Matemática & Ciência

NÚMEROS PRIMOS E DÍZIMAS – UMA APROXIMAÇÃO ENTRE A TEORIA DOS NÚMEROS E A ESCOLA BÁSICA (1)

PRIME NUMBERS AND REPEATING DECIMAL NUMBERS - AN APPROXIMATION BETWEEN THETHEORY OF NUMBERS AND ELEMENTARY SCHOOL (I)

Rubens Vilhena Fonseca[1]
Andreza Thalia Menezes Monteiro[2]
Richard Campos Vilhena Fonseca[3]
Lidhyanne Cristina Silva Lima[4]

Resumo

O presente artigo é o primeiro de dois artigos que apresentam conexões entre a Matemática da Escola Básica e os conteúdos de Teoria dos Números e Álgebra Abstrata. Neste, a ênfase será em tópicos da Teoria dos Números que fundamentam o principal resultado neste artigo, isto é, para um número primo $p > 5$, a expansão decimal de $1/p$ é puramente periódica, os comprimentos dos períodos são sempre pares e, se quebrarmos os dígitos da parte periódica em duas partes e adicionarmos, temos um número para o qual todos os dígitos são iguais a 9. Apresentamos uma prova, em nível elementar, desse resultado conhecido como Teorema de Midy. Os conteúdos da Teoria dos Números que fundamentam os resultados são apresentados tendo sempre em mente os professores da Escola Básica. O texto está estruturado segundo as quatro categorias, propostas por Schoenfeld, de conhecimento/ habilidades necessárias diante de problemas matemáticos.

Palavras-chave: Números primos. Expansão decimal. Teoria dos números. Teorema de Midy.

Abstract

This article is the first of two articles that present connections between Elementary School Mathematics and the contents of Number Theory and Abstract Algebra. In this one, the emphasis will be on Number Theory topics that support the main result in this article, that is, for a prime number p > 5,

[1]Doutor em Educação Matemática pela Pontifícia Universidade Católica de São Paulo. Professor da Universidade do Estado do Para (UEPA). E-mail: rubens.vilhena@uepa.br
[2] Licenciada em Matemática pela Universidade do Estado do Pará (UEPA)
E-mail: andrezathaliamn@gmail.com
[3] Licenciando em Física pela Universidade Católica Paulista (UCA). Bacharelando em Física pela Universidade Federal do Pará (UFPA) – E-mail: richardfonseca207@gmail.com
[4] Licencianda em Matemática pela Universidade do Estado do Pará (UFPA)
E-mail: lidhyanne.lima@aluno.uepa.br

the decimal expansion of 1/p is purely periodic, the period lengths are always even and, if if we break the digits of the periodic part into two parts and add them, we have a number where all the digits are equal to 9. We present a proof, at the elementary level, of this known result Midy's Theorem. The contents of the Theory of Numbers that support the results are presented always keeping in mind the teachers of the Basic School. The text is structured according to the four categories, proposed by Schoenfeld, of knowledge/skills needed in the face of mathematical problems.

Keywords: Prime Numbers. Decimal Expansion. Number Theory. Midy's Theorem.

Introdução

Resolução de problemas matemáticos é a força motivadora para a descoberta e compreensão de novos conceitos. Eles fornecem o pano de fundo para o surgimento de novas ideias. Podemos não ver uma demonstração de uma conjectura imediatamente, no entanto, são as buscas pelas provas dessas conjecturas que proporcionam uma rica interação entre as teorias matemáticas e demonstram, de forma indireta, uma profunda relação entre elas.

> A Resolução de Problemas é um método eficaz para desenvolver o raciocínio e para motivar os alunos para o estudo da Matemática. O processo ensino e aprendizagem pode ser desenvolvido através de desafios, problemas interessantes que possam ser explorados e não apenas resolvidos. (LUPINACCI; BOTIN, 2004, p. 1).

A situação-problema que vamos considerar neste artigo se refere ao período das dízimas com denominadores primos maiores que 5. Por exemplo, o número $\frac{1}{17} = \overline{.058823522941117647}$ possui um bloco de repetição (058823522941117647) de comprimento de 16 dígitos chamado de período. Essa é chamada de *dízima puramente periódica,* pois a parte que se repete inicia imediatamente após a vírgula decimal.

Será que é possível prever antecipadamente qual será o comprimento do período desses tipos de dízimas? O valor do tamanho do período é sempre um divisor de $p-1$? Existe alguma relação entre os períodos de

$^1/_p$ e $^1/_r$? Para responder a essas perguntas e as ramificações matemáticas a que ela nos leva, começaremos por trabalhar em sentido inverso.

Pretendemos mostrar as conexões entre conteúdos de Matemática Superior e Matemática da Escola Básica. Para isso, apresentamos tópicos da Teoria dos Números que fundamentam nosso estudo sobre o período das dízimas de frações geratrizes, que são os recíprocos de números primos $p > 5$, isto é, o período das frações da forma $^1/_p$, e demonstraremos um resultado apresentado por Etienne Midy (1775-1846), em 1835, sobre essas dízimas; uma conjectura em aberto apresentada por Emil Artin (1898-1962), em 1927, a partir dos trabalhos de J. C. F. Gauss (1777-1855); e a conexão entre os divisores primos dos números *repunits* e a ordem de 10 módulos primos. Na última parte deste artigo, apresentamos a definição de números *repunit*s.

