Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

O Último Teorema de Fermat módulo um inteiro

Juliana Fernandes Pereira

Orientador: Prof. Dr. Angelo Calil Bianchi

São José dos Campos
Abril, 2019

PROFMAT

Título: *O Último Teorema de Fermat módulo um inteiro*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos

Abril, 2019

Pereira, Juliana Fernandes

O Último Teorema de Fermat módulo um inteiro, Juliana Fernandes Pereira – São José dos Campos, 2019.

viii, 42f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Fermat's Last Theorem modulo an integer

1. Último Teorema de Fermat. 2. Último Teorema de Fermat módulo um inteiro. 3. Resolução de congruências.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe do Departamento:
Prof. Dr. Eduardo Antonelli

Coordenador do Programa de Pós-Graduação:
Prof. Dr. Angelo Calil Bianchi

JULIANA FERNANDES PEREIRA

O ÚLTIMO TEOREMA DE FERMAT MÓDULO UM INTEIRO

Presidente da banca: Prof. Dr. Angelo Calil Bianchi

Banca examinadora:

Profa. Dra. Grasiele Cristiane Jorge

Prof. Dr. Marcelo Cristino Gama

Prof. Dr. Samuel Augusto Wainer

Data da Defesa: 15 de Abril de 2019

Aqueles que semeiam com lágrimas, com cantos de alegria colherão. Sl. 126:5.

AGRADECIMENTOS

Não há palavras que possam expressar a alegria que há em meu coração! Glória a Deus que em sua infinita graça e criatividade realizou o sobrenatural de uma forma tão natural e chamou a existência coisas que não existiam, como se já existissem. Mais uma vez Deus realizou muito mais do que eu imaginava e me permitiu conquistar mais essa vitória que, com certeza, não poderia ser obtida sozinha. Por isso, quero expressar um pouco da minha gratidão as pessoas que me auxiliaram nessa conquista.

Agradeço a Deus, meu senhor Jesus Cristo, que me sustenta com a destra de Sua justiça e me cerca com Sua infinita misericórdia, pela salvação da minha alma e a mais essa conquista. Graças a Ele mais essa vitoria foi possível, foi Ele quem me sustentou, deu-me sabedoria e graça para alcançá-la. Não há como negar: Deus me surpreende com infinitas bênçãos que nem sei contar. Esta conquista foi uma delas.

Agradeço muito a minha mãe por estar sempre presente em minha vida, por contribuir sempre para meu crescimento pessoal e profissional, por sempre estar ao meu lado em minhas decisões, por vibrar em meus momentos de conquistas, por me aconselhar a não desistir nas dificuldades. Pelas suas orações e súplicas pela minha vida porque tenho certeza de que seus joelhos dobrados me mantiveram de pé. Pelo exemplo de vida, coragem e determinação não me esquecendo do cuidado, carinho, dedicação e compreensão em todos os momentos. Ao meu pai pelo carinho e apoio. À minha irmã, pelo estímulo, carinho, compreensão, amizade e por ter sido a ponte para que eu chegasse aqui. A presença deles em minha vida foi, indubitavelmente, fundamental para mais essa conquista. Eles são presentes de Deus para mim.

Ao professor Dr. Angelo Calil Bianchi pela ajuda, acompanhamento, orientação e estímulo durante a elaboração desse trabalho.

A todos os professores do curso PROFMAT pela paciência e pelas experiências fornecidas.

Aos colegas de turma, pelas alegrias, pela cumplicidade e por tornar minhas sextas-feiras mais leves. Vocês partilharam dos meus anseios tornando-se cúmplices de cada momento. Tenham certeza de que permanecerão em minha mente e coração.

À CAPES pelo apoio financeiro para que pudesse completar essa jornada.

A todas as outras pessoas que contribuíram direta ou indiretamente para a realização desse trabalho e, embora seus nomes não apareçam na relação do agradecimento, foram muito importantes para a realização deste trabalho. A todos deixo registrado aqui minha imensa gratidão e meu “muito obrigada!”.

RESUMO

Este trabalho apresenta o Último Teorema de Fermat na sua versão modular. A explanação inicial é uma abordagem histórica do Último Teorema de Fermat, discorrendo sobre casos específicos até o caminho para sua completa demonstração. Em seguida, explora-se e apresenta-se alguns resultados obtidos do estudo deste teorema quando apresentado na versão módulo um número inteiro, o qual se trata de um assunto pouco conhecido mas completamente explorado. Por fim, apresenta-se uma sequência didática para trabalhar conceitos de aritmética relacionados com o Último Teorema de Fermat e o Último Teorema de Fermat modulo um número inteiro (não em suas formas gerais) para alunos das séries finais do Ensino Fundamental e Médio, baseando-se no ensino de Matemática através de problemas e de sua história.

Palavras-chave: 1. Último Teorema de Fermat. 2. Último Teorema de Fermat módulo um inteiro. 3. Resolução de congruências.

ABSTRACT

This work presents the Last Fermat's Theorem in its modular version. The initial explanation is a historical approach to the Last Fermat's Theorem, an overview on some particular cases and the path to its complete proof. Then, one explore and present some results obtained from the study of this theorem when it is considered modulo an integer number, which is a little known subject but completely explored. Finally, it presents a teaching plan to work arithmetic concepts related to the Last Fermat's Theorem and to the Last Fermat's Theorem modulo an integer number (not in general form) for students at the final years of Elementary and High School, with historical and modeling approach.

Keywords: 1. Fermat's Last Theorem. 2. Fermat's Last Theorem modulo an integer. 3. Resolution of congruences.

SUMÁRIO

INTRODUÇÃO

Ao estudar a história da Matemática podemos encontrar grandes nomes que, de maneira particular e única, deixaram seu legado de conhecimento e contribuição. Um destes nomes é *Pierre de Fermat*, matemático francês que influenciou diversos ramos da Matemática. O que mais chamava a atenção de Fermat é o ramo da Matemática chamado Teoria dos Números, onde se encontra o objeto de estudo deste trabalho.

Nascido em Beaumont de Lomagne, em agosto de 1601, Fermat era filho de comerciantes com uma privilegiada condição financeira, tendo a oportunidade de estudar. Fermat estudou no monastério franciscano e graduou-se em direito na universidade de Orléans. Aos 30 anos de idade, tornou-se Conselheiro do Parlamento de Toulouse e Conselheiro na Câmara dos Requerimentos, atividade que exerceu como profissão. Nas horas livres, dedicava-se com veemência à Matemática, com assuntos relacionados ao que conhecemos como cálculo infinitesimal, geometria analítica e teoria da probabilidade, e com grande dedicação e apreço para a Teoria dos Números. Segundo [12], seu interesse por essa área provavelmente foi desencadeado pela tradução latina do livro de *Aritmética de Diofanto*, feita por *Bachet*, pois diversas de suas descobertas e contribuições foram feitas por meio de anotações nas margens da sua cópia deste livro.

