessas questões.

Abreviações

[**CELL**] - Competição Elon Lages Lima de Matemática

[**GN**] - Gallois Noether

[**OBMU**] - Olimpíada Brasileira de Matemática Universitária

[**OMpD**] - Olimpíada Matemáticos por Diversão

Referências

[1] Bagatini, A. *Olimpíadas de Matemática, Altas Habilidades e Resolução de Problemas*. 82 f. Monografia (Graduação em Matemática) - UFRGS, Porto Alegre, 2010. Disponível em: <http://hdl.handle.net/10183/29144>. Acesso em: 4 de Novembro de 2022.

[2] Costa, G. C. *Ordem de Aparição na Sequência de Fibonacci: um Problema sobre Divisibilidade*. 81 p. Dissertação (Mestrado em Matemática) - UNB, Brasília, 2015. Disponível em: <https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=1887&id2=80134>. Acesso em: 5 de Janeiro de 2023.

[3] Hefez, A. *Aritmética*. Coleção Profmat. 2. ed. Rio de Janeiro: SBM, 2016. 298 p.

[4] Maciel, M. V. M.; Basso, M. V. de A. *Olimpíada Brasileira de Matemática das Escolas Públicas (Obmep): As origens de um projeto de qualificação do ensino de Matemática na educação básica*. X Encontro Gaúcho de Educação Matemática, 2009. Disponível em: <https://www.projetos.unijui.edu.br/matem\atica/cd_egem/>. Acesso em: 4 de Novembro de 2022.

[5] OBM. Olimpíada Brasileira de Matemática, 2023. Provas e gabaritos. Disponível em:<https://www.obm.org.br/como-se-preparar/provas-e-gabaritos/> . Acesso em: 1 de Março de 2023.

[6] OMpD. Matemático por Diversão, [s.d]. Página inicial. Disponível em: <https://matematicopordiversao.wordpress.com/>. Acesso em: 10 de Novembro de 2022.

[7] Ramos, M. G. O. *A Sequência de Fibonacci e o Número de Ouro*. 93 p. Dissertação (Mestrado em Matemática) - UESC, Ilhéus, 2013. Disponível em: <https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=90&id2=27580>. Acesso em: 5 de Janeiro de 2023.

Manoel Rodrigues de A. Neto
Universidade Federal da Paraíba
<manoel_rodriguez@hotmail.com>

Wállace M. de Sousa
Universidade Federal da Paraíba
<wallace@mat.ufpb.br>

Recebido: 27/03/2023
Publicado: 07/06/2023