Nossa proposta se alinha com as pesquisas de Alan Schoenfeld (1985), onde ele assume que a compreensão e o ensino da Matemática devem ser abordados como um domínio de resolução de problemas. Quatro categorias de conhecimento/habilidades são necessárias para alguém ser bem-sucedido na Matemática: (1) *Recursos* – conhecimento de procedimentos e questões da Matemática; (2) *Heurísticas* – estratégias e técnicas para resolução de problemas, tais como trabalhar o que foi ensinado, ou desenhar figuras; (3) *Controle* – decisões sobre quando e quais recursos usar; e (4) *Convicções* – uma visão matemática do mundo, que determina como alguém aborda um problema. Nesse texto, essas quatro categorias estão implícitas.

Para Schoenfeld, o processo de resolução de problemas é, em última análise, um diálogo entre o conhecimento prévio do solucionador de problemas, suas tentativas e seus pensamentos ao longo do caminho (SCHOENFELD, 1982). Como tal, o caminho da solução de um problema é um processo emergente e contextualmente dependente.

Nessa perspectiva, para que possamos dar continuidade sobre a nossa situação-problema e discutirmos os outros resultados, precisamos definir alguns conceitos importantes da Teoria dos Números: Congruências, a função $\varphi(n)$ de Euler, o Pequeno Teorema de Fermat e a Fórmula de Euler, a Ordem de um inteiro módulo m e a Raiz Primitiva de um inteiro n.

O texto visa dar um nível de rigor matemático acessível à Educação Básica. Nossa intenção é que o texto seja acessível aos professores e futuros professores da Educação Básica. Por esse motivo, as demonstrações de alguns resultados serão indicadas nas referências.

Recursos e Controle

Congruências – A aritmética modular

Muitos relógios têm o *design* familiar de 12 horas. Em inglês, designamos se o horário é antes do meio dia ou depois do meio-dia usando as abreviações A.M. e P.M.[5]. Uma referência às 7:00 A.M. significa 7 horas depois da meia-noite; uma referência às 7:00 P.M. significa 7 horas depois do meio-dia. Em ambos os casos, uma vez que 12 é alcançado no relógio, tudo é zerado e começamos de novo com 1. O 12 funciona como um "zero" semelhante ao do conjunto dos Inteiros, por isso, às vezes usamos a expressão "zero hora".

Se quisermos determinar um momento no futuro ou no passado, é necessário considerar se passamos das 12 horas. Para determinar o horário 8 horas após as 3 horas, acrescentamos 8 ao 3. Como não passamos das 12 horas, o horário é 11 horas da manhã (Figura 1A). No entanto, para determinar o tempo 8 horas após as 9 horas, devemos levar em consideração que passamos das 12 horas. Portanto, 8 horas após as 9 horas são 5 horas da tarde, como mostrado na Figura 1B.

[5]A abreviatura A.M. vem do Latim *ante* (antes) *meridiem* (meio-dia). A abreviação P.M. vem do Latim *post* (depois) *meridiem* (meio-dia).

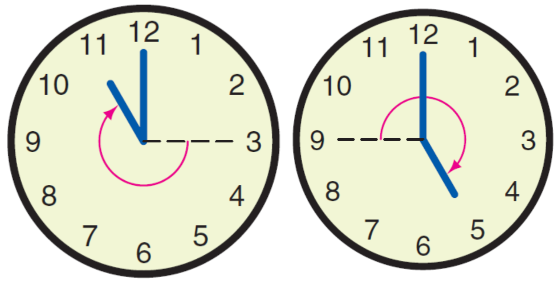

Figura 1A e 1B – Passado e presente no relógio
Fonte: Elaborada pelos autores (2022)

O que temos, de fato, é um ciclo de tamanho 12, no qual os resultados são todos os restos possíveis numa divisão por 12:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Então, ao somarmos no relógio 9 mais 8, o que queremos é o resto da divisão dessa soma por 12. Ou seja, 9 + 8 = 17 e o resto da divisão de 17 por 12 é 5. Por isso, nos referimos às 17h como 5h da tarde.

Situações como essas, que se repetem em ciclos, são representadas matematicamente usando aritmética modular, ou *congruência módulo n* (ROSEN, 2011).

Definição: Dois inteiros a e r são ditos serem congruentes módulo n, onde n é um número natural, *se,* $\frac{a-r}{n} = q$, onde q é um inteiro. Nesse caso, escrevemos$a \equiv r\ (mod\ n)$. O número n é chamado de módulo. A declaração $a \equiv r\ (mod\ n)$ é chamada de congruência.