Uma de suas contribuições é o teorema enunciado por ele, em torno de 1637, com as seguintes palavras: *"Dividir um cubo em dois cubos, uma quarta potência ou, em geral uma potência qualquer em duas potências da mesma denominação acima da segunda é impossível"*, de acordo com [4]. Este teorema é conhecido hoje como *O Último Teorema de Fermat*. Em linguagem matemática, podemos enunciar esse teorema da seguinte forma:

A equação $X^n + Y^n = Z^n$***, com*** $n \in \mathbb{N}$***,*** $n \geq 3$***, no conjunto dos números inteiros*** $\mathbb{Z}$ ***só admite soluções triviais.***

Alguns matemáticos demostraram a validade desse teorema para casos isolados de n. O próprio Fermat, em algumas de suas anotações deixou a demonstração para o caso com $n = 4$. Em 1753, *Euler*, outro gigante da Matemática, provou o resultado para o caso $n = 3$ e, em 1825, *Legendre* e *Dirichlet* conseguiram demonstrar o resultado isoladamente para o caso $n = 5$. O caso $n = 7$ foi provado por *Lamé*, em 1839.

A prova completa desse teorema foi realizada em 1995 por *Andrew Wiles*, professor da Universidade de Princeton, ao provar a *Conjectura de Taniyama-Shimura* sobre curvas elípticas. Isto se deu após mais de 350 anos do apontamento de Fermat.

Assim como é para muitos matemáticos, o Último Teorema de Fermat é uma inspiração para este trabalho, em sua forma, não em sua raramente compreendida demonstração. O objetivo central deste trabalho é discutir alguns aspectos relacionados a este teorema em sua versão modular (ou módulo um inteiro), do ponto de vista puramente aritmético, para

alguns casos particulares e concluir com o teorema que garante a existência de soluções para congruência a primos específicos, explorando e desenvolvendo algumas ferramentas básicas de aritméticas e coloração de grafos.

Este trabalho está estruturado da seguinte forma: nas preliminares do trabalho apresentamos os conceitos aritméticos de inteiros *módulo m* e resolução de congruências, os quais são pertencentes à teoria dos números e essenciais para a compreensão do conteúdo restante. O segundo capítulo é uma apresentação da parte histórica e dos desenvolvimentos acerca do Último Teorema de Fermat. No terceiro capítulo, que é a parte central e de conteúdo matemático diferenciado, apresentamos a formulação do problema na versão modular, algumas explorações de casos particulares e uma breve discussão sobre a existência de solução sob condições na congruência. No capítulo seguinte, apresentamos o respaldo teórico-metodológico sobre a importância do ensino de Matemática através da sua história e da resolução de problemas e as metodologias empregadas na proposta didática. Por último, apresentamos uma proposta didática que explora os conceitos básicos abordados.

As referências nas quais este trabalho se respalda são: [4] e [12] para a parte histórica; [5] para a parte de Teoria dos Números; [9], [13], [14] e [6] para a parte específica da versão modular do Teorema de Fermat, cuja referência original acerca do assunto remete a [11]; [3], [7] e [10] para a apresentação da metodologia didática e [2] para proposta didática.

1

PRELIMINARES

Neste capítulo apresentaremos o conceito de congruências módulo um inteiro e resolução de congruências, bem como suas propriedades, essenciais para a compreensão do conteúdo principal deste trabalho.

1.1 INTEIROS MÓDULO M

De uma maneira bem simples, podemos dizer que a ideia de congruência módulo um inteiro está relacionada ao resto da divisão de um número por este inteiro. Pelo algoritmo da divisão de Euclides, os possíveis restos r da divisão de um número inteiro a por um inteiro m são precisamente os números r tais que $0 \leq r < m$. Assim, todo número natural a está associado, pelo resto de sua divisão por m, a um, e somente um, dos números $0, 1, \ldots, m-1$.

Definição 1.1. *Dados $a, b, m \in \mathbb{Z}$ e $m \geq 1$, dizemos que a e b são congruentes módulo m se os restos da divisão euclidiana de a e b por m forem iguais. Nesse caso, a representação é a que segue:*

$$a \equiv b \mod m \quad \textit{ou, simplesmente,} \quad a \equiv_m b.$$

Quando a e b não são congruentes módulo m representamos por:

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

Exemplo 1.2. $9 \equiv 14 \mod 5$ *pois os restos da divisão de 9 e de 14 por 5 são iguais, ou seja, resto 4.* $18 \not\equiv 41 \mod 6$ *pois os restos da divisão de 18 e de 41 por 6 são diferentes.*

As congruências módulo um inteiro apresentam as seguintes propriedades imediatas:

Proposição 1.3. *Seja $a, b, m \in \mathbb{Z}$ e $m \geq 1$, temos:*

1. *Reflexiva: $a \equiv a \mod m$;*
2. *Simétrica: se $a \equiv b \mod m$, então $b \equiv a \mod m$;*
3. *Transitiva: se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$.* □

Para averiguar se a é congruente a b módulo m não é necessário efetuar ambas as divisões. Para essa validação, basta utilizar da seguinte condição:

Proposição 1.4. *Dados $a, b, m \in \mathbb{Z}$, com $m \geq 1$, temos $a \equiv b \mod m$ se, e somente se, m divide $a - b$.*

Demonstração. Pelo algoritmo da divisão euclidiana, podemos escrever $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Assim, $a - b = m(q_1 - q_2) + (r_1 - r_2)$. Como $0 \leq r_1 - r_2 < m$, m divide $a - b$ se, e somente se, $r_1 - r_2 = 0$, para isso devemos ter $r_1 = r_2$. □

A notação de congruência é uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme a proposição a seguir.

Proposição 1.5. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m \geq 1$. Temos:*

1. *Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.*

2. *Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $ac \equiv bd \mod m$.*

Demonstração. Se $a \equiv b \mod m$ e $c \equiv d \mod m$, pela proposição anterior $m|(b-a)$ e $m|(d-c)$. Então,

1. $m|[(b-a)+(d-c)]$. Como a soma de números inteiros apresenta as propriedades comutativa e associativa, podemos escrever $m|[(b+d)-(a+c)]$, o que equivale a $a + c \equiv b + d \mod m$.

2. $m|[d(b-a)]$ e $m|[a(d-c)]$ e segue que $m|[d(b-a)+a(d-c)]$, o que é equivalente a $m|[bd-ac]$ e, ainda pela Proposição 1.4, $ac \equiv bd \mod m$.