Observe que, se $a \equiv r\ (mod\ n)$, então $\frac{a-r}{n} = q$, o que nos leva a $a - r = nq$. Dessa forma, podemos afirmar que:

$$a \equiv r\ (mod\ n) \Leftrightarrow \frac{a-r}{n} = q \Leftrightarrow a - r = nq \Leftrightarrow a = nq + r, \text{onde } n, q \in \mathbb{Z} \text{ e } n > 0.$$

Assim, do nosso exemplo, podemos dizer que:

$$17 \equiv 5\ (mod\ 12) \Leftrightarrow \frac{17-5}{12} = q \Leftrightarrow 17 - 5 = 12q \Leftrightarrow 17 = 12q + 5,$$

$$\text{onde } 12,\ q \in \mathbb{Z} \text{ e } 12 > 0.$$

Função $\varphi(n)$ de Euler

Definição 1: Chama-se função *phi de Euler* a função aritmética φ, assim definida para todo inteiro positivo n: $\varphi(n)$ é igual ao número de inteiros positivos menor que n e que são relativamente primos com n.

Em outros termos, $\varphi(n)$ é igual ao número de inteiros da sequência finita $\{1, 2, 3, \dots, n-1, n\}$ que são relativamente primos com n. Portanto, em linguagem dos conjuntos, $\varphi(n)$ é igual ao número de elementos (cardinal) do conjunto:

$$\varphi(n) = \#\{a \in \mathbb{N} | 1 \leq a \leq n \ \text{ e } \ \text{MDC}(a, n) = 1\}$$

Em particular, $\varphi(1) = 1$ porque o único inteiro positivo $n \leq 1$ é o próprio 1 e o $mdc(1,1) = 1$. E, $\varphi(n) < n$ para todo $n \geq 2$.

A Tabela abaixo dá os valores de $\varphi(n)$ para os onze primeiros inteiros positivos:

n	1	2	3	4	5	6	7	8	9	10	11
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10

Tabela 1 – Valores de $\varphi(n)$ para os onze primeiros inteiros positivos
Fonte: Elaborada pelos autores (2022)

Teorema 1: Seja o número primo p, então $\varphi(p) = p - 1$ (VIEIRA, 2015).

O Pequeno Teorema de Fermat

O *Pequeno Teorema de Fermat* afirma que, se p é um primo e p não divide um inteiro positivo a, então,

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

Em outras palavras, o Pequeno Teorema de Fermat indica que, se considerarmos qualquer inteiro positivo não divisível por um primo p, então a divisão e a^{p-1} por p, sempre deixa resto 1 (BURTON, 2016).

Fórmula de Euler

Essa fórmula certamente não é verdade, se substituirmos p por um número composto m. Por exemplo, $2^{9-1} \equiv 4\ (mod\ 9)$. Então, a pergunta é: se há alguma potência, dependendo do módulo m, de tal forma que:

$$a^{?} \equiv 1\ (mod\ n)?$$

Nossa primeira observação é que isso é impossível se MDC(a, n) > 1. Para ver o porquê, suponha que $a^k \equiv 1\ (mod\ n)$. Portanto, $a^{\,k} = 1 + mq$ para algum inteiro q, então MDC(a, n) divide $a^k - nq = 1$. Em outras palavras, se alguma potência de a é congruente a 1 módulo n, desse modo, devemos ter MDC(a, n) = 1. Isso sugere que nós olhamos para o conjunto de números que são relativamente primos com n,

$$\varphi(n) = \#\{a : 1 \leq a < n\ e\ \mathrm{MDC}(a, n) = 1\}$$

Suponha, por exemplo, que queremos encontrar uma potência de 7 que seja congruente a 1 módulo 10. Em vez de considerar todos os números $1 \leq a < 10$, vamos apenas tomar os números que são relativamente primos com 10. Eles são:

$$1, 3, 7, 9\ (mod\ 10)$$

Se multiplicarmos cada um deles por 7,temos:

$$7 \cdot 1 \equiv 7\ (mod\ 10),\ 7 \cdot 3 \equiv 1\ (mod\ 10),$$
$$7 \cdot 7 \equiv 9\ (mod\ 10),\ 7 \cdot 9 \equiv 3\ (mod\ 10).$$

Note que, temos de volta os mesmos números, mas rearranjados. Então, se os multiplicarmos todos juntos, teremos o mesmo produto,

$$(7 \cdot 1)\ (7 \cdot 3)\ (7 \cdot 7)\ (7 \cdot 9) \equiv 1 \cdot 3 \cdot 7 \cdot 9\ (mod\ 10)$$

$$7^4\ (1 \cdot 3 \cdot 7 \cdot 9) \equiv 1 \cdot 3 \cdot 7 \cdot 9\ (mod\ 10).$$

Agora, podemos cancelar $(1 \cdot 3 \cdot 7 \cdot 9)$ para obter $7^4 \equiv 1\ (mod\ 10)$.

De onde vem o expoente 4? É igual ao número de inteiros entre 1 e 10, relativamente primos com 10, ou seja, o expoente é 4 porque $\varphi(10) = 4$.

Isso sugere a verdade da seguinte fórmula (SANTOS,1998):

Teorema 5 *(Fórmula de Euler):* Se $\text{MDC}(a, n) = 1$, então,

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

Observe que, se n é igual a um número primo ímpar p, a Fórmula de Euler se reduz ao *Pequeno Teorema de Fermart*, de acordo com o Teorema 1:

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

A fórmula de Euler é uma generalização do *Pequeno Teorema de Fermat* para inteiros não primos.

Ordem de um Inteiro módulo n

Sejam a e $n > 1$ dois inteiros, tais que o MDC(a, b) = 1. Pela fórmula de Euler:

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

isto é, $\varphi(n)$ é uma solução inteira e positiva da congruência exponencial:

$$a^k \equiv 1(mod\ n).$$

Entretanto, essa congruência pode ter soluções inteiras e positivas menores que $\varphi(n)$.

Assim, para a = 5 e n =17, por exemplo, vejamos na Tabela 2 que nos dá todas as potências de a módulo 17, isto é, $a^k(mod\ 17)$, onde $1 \leq k \leq 16$:

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	9	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Quadro 1 – Ordens de a módulo 17
Fonte: Elaborada por Rubens Vilhena Fonseca (2022)

Pelo Quadro1, a congruência $5^k \equiv 1(mod\ 17)$ admite também a solução k = 4, e as soluções k= 8 e k =12. Essas soluções são menores que $\varphi(12)$.

A menor dessas soluções, k=4, é chamada de *ordem* de 5 módulo 17. Em símbolos: $O_{17}(5) = 4$.

Observe, no Quadro1, que a ordem cria um padrão nos valores das potências. Elas passam a ter valores sempre ordenados, antes e depois da ordem. A ordem de um número a módulo um primo p sempre divide $\varphi(p) = p - 1$ (BURTON, 2016).

Definição: Sejam a um inteiro positivo e $p > 5$ um primo, tais que o MDC(a, p) = 1. Chama-se ordem de a módulo p o menor inteiro positivo k, tal que $a^k \equiv 1(mod\, p)$.

Observe, pelo Quadro 1, que se a = 10, a ordem de 10 módulo 17 seria igual a $\varphi(17)$, ou seja, $O_{17}(10) = \varphi(17) = 16$. Vamos definir esse caso.

Raiz Primitiva

Definição: Chama-se raiz primitiva de um número primo p um inteiro r, tal que MDC(r, p) = 1, e a ordem de r módulo p é $\varphi(p)$, isto é, $O_p(r) = \varphi(p)$.

Em outros termos, raiz primitiva de um primo p é um inteiro r,tal que:

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

e $r^k \not\equiv 1(mod\, p)$, para todo inteiro positivo $k < \varphi(p)$ (ROSEN, 2011).

Pelo Quadro 1, pode-se ver que 3, 5, 6, 7,10, 11, 12 e 14 são as raízes primitivas de 17. Todos esses números têm ordem 16 módulo 17.

Observe que na linha onde estão as raízes primitivas, temos todos os valores do intervalo $1 \leq p \leq \varphi(p)$.

Agora, estamos em condições de analisar as questões sobre o comprimento do período da expansão decimal de ${}^{1}/_{p}$ e ${}^{r}/_{p}$.

Heurísticas – Estratégias e técnicas

O comprimento da expansão da fração recíproca $^1/_p$ e a ordem de 10 módulo p

Antes de enunciarmos uma proposição que relaciona o comprimento da expansão decimal de uma fração recíproca $^1/_p$ para $p > 5$ e a ordem de 10 módulo p, vamos considerar o Quadro 2, que nos dá todas as potências de a módulo 13, isto é, $a^k (mod\ 13)$, onde $1 \leq k \leq 12$.

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1
3	*9*	*1*	*3*	*9*	*1*	*3*	*9*	*1*	*3*	*9*	*1*
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	4	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

Quadro 2 – Ordens de a módulo 13
Fonte: Elaborado por Rubens Vilhena Fonseca (2022)

Pelo Quadro 2, verificamos que a ordem de 10 módulo 17 é $\varphi(17) = 16$, logo 10 é uma raiz primitiva de 17.

No Quadro 3, podemos ver que 10 não é uma raiz primitiva de 13, uma vez que a ordem de 10 módulo 13 é 6.

Agora, observe o tamanho dos períodos de ${}^{1}/_{13}$ e ${}^{1}/_{17}$. Eles são iguais à ordem de 10 módulo o denominador.

$$\frac{1}{17} = \overline{.0588235229411176 47}$$

$$\frac{1}{13} = \overline{.076923}$$

Os comprimentos dos períodos de ${}^{1}/_{17}$ e ${}^{1}/_{13}$ dividem, respectivamente, os valores de $\varphi(17)$ e $\varphi(13)$.

Para estabelecermos esse fato, provaremos a natureza da expansão decimal dos números racionais.

Lema1. Sejam a e n inteiros positivos, com $n > 1$ e MDC(a, n) = *1*. Seja$n = 2^{\alpha}5^{\beta}m$, com MDC(m, 10) = 1. Então, a expansão decimal de ${}^{a}/_{n}$ é periódica se, e somente se, $m > 1$. Além disso, se $m > 1$, o comprimento da parte não periódica é $\max\{\alpha, \beta\}$, enquanto o comprimento da parte periódica é igual a $\mathcal{O}_m(10)$.