□

Corolário 1.6. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \mod m$, então $a^n \equiv b^n \mod m$.* □

As propriedades a seguir referem-se a regra do cancelamento para as congruências.

Proposição 1.7. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos:*

1. *$a + c \equiv b + c \mod m \Leftrightarrow a \equiv b \mod m$.*

2. *$ac \equiv bc \mod m \Leftrightarrow a \equiv b \mod \frac{m}{mdc(c,m).}$*

Demonstração. 1. Se $a + c \equiv b + c \mod m$, então $m|[(b+c)-(a+c)]$ e, pelas propriedades da adição com inteiros, $m|[b-a]$, ou seja, $a \equiv b \mod m$. Por outro lado, se $a \equiv b \mod m$, segue pela Proposição 1.5, item 1, que $a + c \equiv b + c \mod m$, uma vez que $c \equiv c \mod m$.

2. Como a congruência $ac \equiv bc \mod m$ pode ser escrita como $m|(b-a)c$, temos

$$m|(b-a)c \Leftrightarrow \frac{m}{mdc(c,m)} \mid (b-a)\frac{c}{mdc(c,m)} \Leftrightarrow \frac{m}{mdc(c,m)} \mid (b-a),$$

pois $\frac{m}{mdc(c,m)}$ e $\frac{c}{mdc(c,m)}$ são coprimos. Logo, $a \equiv b \mod \frac{m}{mdc(c,m)}$.

□

Para a operação de multiplicação ainda podemos apresentar as seguintes propriedades também imediatas:

Proposição 1.8. *Sejam $a, b, m, n, m_1, \ldots, m_r \in \mathbb{Z}$. Temos:*

1. *Se $a \equiv b \mod m$ e $n|m$, então $a \equiv b \mod n$.*
2. *$a \equiv b \mod m_i, \forall\ i = 1, \ldots, r \Leftrightarrow a \equiv b \mod mmc(m_1, \ldots, m_r)$.*
3. *Se $a \equiv b \mod m$, então $mdc(a, m) = mdc(b, m)$.* □

1.2 FUNÇÃO FI DE EULER $\Phi(m)$

Definição 1.9. *Sistema completo de resíduos modulo m, $m \geq 1$, é um conjunto de números inteiros cujos restos pela divisão por m são todos os números $0, 1, \ldots, m-1$, sem repetição de restos e em uma ordem qualquer.*

Definição 1.10. *Sistema reduzido de resíduos módulo m, $m \geq 1$, um conjunto de números inteiros $r_1, \ldots, r_s$ que satisfazem as seguintes condições:*

1. *$mdc(r_i, m) = 1$, para todo $i = 1, \ldots, s$;*
2. *$r_i \not\equiv r_j \mod m$, se $i \neq j$;*
3. *Para cada $n \in \mathbb{Z}$ tal que $mdc(n, m) = 1$, existe i tal que $n \equiv r_i \mod m$.*

Exemplo 1.11. *O conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ é um sistema completo de resíduos módulo 12 e $B = \{1, 5, 7, 11\}$ é um sistema reduzido de resíduos módulo 12.*

Observe que um sistema completo de resíduos módulo m sempre possui m elementos e, dado um sistema completo de resíduos módulo m, basta eliminarmos os elementos que possuem divisores comuns com m para obtermos um sistema reduzido de resíduos módulo m.

Exemplo 1.12. *Dado o sistema completo de resíduos $\{8, 9, 10, 11, 12, 13, 14, 15\}$ módulo 8, basta retirarmos os números $8, 10, 12, 14$, pois possuem divisores comuns com 8 para obtermos um sistema reduzido de resíduos módulo 8, ou seja, o conjunto $\{9, 11, 13, 15\}$.*

Definição 1.13. *Seja m um inteiro positivo, definimos como função fi de Euler, denotada como $\Phi(m)$, a função $\Phi : \mathbb{N} \longrightarrow \mathbb{N}$, tal que $\Phi(1) = 1$ e, para $m \geq 2$, associa m ao número de elementos do sistema reduzido de resíduos módulo m.*

Note, pela definição, que $\Phi(m) \leq m - 1$, para todo $m \geq 2$, e $\Phi(m) = m - 1$ se, e somente se, m for um primo.

O cálculo da função $\Phi(m)$, a partir da fatoração em primos de m, depende de duas propriedades fundamentais que precisam ser estabelecidas:

Proposição 1.14. *1. Sejam $m, m' \in \mathbb{N}$ tais que $mdc(m, m') = 1$. Então,*

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

Em outras palavras, a função Fi é multiplicativa quando $mdc(m, m') = 1$.

2. Se p é um número primo e r um número natural, então temos

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

□

Exemplo 1.15. *Vejamos com exemplo o cálculo de $\Phi(6)$ e $\Phi(8)$.*

1. *Como $mdc(2, 3) = 1$, $\Phi(6) = \Phi(2.3) = \Phi(2).\Phi(3) = 2.1 = 2$. O que é facilmente verificado pela citação dos elemento do conjunto do sistema reduzido de resíduos módulo 6, que é o conjunto $\{1, 5\}$ que possui 2 elementos.*

2. *Como $8 = 2^3$, $\Phi(8) = \Phi(2^3) = 2^3 - 2^{3-1} = 8 - 4 = 4$, que são os elementos do conjunto $\{1, 3, 5, 7\}$.*

O teorema a seguir enuncia um resultado interessante para congruências envolvendo potências de números inteiros:

Teorema 1.16. *(Teorema de Euler) Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $mdc(a, m) = 1$. Então,*

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

□

Como consequência desse teorema, podemos enunciar o *Pequeno Teorema de Fermat*, o qual possui, também, demonstrações independentes do Teorema de Euler.

Teorema 1.17. *(Pequeno Teorema de Fermat) Se p é um número primo e $a \in \mathbb{Z}$, então*

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

Alem disso, se p não divide a, então

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

□

Exemplo 1.18. *Sejam $a = 5$ e $p = 3$. Temos $5^3 = 125 \equiv 5 \mod 3$ e, como 3 não divide 5, também temos $5^{3-1} = 5^2 = 25 \equiv 1 \mod 3$.*

As demostrações omitidas nessa seção, por não serem alvo primordial deste trabalho, podem ser encontradas em [5].

1.3 FUNÇÃO E NÚMERO DE CARMICHAEL

Vimos na seção anterior que se p é primo e não divide a, então $a^{p-1} \equiv 1 \mod p$. Contudo, há números compostos que satisfazem a mesma condição para alguma base $a \in \mathbb{Z}$.