Prova. A expansão decimal de a/n é finita se, e somente se, a/n é da forma $A/10^k$ para os inteiros A, $k > 0$, o que é verdade se, e somente se, $n \mid 10^k$. Essa última afirmação se mantém precisamente quando $m = 1$, e isso completa a primeira parte do lema.

Suponha que $n = 2^{\alpha}5^{\beta}.m$, com MDC($m$, 10) = 1 e $m > 1$. O conjunto dos elementos de $a.10^i (mod\, n)$ é cíclico, logo há, pelo menos, dois termos que devem ser iguais a módulo n. Se escolhermos o primeiro par desse tipo, digamos $a.10^s$ e $a.10^{s+l}$, então,

$$10^s \equiv 10^{s+l}\,(mod\, n) \quad (1),$$

uma vez que MDC(a, n) = 1. Como consequência, temos que,

$$10^l \equiv 1\,(mod\, m),$$

uma vez que o MDC(m, 10) = 1.

Da congruência (1), implica que $a.10^{s+k} \equiv a.10^{s+l+k}(mod\ n)$para cada $k \geq 0$, logo o comprimento do período será igual a:$l = \mathcal{O}_m(10)$.

Da congruência (1), vemos que $2^{\alpha}.5^{\beta}$ é divisível por 10^{s}, uma vez que cada valor é, relativamente, primo com $10^{l} - 1$. O menor valor s é igual ao max{3, 4}, e representa o comprimento da parte não periódica.

Em particular, o Teorema nos mostrou que, para primos $p > 5$ que têm 10 como raiz primitiva, o comprimento do período de $1/p$ será $\varphi(p)$. E, para os casos em que 10 não é uma raiz primitiva, o comprimento será: $\mathcal{O}_p(10)$.

Um resultado curioso, em Teoria dos Números sobre o período de uma dízima desse tipo de frações, foi demonstrado por Etienne Midy (1775-1846) em 1836.

Noves dentro – O Teorema de Midy

Pode-se ver, usando os Quadros1 e 2 como modelos, que a ordem de 10 módulo os primos 7, 11 e 19, por exemplo, são respectivamente $\varphi(7) = 6$, 2 e $\varphi(19) = 18$.E o tamanho de seus períodos tem os seguintes valores:

$$\frac{1}{7} = \overline{.142857}$$

$$\frac{1}{11} = \overline{.09}$$

$$\frac{1}{19} = \overline{.052631578947368421}.$$

Como todo primo maior que cinco é ímpar, $\varphi(p)$ será sempre um número par e, como a ordem de 10 módulo p divide $\varphi(p)$, essa ordem também sempre será par.

Em tais casos, se quebrarmos os dígitos do período ao meio, ou seja, em dois blocos de mesmo tamanho e os adicionarmos, ao que parece, obtemos um número com apenas 9's:

$$^1/_7 \to 142 + 857 = 999;$$

$$^1/_{13} \to 076 + 923 = 999;$$

$$^1/_{17} \to 05882352 + 94117647 = 99999999;$$

$$^1/_{19} \to 052\ 631\ 578 + 947\ 368\ 421 = 999999999.$$

Para seguirmos em frente, precisamos explicar a natureza da expansão decimal dos números racionais $^r/_p$ e de um conteúdo do Ensino Básico: Progressões Geométricas.

Progressões Geométricas infinitas e as dízimas de $^r/_p$

Consideremos a soma de uma Progressão Geométrica infinita de razão $0 < q < 1$ (LIMA *et al.*, 2016):

$$b + bq + bq^2 + bq^3 + \cdots = \frac{b}{1-q}.$$

Vamos aplicar esse resultado em $\frac{1}{13}$:

$$\frac{1}{13} = 0.\overline{076923} = \frac{76923}{10^6} + \frac{76923}{10^{12}} + \frac{76923}{10^{18}} + \cdots$$
$$= \frac{76923}{10^6}\left(1 + \frac{1}{10^6} + \frac{1}{10^{12}} + \cdots\right) = \frac{76923}{10^6\left(1 - \frac{1}{10^6}\right)} = \frac{76923}{10^6 - 1}.$$

De forma mais geral, se um decimal tem um período representado pelo número A de t dígitos, e esse período começa após s posições à direita da vírgula decimal, podemos escrever o decimal na forma:

$$\frac{n}{c} = P + \frac{Q}{10^s} + \frac{A}{10^{s+t}} + + \frac{A}{10^{s+2t}} + + \frac{A}{10^{s+3t}} + \cdots$$

$$= P + \frac{Q}{10^s} + \frac{1}{10^s}\left[\frac{A}{10^t} + \frac{A}{10^{2t}} + \frac{A}{10^{3t}} + \cdots\right]$$

$$= P + \frac{Q}{10^s} + \frac{1}{10^s} \cdot \frac{A}{10^t - 1}$$

Se $n < c$, a parte inteira P é zero; e se, além disso, o período do decimal começa após a vírgula decimal, então $s = 0$, e temos:

$$\frac{n}{c} = \frac{A}{10^t} + \frac{A}{10^{2t}} + \frac{A}{10^{3t}} + \cdots = \frac{A}{10^t - 1}.$$