Definição 1.19. *Seja $a, n \in \mathbb{Z}$ e n um número composto tal que $a^{n-1} \equiv 1 \mod n$ para algum a, então n é chamado de pseudoprimo de Fermat na base a.*

Exemplo 1.20. *O número 341 é um pseudoprimo na base 2, pois se tomarmos $a = 2$ e $n = 341$, o qual é um número composto pois $341 = 11 \cdot 31$, temos $2^{340} \equiv 1 \mod 341$, visto que $2^{10} \equiv 1 \mod 341$. Por outro lado, se tomarmos $a = 3$ e $n = 341$ a congruência $a^n \equiv 1 \mod n$ não é válida, uma vez que $3^{340} \equiv 56 \mod 341$.*

Fica evidente que existem números que não são pseudoprimos para todas as bases conforme a definição a seguir.

Definição 1.21. *Sejam $n, a \in \mathbb{Z}$ e n um número composto ímpar. Se $a^{n-1} \equiv 1 \mod n$ para todo $1 < a < n$, onde a é um número coprimo com n, dizemos que n é um número de Carmichael.*

O menor número de Carmichael é 561. Para verificarmos isso, seria necessário provar que $a^{560} \equiv 1 \mod 561$ para todo $a = 2, 3, \ldots, 560$ coprimo com 561, o que tornaria a prova bem trabalhosa. Mas, o teorema a seguir nos mostra uma forma bem mais simples de verificar se um número satisfaz a condição do número de Carmichael. A demonstração será omitida por não conter método ou técnica necessários ao que se segue, porém esta e as demais demonstrações dessa seção podem ser encontradas em [8].

Teorema 1.22. *(Teorema de Korselt) Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz:*

1. *p^2 não divide n;*
2. *$p - 1$ divide $n - 1$.* □

Exemplo 1.23. *O número $561 = 3 \cdot 11 \cdot 17$ é um número de Carmichael, pois*

- *3^2 não divide 561, $3 - 1 = 2$ e $2 \mid 560$,*
- *11^2 não divide 561, $11 - 1 = 10$ e $10 \mid 560$,*
- *17^2 não divide 561, $17 - 1 = 16$ e $16 \mid 560$.*

Definição 1.24. *Seja n um inteiro positivo, definimos como função de Carmichael, denotada como $\lambda(n)$, a função $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ que associa n ao menor número inteiro positivo $\lambda(n) = m$ para o qual todo $a \in \mathbb{N}$ coprimo com n satisfaz $a^m \equiv 1 \mod n$.*

Observe que essa função está bem definida devido a existência do número $\Phi(n)$ com tal propriedade e o Princípio da Boa Ordenação[1].

Exemplo 1.25. *$\lambda(14) = 6$, pois $3^6 \equiv 1 \mod 14$, $5^6 \equiv 1 \mod 14$, $9^6 \equiv 1 \mod 14$, $11^6 \equiv 1 \mod 14$ e $13^6 \equiv 1 \mod 14$.*

O cálculo da função $\lambda(n)$, com $n \in \mathbb{N}$, a partir da fatoração de n em números primos, apresenta as seguintes proposições:

Proposição 1.26. *Seja $p, k \in \mathbb{N}$, p primo. Temos:*

1. *$\lambda(p^k) = (p-1)p^{k-1}$, se $k \geq 2$;*
2. *$\lambda(p_1^{k_1}.p_2^{k_2}\dots p_r^{k_r}) = mmc(\lambda(p_1^{k_1}), \lambda(p_2^{k_2})\dots\lambda(p_r^{k_r}))$, onde $p_1, p_2, \dots, p_r$ são primos distintos da fatoração de n e $k_1, k_2, \dots, k_r \in \mathbb{N}$.* □

Exemplo 1.27. *$\lambda(6) = 2$, pois $6 = 2 \cdot 3$ e $\lambda(2 \cdot 3) = mmc(\lambda(2), \lambda(3)) = mmc(1, 2) = 2$. Assim, para todo número natural a, coprimo com 6, temos $a^2 \equiv 1 \mod 6$.*

1.4 RESOLUÇÃO DE CONGRUÊNCIAS

Seja $f(X_1, \dots, X_r)$ um polinômio com coeficientes inteiros nas variáveis $X_1, \dots, X_r$. Resolver a congruência $f(X_1, \dots, X_r) \equiv 0 \mod m$ é determinar, se existirem, os números inteiros $x_1, \dots, x_r$, tais que $f(x_1, \dots, x_r) \equiv 0 \mod m$. Pelas propriedades da congruência módulo m, se $a \in \mathbb{Z}$ é solução da congruência $f(x) \equiv 0 \mod m$, então também será qualquer outro inteiro a' congruente a a, o que chamamos de *classes de congruências*. Assim, se $a \equiv a' \mod m$ e $f(a) \equiv 0 \mod m$, então $f(a') \equiv 0 \mod m$.

Definição 1.28. *Solução da congruência $f(X_1, \dots, X_r) \equiv 0 \mod m$ é um conjunto de todas as classes de congruência módulo m que satisfazem a congruência.*

Exemplo 1.29. *Considere a congruência $8X \equiv 4 \mod 12$. Por inspeção, as classes de soluções para essa congruência são $2, 5, 8$ e $11 \mod 12$. Observe ainda que nem sempre a congruência possui soluções, como é o caso da congruência $x^2 - x + 1 \equiv 0 \mod 2$ já que, para todo o inteiro a, temos $a^2 \equiv a \equiv 1 \mod 2$ ou $a^2 - a \equiv 0 \mod 2$ e, portanto, $a^2 - a + 1 \equiv 1 \mod 2$.*

Definição 1.30. *O grau de uma congruência $f(x) \equiv 0 \mod m$ é igual ao maior expoente de f tal que m não divide o respectivo coeficiente.*

Exemplo 1.31. *Por exemplo, a congruência $x^3 - x + 1 \equiv 0 \mod 2$ tem grau 3, enquanto que a congruência $3x^4 - x^2 + 2 \equiv 0 \mod 3$ tem grau 2.*

Teorema 1.32. *Sejam p um número primo e $f(x) \equiv 0 \mod p$ uma congruência de grau n, então esta congruência tem no máximo n soluções.*

[1] Termo encontrado, por exemplo, em [5]

Demonstração. A demonstração é feita por indução em n. Para $n = 0$, $f(x) = a_0$, $a_0 \in \mathbb{Z}$ e, por hipótese, p não divide a_0, logo a congruência $f(x) \equiv 0 \mod p$ não tem soluções. Agora, seja $n \in \mathbb{N}$ e suponha que o número de soluções de qualquer congruência polinomial módulo p com grau igual ou inferior a n é, no máximo, igual a n. Vamos provar que o resultado é válido para $n + 1$.

Suponha $f(x) = a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$, com $p \nmid a_{n+1}$, e que a congruência $f(x) \equiv 0 \mod p$ tenha mais que $n + 1$ soluções, ou seja, existem $x_1, x_2, \ldots, x_{n+1}, x_{n+2} \in \mathbb{Z}$ verificando $f(x) \equiv 0 \mod p$ tais que $x_i \not\equiv x_j \mod p$, se $i, j \in \{1, 2, \ldots, n + 2\}$ são distintos.

Considere o polinômio não nulo $g(x) = f(x) - a_{n+1}(x - x_1)(x - x_2)\ldots(x - x_{n+1})$ e observe que seu grau é igual ou inferior a n. Além disso, para $i = 1, 2, \ldots, n + 1$, temos $g(x_i) = f(x_i) \equiv 0 \mod p$ e, assim, $g(x) \equiv 0 \mod p$ é uma congruência de grau igual ou inferior a n que admite pelo menos $n + 1$ soluções, o que contradiz a hipótese de indução. Logo, $f(x) \equiv 0$ tem, no máximo, $n + 1$ soluções.

□

Exemplo 1.33. *A congruência* $x^3 - x + 1 \equiv 0 \mod 2$ *tem grau* 3 *e, assim, pode ter até* 3 *soluções, enquanto que a congruência* $3x^4 - x^2 + 2 \equiv 0 \mod 3$ *tem grau* 2 *e possui no máximo* 2 *soluções.*

2

O ÚLTIMO TEOREMA DE FERMAT

O *Último Teorema de Fermat* trata de uma equação, denominada Equação de Fermat, cuja busca por soluções inteiras intrigou gerações de matemáticos. A equação em questão é

$$X^n + Y^n = Z^n,$$

com $n \in \mathbb{N}$, onde X, Y e Z são incógnitas algebricamente independentes. O conjunto solução S desta equação, no âmbito da Aritmética, é estudado entre os números inteiros, isto é,

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid x^n + y^n = z^n\} \subset \mathbb{Z}^3.$$

Definição 2.1. *Seja a trinca de inteiros (x, y, z) solução da equação $X^n + Y^n = Z^n$, com $n \in \mathbb{N}$. Se uma de suas entradas for igual a zero, então a trinca é chamada solução trivial e quando suas entradas não possuem fator comum a trinca será chamada de trincas primitivas.*

Evidentemente que esta equação possui infinitas soluções inteiras triviais para qualquer $n \in \mathbb{N}$. Por exemplo,

- as trincas da forma $(0, a, a)$ e $(a, 0, a)$, $a \in \mathbb{Z}$, são soluções para qualquer $n \in \mathbb{N}$;
- as trincas $(0, a, -a)$ e $(-a, 0, a)$, $a \in \mathbb{Z}$, são soluções para $n \in \mathbb{N}$ par;
- as trincas $(a, -a, 0)$ ou $(-a, a, 0)$, $a \in \mathbb{Z}$, são soluções para $n \in \mathbb{N}$ ímpar.

Além disso, se $(x, y, z) \in \mathbb{Z}^3$ é uma solução da Equação de Fermat, então $(cx, cy, cz), c \in \mathbb{Z}$, também será. Entretanto, estas trincas carregam consigo um certo "imediatismo" e não são as trincas que realmente desejamos investigar propriedades.

Agora podemos enunciar o Último Teorema de Fermat de maneira precisa:

A equação $X^n + Y^n = Z^n$, com $n \in \mathbb{N}$, $n \geq 3$, só admite soluções inteiras triviais.

Nas próximas seções serão apresentados os resultados obtidos nas tentativas de se demonstrar este teorema (enquanto ainda era conjectura), feitos para casos específicos de $n \in \mathbb{N}$. O caso $n = 1$ é bastante simples e o caso $n = 2$ é algo muito anterior a Fermat, como veremos a seguir.

2.1 O CASO $n = 1$: PONTOS INTEIROS EM UM PLANO

O caso $n = 1$ resulta na equação

$$X + Y = Z,$$

com X, Y e $Z \in \mathbb{Z}$, cujas soluções são as infinitas trincas da forma $(x, y, x + y) \in \mathbb{Z}^3$. Observe que esta equação determina um plano em $\mathbb{R}^3$, o plano $X + Y - Z = 0$ e, portanto, as soluções da Equação de Fermat são pontos deste plano que possuem todas as coordenadas inteiras.

2.2 O CASO $n = 2$: O TEOREMA DE PITÁGORAS

No caso $n = 2$ obtemos a conhecida equação

$$X^2 + Y^2 = Z^2,$$

com X, Y e $Z \in \mathbb{Z}$. Esta equação é conhecida por compor o *Teorema de Pitágoras*, o qual estabelece a relação entre os lados de um triângulo retângulo. Pitágoras, uma das mais influentes mentes matemáticas, estudou as trincas que solucionavam esta equação e obteve parte do seu conjunto solução:

$$\left\{(x, y, z) \in \mathbb{Z}^3 \ : \ x = \frac{n^2 - 1}{2}, y = n, z = \frac{n^2 + 1}{2}, \text{ com } n \in \mathbb{Z} \text{ ímpar } \right\}.$$

De acordo com [5], esse conjunto, entretanto, não abrangia todas as soluções. Posteriormente, Euclides provou que as soluções dessa equação podem ser expressas de modo único, a menos da ordem de x e y, por

$$\Big\{(x, y, z) \in \mathbb{Z}^3 \mid x = n^2 - m^2, y = 2nm, z = n^2 + m^2, \text{ com } n, m \in \mathbb{Z},$$

$$n \geq m, \ mdc(m, n) = 1 \text{ e } m \text{ e } n \text{ com paridades distintas}\Big\}.$$

Exemplo 2.2. *Seja $m = 1$ e $n = 2$ temos como uma solução da equação $X^2 + Y^2 = Z^2$ a trinca $(3, 4, 5)$.*