Em seguida, faremos os desenvolvimentos matemáticos para mostrar que, quando um primo $p > 5$, tal que MDC$(p, 10) = 1$, $^n/_p$ é periódica, e seu período começa na vírgula decimal. Vamos considerar apenas frações adequadas; para $n > p$, temos $n = pq + r$, com $r < p$, então,

$$\frac{n}{p} = q + \frac{r}{p}.$$

O inteiro q precede a vírgula decimal, e segue a expansão $\frac{r}{p}$.

Vamos considerar $a = 10$. Se $p > 5$ é um primo, pelo *Pequeno Teorema de Fermat*:

$$a^{p-1} \equiv 1 (mod\ p) \Leftrightarrow 10^{p-1} \equiv 1 (mod\ p).$$

Isso nos diz que existe um inteiro k, tal que:

$$10^{p-1} - 1 = kp.$$

Tomando os recíprocos de ambos os termos e multiplicando por k, vem:

$$\frac{1}{p} = \frac{k}{10^{p-1} - 1},$$

$$\frac{r}{p} = \frac{rk}{10^{p-1} - 1}.$$

Como $r < p$, então $rk < 10^{p-1}$, logo rk tem no máximo $p - 1$ dígitos. Vê-se que o membro direito de $\frac{r}{p}$ é a soma da série geométrica:

$$\frac{r}{p} = \frac{kr}{10^{p-1}} + \frac{kr}{10^{2(p-1)}} + \frac{kr}{10^{3(p-1)}} + \cdots$$

que representa uma repetição decimal do bloco com $p - 1$ dígitos, representado pelo número *kr*. Assim, o comprimento do período da dízima de ${}^{r}/_{p}$ é $\varphi(p)$ ou um divisor de $\varphi(p)$.

Da mesma forma que deduzimos ${}^{r}/_{p}$ a partir do *Pequeno Teorema de Fermat*, obtemos:

Se l é um inteiro positivo tal que p divide $10^{l} - 1$, temos

$$\frac{r}{p} = \frac{P}{10^{l} - 1},$$

onde P é um inteiro positivo menor que 10^{l} para o qual a expansão de $\frac{r}{p}$ se repete após l dígitos.

Por outro lado, se a expansão de $\frac{r}{p}$ repete após l dígitos, então,

$\frac{r}{p} = \frac{A}{10^{l}-1}$ (onde A é o período da expansão $\frac{r}{p}$).

Desta forma,

$$pA = r(10^{l} - 1).$$

Como p não divide r, então p divide $10^{l} - 1$.

Concluímos que a expansão decimal de $^{r}/_{p}$ se repete após l dígitos se, e somente se, $10^{l} - 1$ é divisível por p. Em particular, o número de dígitos d no menor período de $^{r}/_{p}$ é o menor inteiro l tal que $10^{l} - 1$ é divisível por p.

Observe que o comprimento do período de $^{r}/_{p}$ depende apenas de p, não de r.

Estamos agora em condições de provar que a soma das metades dos blocos do período é um número composto apenas de 9's. Aqui assumimos que o período A da expansão decimal de $^{r}/_{p}$ com $p > 5$, tem um número igual, digamos $2d$, de dígitos:

$$\frac{r}{p} = 0,\overline{\alpha_1\alpha_2 \cdots \alpha_d\alpha_{d+1}\alpha_{d+2} \cdots \alpha_{2d}} = 0,A.$$

Escrevemos A na forma:

$$A = M.10^d + N, \quad N < 10^d, (1)$$

onde M e N são os números de d-dígitos que compõem as duas metades de A; queremos mostrar que $M + N = \underbrace{999 \dots 9}_{d\ dígitos} = 10^d - 1.$

A partir do que já vimos,

$$\frac{r}{p} = \frac{A}{10^{2d} - 1}, (2)$$

Logo,

$$pA = r(10^{2d} - 1) = r(10^d - 1)(10^d + 1).$$

Uma vez que $^{r}/_{p}$ é uma fração irredutível, p não divide r. Além disso, p não divide $10^d - 1$, pois, se o fizesse, o comprimento do período de $^{r}/_{p}$ seria d em vez de $2d$. O que nos prova que o comprimento do período é igual à ordem de 10 módulo p. Assim, o primo p divide $10^d + 1$. Usamos a representação (1) para escrever (2) na forma:

$$\frac{r}{p} = \frac{A}{10^{2d} - 1} = \frac{M10^d + N}{(10^d - 1)(10^d + 1)}.$$

De onde,

$$\frac{r(10^d + 1)}{p} = \frac{M.10^d + N}{10^d - 1} = \frac{M.10^d - M + M + N}{10^d - 1} =$$

$$= \frac{M\left(10^d - 1\right) + M + N}{10^d - 1} = M + \frac{M+N}{10^d - 1}. \quad (3)$$

O primeiro membro das equações (3) é um inteiro positivo porque p divide $10^d + 1$, portanto, o último membro é a soma de dois inteiros.