2.3 OS CASOS NECESSÁRIOS PARA SE CHEGAR AO CASO GERAL

Devido ao Teorema Fundamental da Aritmética, todo número natural n é da forma $n = 2^a p_1^{r_1} \dots p_s^{r_s}$, onde $p_1, \dots, p_s$ são números primos ímpares distintos, $a, r_1, \dots, r_s \in \mathbb{N} \cup \{0\}$, $s \in \mathbb{N} \cup \{0\}$. Assim, qualquer número natural n maior que 2 é divisível por 4 ou por um número primo ímpar, ou seja, n é da forma $4k$ ou pk, com $k \in \mathbb{N}$ e p um

número primo ímpar. Com isso, a Equação de Fermat $X^n + Y^n = Z^n$ para $n > 2$ pode ser reescrita em uma das formas

$$X^{4k} + Y^{4k} = Z^{4k} \quad \text{ou} \quad X^{pk} + Y^{pk} = Z^{pk}.$$

Observe que a equação $X^{4k} + Y^{4k} = Z^{4k}$ pode ser reescrita como $(X^k)^4 + (Y^k)^4 = (X^k)^4$. Desse modo, para qualquer trinca (x, y, z) que satisfaz a equação $X^{4k} + Y^{4k} = Z^{4k}$, a trinca (x^k, y^k, z^k) será solução da equação $X^4 + Y^4 = Z^4$. Logo, se $X^{4k} + Y^{4k} = Z^{4k}$ possuir solução não trivial, então a equação $X^4 + Y^4 = Z^4$ também possui. Assim, se $X^4 + Y^4 = Z^4$ não possuir solução não trivial, então $X^{4k} + Y^{4k} = Z^{4k}$ também não possui. Analogamente, se $X^p + Y^p = Z^p$ não possuir solução não trivial, então $X^{pk} + Y^{pk} = Z^{pk}$ também não possui. Portanto, para provar que a equação de Fermat não possui soluções não triviais para $n \geq 3$ basta provar que estas não existem para os casos $n = 4$ e para n sendo um número primo ímpar.

Resumidamente, o Último Teorema de Fermat se torna equivalente (reduzido) ao seguinte:

Teorema 2.3. *A Equação de Fermat não possui solução não trivial para $n \in \mathbb{N}$, com $n = 4$ ou n um número primo ímpar.* □

Nas próximas seções deste capítulo nos respaldamos em [12] e apresentamos os caminhos de alguns matemáticos até chegar à demonstração do Último Teorema de Fermat.

2.4 O CASO $n = 4$: A EQUAÇÃO BIQUADRÁTICA

A demonstração desse caso foi feita por Fermat ao provar que a equação $X^4 + Y^4 = Z^2$ não apresenta soluções não triviais. Fermat se deparou com equações do tipo $X^4 + Y^4 = Z^2$ quando estudava a área de um triângulo pitagórico, ou seja, um triangulo retângulo cujos lados são números inteiros, a fim de verificar se esta poderia ser um quadrado perfeito. Fermat provou que essa equação não apresentava soluções não triviais e desenvolveu essa demostração baseada no método da descida infinita, a qual, a grosso modo, assemelha-se ao princípio da boa ordenação dos naturais, ou seja, suponha que a equação tenha como solução os inteiros (a, b, c), com $c > 0$, o método consiste em encontrar outra solução de inteiros (a', b', c') com $0 < c' < c$. Repetindo este procedimento várias vezes, é possível encontrar uma solução (a'', b'', c''), com 0 <c"< 1, o que seria um absurdo. Os detalhes dessa demonstração podem ser encontrados em [1, Cápitulo 6]. Assim, como qualquer solução da equação $X^4 + Y^4 = Z^4$ daria uma solução da equação $X^4 + Y^4 = Z^2$, pelo mesmo raciocinio explicitado no final da seção anterior, ao provar que esta equação não possui solução não trivial Fermat provou o caso $n = 4$.

Esse foi o primeiro resultado importante para a demonstração do teorema porque a prova para esse expoente restringe os demais valores de n a apenas aos números primos ímpares, como explicitado na seção anterior.

2.5 O CASO $n = 3$: A EQUAÇÃO CÚBICA

O próximo caso demonstrado foi o caso $n = 3$, divulgado em 1753 por Leonard Euler, e sua prova para este caso também é baseada no método da descida infinita e envolve o conceito de número imaginário, os detalhes podem ser encontrados em [1, Cápitulo 6]. Este foi o primeiro matemático que apresentou uma prova significativa do teorema. Euler acreditava que se conseguisse provar o teorema para $n = 3$ então poderia generalizar a demonstração para os demais valores de n.

2.6 AS DEMAIS PROVAS

As provas dos demais n primos foram apresentadas por diversos matemáticos separadamente. Em 1828, Dirichlet publicou sua demostração para $n = 5$ usando argumentos sobre a aritmética do corpo $K = \mathbb{Q}(\sqrt{5})$ e, em 1832, também provou o caso $n = 14$. O próximo avanço considerável foi em 1839, quando Lamé provou a equação para $n = 7$ utilizando identidades polinomiais. Por volta de 1950, Ernest Kummer obteve êxito em demostrar que o teorema era verdadeiro para os n primos menores que 100 com exceção de 37, 59 e 67, realizando um avanço significativo na demostração do teorema.

Com o avanço da computação, diversos matemáticos provaram o teorema para variados valores de n, ao passo que em 1980 estava provado para todos os valores de $n \leq 125.000$ e, em 1993, esse valor se expandiu para $n \leq 4.000.000$.

A partir de 1970, foi possível estabelecer uma conexão do teorema enunciado por Fermat com a Teoria das Curvas Elípticas e, em 1984, o matemático Gerhard Frey, apresentou a ideia de que se pudesse provar uma conjectura desta área, devida a Taniyama-Shimura, de que cada equação elíptica está associada a uma forma modular, então a equação de Fermat não teria soluções não triviais para $n \geq 3$. Com base nesta nova perspectiva, Andrew Wiles, em 1995, criando uma ponte entre campos totalmente distintos da Matemática, encontrou uma demostração para a conjectura de Taniyama-Shimura e, consequentemente, provou o que hoje é conhecido como o Último Teorema de Fermat.

3

O ÚLTIMO TEOREMA DE FERMAT MÓDULO UM INTEIRO

Nessa seção estudaremos as congruências do tipo

$$X^n + Y^n \equiv Z^n \mod m,$$

com $X, Y, Z \in \mathbb{Z}$, $m, n \in \mathbb{N}$, que podem ser escritas de modo equivalente como

$$X^n + Y^n - Z^n \equiv 0 \mod m.$$

Resolver essas congruências significa encontrar, se existirem, números inteiros x, y, z tais que $x^n + y^n - z^n \equiv 0 \mod m$, ou seja, o conjunto solução S, o qual é expresso como

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid x^n + y^n \equiv z^n \mod m\} \subset \mathbb{Z}^3.$$

Adotamos $m \geq 1$ porque o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, o que torna desinteressante o estudo dessa congruência módulo 1. Também é irrelevante o estudo dessa congruência módulo $-m$ já que coincide com o estudo de m.

Definição 3.1. *Considere a trinca de inteiros (x, y, z) solução da congruência $X^n + Y^n \equiv Z^n \mod m$, com $n, m \in \mathbb{N}$. Se uma de suas entradas for congruente a zero módulo m, então a trinca é chamada solução trivial e quanto suas entradas não possuem fator comum a trinca será chamada de trinca primitiva.*

Assim, para quaisquer $n, m \in \mathbb{N}$, essa congruência apresenta infinitas soluções como por exemplo as trincas da forma (x, y, z) tais que:

- $x \equiv 0$ e $y \equiv z \mod m$ ou $y \equiv 0$ e $x \equiv z \mod m$;
- $x \equiv -y$ e $z \equiv 0 \mod m$, para n ímpar;
- $x \equiv 0$ e $y \equiv -z \mod m$ ou $y \equiv 0$ e $x \equiv -z \mod m$, para n par.

Note que se $(x, y, z) \in \mathbb{Z}^3$ é uma solução da congruência, então $(cx, cy, cz), c \in \mathbb{Z}$, também será. Contudo, estas trincas são desinteressantes para o nosso estudo, pois apresentam um imediatismo e não são as trincas que realmente desejamos investigar propriedades.

3.1 UMA REDUÇÃO PARA O CASO COM m PRIMO

Sabemos que cada número inteiro é congruente módulo m a um dos números inteiros $0, 1, \ldots, m-1$. Assim, se (x, y, z) é uma solução para a congruência $X^n + Y^n \equiv Z^n \mod m$, com $n \in \mathbb{N}$, temos as seguintes opções:

1. $x \equiv 0 \mod m$, o que nos daria uma solução trivial, o que não estamos interessados nesse momento;

2. $x \equiv x_1 \mod m$, com $x_1 \in \{1, 2, \ldots, m-1\}$.

Além disso, se $x \equiv x_1 \mod m$ então, pela Proposição 1.5, $x^n \equiv x_1^n \mod m$. De modo análogo, podemos proceder com y e com z. Assim, podemos restringir a nossa busca por soluções não triviais (x, y, z) da congruência $X^n + Y^n \equiv Z^n \mod m$, com $n \in \mathbb{N}$, para $0 \leq x, y, z < m$.

Observe ainda que, escrevendo $m = p_1^{r1} \ldots p_s^{rs}$, onde $p_1, \ldots, p_s$ são números primos distintos, $r_1, \ldots, r_s \in \mathbb{N}$, $s \in \mathbb{N}$, podemos concluir pela Proposição 1.8 que a congruência $X^n + Y^n \equiv Z^n \mod m$ admite solução se, e somente se, a congruência $X^n + Y^n \equiv Z^n \mod p_i^{r_i}$, $i = 1, \ldots s$, também admite. Por outro lado, pela mesma proposição, se a congruência $X^n + Y^n \equiv Z^n \mod p_i^{r_i}$ admite solução, então a congruência $X^n + Y^n \equiv Z^n \mod p_i$ também admite.

Diante disso, o principal resultado deste capítulo se concentrará na busca por soluções não triviais da congruência

$$X^n + Y^n \equiv Z^n \mod p$$

onde $n, p \in \mathbb{N}$ e p é primo.

3.2 OS RELEVANTES VALORES DE n PARA CADA PRIMO p FIXADO

Dado um primo $p \in \mathbb{N}$ as congruências

$$X^n + Y^n \equiv Z^n \mod p,$$

com $X, Y, Z \in \mathbb{Z}$ e $n \in \mathbb{N}$, se reduzem a uma quantidade finita de congruências a serem estudadas.

De maneira precisa, pelo Pequeno Teorema de Fermat, temos $a^{p-1} \equiv 1 \mod p$ sempre que p e a forem coprimos. Logo, usando o algoritmo da divisão euclideana, cada $n \in \mathbb{N}$ pode ser escrito da forma

$$n = a(p-1) + r,$$

onde $a, r \in \mathbb{Z}$ e $0 \leq r < p-1$. Logo,

$$\begin{aligned} x^n + y^n - z^n &\equiv x^{a(p-1)+r} + y^{a(p-1)+r} - z^{a(p-1)+r} \mod p \\ &\equiv (x^{(p-1)})^a x^r + (y^{(p-1)})^a y^r - (z^{(p-1)})^a z^r \mod p \\ &\equiv x^r + y^r - z^r \mod p, \end{aligned}$$

sempre que x, y e z forem coprimos com p. Assim, estudar as soluções não triviais congruência

$$X^n + Y^n \equiv Z^n \mod p$$

se reduz a estudar as soluções não triviais de uma das congruências

$$X^r + Y^r \equiv Z^r \mod p,$$

para algum $r \in \mathbb{N}$ tal que $0 < r < p-1$.

3.3 EXEMPLOS DE DIVERSOS CASOS PARTICULARES

Nesta seção apresentaremos algumas situações onde a congruência $X^n + Y^n \equiv Z^n \mod p$, para $n, p \in \mathbb{N}$, com p primo apresenta ou não soluções não triviais.

Não é difícil ver que todas as soluções da Equação de Fermat também resolvem a congruência em estudo. Porém, existirão soluções da congruência que não originarão soluções para a Equação de Fermat.

3.3.1 *Os casos $n = 1$ e $p \geq 2$*

Neste caso, todas as soluções da Equação de Fermat para o caso $n = 1$ validam esta congruência, ou seja, as trincas de inteiros $(x, y, x+y)$ resolvem esta congruência. Mas o conjunto solução nesse caso é mais amplo já que as trincas de inteiros cujas entradas são congruentes a esta, isto é, $(a, b, a+b)$ tais que $a \equiv_p x$ e $b \equiv_p y$, também são solução para a congruência apresentada.

Exemplo 3.2. *As trincas $(1, 2, 3)$ e $(3, 4, 7)$ são soluções distintas da equação de Fermat e, consequentemente, também são soluções da congruência $X + Y \equiv Z \mod 5$. Além disso, $(3, 4, 2)$ é solução desta congruência, mas $(3, 4, 2)$ não é solução da equação de Fermat.*

3.3.2 *Os casos $n = 2$ e $p \geq 2$*

As soluções do Teorema de Pitágoras são soluções para esta congruência para todo primo p. Porém, com a escolha de diversos primos p pode-se gerar casos bem distintos.

Por exemplo, se tomarmos $p = 3$ e $n = p - 1 = 2$ a congruência não terá soluções além das triviais, de acordo com a Proposição 1.17. Isso ocorre porque, se x, y e z são coprimos com p e $x \not\equiv_p 0$, $y \not\equiv_p 0$ e $z \not\equiv_p 0$ então, $x^2 \equiv y^2 \equiv z^2 \equiv 1 \mod 3$ assim $x^2 + y^2 \equiv z^2 \mod 3$ resultaria em $1 + 1 = 2 \equiv 1 \mod 3$, o que é um absurdo. Esse caso é uma especificidade do caso geral apresentado na Seção 3.4, quando apresentamos algumas consequências do Pequeno Teorema de Fermat na congruência em estudo.