Os números M e N têm d dígitos cada, isto é,

$$0 < M + N \leq 10^d - 1 + 10^d - 1,$$

$$0 < M + N \leq 2(10^d - 1).$$

Então,

$$0 < \frac{M + N}{10^d - 1} \leq 2.$$

A igualdade só poderia ser válida se $M = N = 10^d - 1$, nesse caso, cada dígito em A seria 9; mas, então, o período teria um dígito que negaria a afirmação do comprimento do período ser par. E, como a expressão é um número inteiro, portanto, teremos:

$$\frac{M + N}{10^d - 1} = 1.$$

Assim,

$$M + N = 10^d - 1.$$

Provando que, de fato, a soma dos blocos do período das dízimas do tipo $^{r}/_{p}$ é um número com apenas 9's, resultado conhecido como *Teorema de Midy*.

Controle de convicções

O problema do tamanho do período de recíprocos de números primos e a soma dos blocos desses períodos tem sido objeto de intensas pesquisas em Teoria dos Números (GUPTA; SURY, 2005), desencadeando diversas pesquisas que permitem uma visão matemática cada vez mais aprofundada do assunto e as diversas ramificações que os pesquisadores matemáticos abordaram o problema. Assim finalizamos, apresentando conjecturas feitas por Gauss e Artin que, apesar dos avanços matemáticos, ainda não foram respondidas e quando um número primo divide um número *repunit.*

Gauss e Artin

Como todo primo possui, pelo menos, uma raiz primitiva (ROSEN, 2011), Emil Artin fez a seguinte conjectura em 1927:

> **Conjectura de Artin sobre raízes primitivas.** Se o inteiro $a \neq -1$ não é um quadrado perfeito, então é raiz primitiva para uma infinidade de primos (STEWART, 2015).

Ainda não se conhece nenhum número para o qual a conjectura seja verdadeira. Gauss já havia conjecturado, para o caso particular do número 10, que existem infinitos primos p tal que 10 é uma raiz primitiva de p. Em outras palavras, existem infinitos primos p tal que uma expansão na decimal de $^{1}/_{p}$ tem o período máximo $\varphi(p) = p - 1$?

O quadro 3 corresponde a uma tabela dos primos menores que 500 que tem 10 como raiz primitiva:

7,	17,	19,	23,	29,	47,	59,
61,	97,	109,	113,	131,	149,	167,
179,	181,	193,	223,	229,	233,	257,
263,	269,	313,	337,	367,	379,	383,
389,	419,	433,	461,	487,	491,	499.

Quadro 3 – Números primos menores que 500que tem 10 como raiz primitiva
Fonte: Elaborada pelos autores (2022)

As descobertas da matemática têm sido de suma importância para o crescimento e desenvolvimento da humanidade e contribuem para o entendimento de situações e problemas nos quais ela encontra-se envolvida. Logo, problemas em aberto nos mostram que a matemática continua a produzir desafios e que a solução deles pode vir a trazer novos benefícios aos serem humanos.

Repunits

Os *números repunits* (BEILER, 1964), conforme o próprio termo, em inglês, indica (*repunit number, rep + units, ou seja, repeated unit*), são números formados apenas por algarismos todos iguais a 1. Assim, os primeiros "repunits", são os seguintes:

$$1, 11, 111, 1111, 11111, 111111, \ldots$$

O termo "*repunit*" foi criado, em 1966, pelo matemático, ligado à Teoria dos Números, Albert H. Beiler, e consta no seu livro *Recreations in the Theory of Numbers.*

Um processo para se obter um desses números, atendendo à sua ordem *n*, será utilizar a seguinte expressão:

$$R_r = \frac{10^r - 1}{9}$$

Claro que a igualdade acima é valida para os múltiplos de *r.*

$$R_{nr} = \frac{10^{nr} - 1}{9}$$

Assim, se quisermos o número *repunit* com 5 dígitos iguais a 1, temos:

$$R_5 = \frac{10^5 - 1}{9} = \frac{99999}{9} = 11111.$$

Teorema. Para qualquer número primo $p > 5$, R_r que é divisível por p é aquele cujo r é igual $\varphi(p)$. Em símbolos,

$$p|R_r \Leftrightarrow r = \varphi(p),\ p > 5.$$

Para exemplificar, sabemos que $\varphi(13) = 12$.

Logo, $R_{12} = 111111111111$ é divisível por 13.

Uma prova é dada a seguir.

Prova. Seja $10^r - 1 = 9R_r$. Para um primo $p > 5$, considere que uma vez que $\text{MDC}(p, 10) = 1$, pelo *Pequeno Teorema de Fermat*, temos:

$10^{p-1} \equiv 1(mod\ p)$.

Então, $p|\left(10^{(p-1)} - 1\right)$, como $10^{(p-1)} - 1 = 9R_{(p-1)}$, logo, $p|9R_{(p-1)}$ e, sendo $\text{MDC}(9, p) = 1$, concluímos que $p|R_{(p-1).}$

Mas, 13 também divide $R_6 = 111111$. E 6 é o comprimento do período de $^1/_{13}$ que, como já vimos, é dado pela ordem de 13 módulo 10. Esse é um caso especial da prova dada acima. Assim, afirmamos que:

Corolário. Para qualquer número primo p> 5, R_r que é divisível por p é aquele cujo r é igual período l de $1/p$. Em símbolos,

$$p|R_r \Leftrightarrow r = l = \mathcal{O}_p(10), p > 5.$$

Prova. Sendo MDC*(*10, *r)*=1 e seguindo a prova dada para o Teorema, examinemos os $r + 1$ números 0, 9, 99, 999,..., $10^r - 1$ até que, pelo

Princípio da casa dos pombos[6], encontremos dois que são congruentes módulo r, digamos $10^j - 1 \equiv 10^k - 1 \ (mod\ r)$, então, $10^{j-k} \equiv 1 \ (mod\ r)$. Portanto, de fato $r|10^{j-k} - 1 = 999 \cdots 999$, isto é, *j-k noves*.

Usando o mesmo argumento do *Princípio da casa dos pombos* se prova que, se MDC(p, r) =1, então, existe algum inteiro $l \geq 1$ tal que $p^l \equiv 1(mod\ r)$. O menor l para o qual a congruência é verdadeira é chamado de *ordem* de a módulo r, denotado por $l = \mathcal{O}_p(10)$. Além disso, temos $p^k \equiv 1(mod\ r) \Leftrightarrow l|r$ (o que é equivalente a $l = \mathcal{O}_p(10)$).

Essas questões são apenas para encerrar e deixar o leitor curioso em investigar mais sobre o assunto. Abordaremos novamente essas questões relacionadas com as dízimas a partir de suas conexões com tópicos da Álgebra Abstrata em nosso próximo artigo.

Conclusão

Ao abordar as conexões entre Teoria dos Números e os conteúdos da Escola Básica, no contexto da teoria da resolução de problemas de Schoenfeld, foi necessário o conhecimento de recursos que incluem o procedimento de como identificar os períodos de dízimas do tipo $^r/_p$, $p > 5$ um primo e $r < p$, o significado dessa ação e os fundamentos matemáticos indispensáveis. Uma heurística importante foi apresentar algumas expansões decimais que permitiram perceber padrões e também foi uma estratégia de controle. Quanto à nossa convicção, ela se mostrou nas argumentações que foram ilustradas e construídas em vez de apenas colocadas axiomaticamente.

Schoenfeld reconhece que as heurísticas de resolução de problemas são, de fato, entidades pessoais que dependem do conhecimento prévio do

[6]O *Princípio da Casa dos Pombos* é um método de demonstração, também conhecido como *Princípio de Dirichlet*. Sua versão mais simples é a seguinte: “Se em n caixas são postos n + 1 pombos, então pelo menos uma caixa terá mais de um pombo.”

solucionador, como também a compreensão do problema em questão. Assim, os problemas que uma pessoa pode resolver, por meio de sua heurística pessoal, são finitos e limitados.

Sendo assim, é necessário que o educador seja capaz de fazer as interações entre os vários tipos e níveis de Matemática para seus alunos, de modo a ampliar suas heurísticas e provocar as curiosidades matemáticas que os motivem.

Referências

BEILER, A. H. **Recreations in the theory of numbers**. 2nd revised ed. New York: Dover Publications, 1964.

BURTON, D. M. **Teoria elementar dos números**. Tradução de Gabriela dos Santos Barbosa. 7. ed. Rio de Janeiro: LTC, 2016.

GUPTA, A.; SURY, B. Decimal Expansion of 1/p and Subgroup Sums. **Integers: Electronic Journal of Combinatorial Number Theory**, [*S. l.*], v. 5, A-19, p. 1-5, 2005.

LIMA, E. L. *et al.* **A Matemática do ensino médio**. 6. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006. Coleção do Professor de Matemática. 2. v.

LUPINACCI, M. L. V.; BOTIN, M. L. M. Resolução de problemas no ensino de matemática. *In*: ENCONTRO NACIONAL DE EDUCAÇÃO MATEMÁTICA, 8., 2004, Recife. **Educação Matemática:** um compromisso social. Recife: UFPE/Sociedade Brasileira de Educação Matemática, 2004.

ROSEN, K. H. **Elementary number theory**: and its applications. London: Pearson, 2011.

SANTOS, J. P. O. **Introdução à teoria dos números**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada/CNPq, 1998.

SCHOENFELD, A. **Mathematical problem solving**. New York: Academic Press, 1985.

STEWART, I. **Os mistérios matemáticos do professor Stewart**: resolvidos por Hemlock Soames e o dr. Watsup. 1. ed. Rio de Janeiro: Zahar, 2015.

VIEIRA, V. L. **Um curso básico em teoria dos números**. Campina Grande: EDUEPB/São Paulo: Livraria da Física, 2015.