3.3.3 *Os casos* $X^n + Y^n \equiv Z^n \mod 2$

Dado um número inteiro $k \in \mathbb{Z}$, há duas possibilidades:

1. o resto da divisão de k por 2 é 0, ou seja, $k \equiv 0 \mod 2$;
2. o resto da divisão de k por 2 é 1, ou seja, $k \equiv 1 \mod 2$.

Além disso, da Proposição 1.5, se $k \equiv 0 \mod 2$, então $k^n \equiv 0^n \equiv 0 \mod 2$ e, se $k \equiv 1 \mod 2$, então $k^n \equiv 1^n \equiv 1 \mod 2$. Por outro lado, sabemos que a soma de dois números pares ou dois números ímpares sempre é um número par e a soma de um número ímpar com um número par é sempre um número ímpar. Assim, não podemos ter uma solução não trivial da congruência, pois $x \equiv 1 \mod 2$, $y \equiv 1 \mod 2$ e $z \equiv 1 \mod 2$ implicaria em

$$0 \equiv x^n + y^n \equiv z^n \equiv 1 \mod 2,$$

o que não pode ocorrer. Desse modo, no caso $p = 2$ as soluções da congruência $X^n + Y^n \equiv Z^n \mod 2$ são apenas as soluções triviais.

3.3.4 *Os casos* $X^n + Y^n \equiv Z^n \mod 3$

Similarmente ao que fizemos no caso anterior, todo número inteiro $k \in \mathbb{Z}$, pode ser escrito como uma das três formas: $3k$, $3k + 1$ ou $3k + 2$ com $k \in \mathbb{Z}$, ou seja, os possíveis restos da divisão de um número inteiro por 3 são $0, 1$ ou 2. Decorre disso que, dado $k \in \mathbb{Z}$, vale apenas uma das possibilidades:

1. $k \equiv 0 \mod 3$;
2. $k \equiv 1 \mod 3$;
3. $k \equiv 2 \mod 3$.

Novamente pela Proposição 1.5, seguindo o raciocínio anterior, temos que analisar apenas três situações com $x, y \in \mathbb{Z} \setminus \{3\mathbb{Z}\}$:

1. se $x \equiv 1 \mod 3$ e $y \equiv 1 \mod 3$, então $x^n + y^n \equiv 2 \mod 3$;
2. se $x \equiv 2 \mod 3$ e $y \equiv 2 \mod 3$, então $x^n + y^n \equiv (-1)^n + (-1)^n \mod 3$;

3. se $x \equiv 1 \mod 3$ e $y \equiv 2 \mod 3$, então $x^n + y^n \equiv 1 + (-1)^n \mod 3$.

Observe que, se n for par, a congruência apresenta apenas soluções triviais, já que das situações apresentadas acima temos $2 \equiv x^n + y^n \equiv z^n \mod 3$, porém $z^n \equiv 1 \mod 3$ para todo $z \in \mathbb{Z} \setminus 3\mathbb{Z}$, o que resultaria no absurdo $2 \equiv x^n + y^n \equiv z^n \equiv 1 \mod 3$. Numa análise similar, para n ímpar, se $z \in \mathbb{Z} \setminus 3\mathbb{Z}$, então $z^n \equiv 2 \mod 3$ ou $z^n \equiv 1 \mod 3$, e nos casos 1, 2 e 3 temos $x^n + y^n \equiv 2 \mod 3$, $x^n + y^n \equiv 1 \mod 3$ e $x^n + y^n \equiv 0 \mod 3$, respectivamente. Portanto, a congruência $X^n + Y^n \equiv Z^n \mod 3$ apresenta as seguintes soluções não triviais: $x \equiv y \equiv 1 \mod 3$ e $z \equiv 2 \mod 3$ ou $x \equiv y \equiv 2 \mod 3$ e $z \equiv 1 \mod 3$.

3.4 CONSEQUÊNCIAS DE ALGUNS TEOREMAS DESTE TRABALHO

O Teorema de Euler, o Pequeno Teorema de Fermat e a função de Carmichael nos permitem encontrar casos em que a congruência em estudo sempre apresenta soluções ou não apresenta soluções não triviais.

• **O caso $X^p + Y^p \equiv Z^p \mod p$, com $p \in \mathbb{Z}$ primo:** as soluções dessa congruência são as mesmas apresentadas na Seção 3.3.1 para o caso $n = 1$, pois, pelo Pequeno Teorema de Fermat, para cada $x, y, z \in \mathbb{Z}$, tem-se $x^p \equiv x \mod p$, $y^p \equiv y \mod p$ e $z^p \equiv z \mod p$, e segue da Proposição 1.5, item 1, que $x^p + y^p \equiv x + y \mod p$ e, pela Proposição 1.3, item 3, temos $x + y \equiv z \mod p$.

• **O caso $X^{p-1} + Y^{p-1} \equiv Z^{p-1} \mod p$, com $p \in \mathbb{Z}$ primo:** esta congruência não possui soluções não triviais. De fato, quando p não dividir nenhum dos números $x, y, z \in \mathbb{Z}$, pelo Pequeno Teorema de Fermat, $x^{p-1} \equiv 1 \mod p$, $y^{p-1} \equiv 1 \mod p$ e $z^{p-1} \equiv 1 \mod p$. Assim, a congruência $x^{p-1} + y^{p-1} \equiv z^{p-1} \mod p$ corresponde a $2 \equiv 1 \mod p$ sempre que $x, y, z \in \mathbb{Z} \setminus \{p\mathbb{Z}\}$, o que é um absurdo.

• **Os casos $X^{\lambda(m)} + Y^{\lambda(m)} \equiv Z^{\lambda(m)} \mod m$ e $X^{\Phi(m)} + Y^{\Phi(m)} \equiv Z^{\Phi(m)} \mod m$:** analogamente ao item anterior, outros valores para os quais as congruências não apresentam solução não trivial são $n = \lambda(m)$ ou $\Phi(m)$, onde $\lambda(m)$ é a função de Carmichael aplicada em m e $\Phi(m)$ é a função Fi de Euler aplicada em m. Isso porque as congruências

$$x^{\lambda(m)} + y^{\lambda(m)} \equiv y^{\lambda(m)} \mod m$$

e

$$x^{\Phi(m)} + y^{\Phi(m)} \equiv y^{\Phi(m)} \mod m,$$

onde $x, y, z, m \in \mathbb{Z}$ e m é coprimo com x, com y e com z, também se reduzem a

$$2 \equiv 1 \mod m,$$

pois

$$x^{\lambda(m)} \equiv 1 \mod m,\ x^{\Phi(m)} \equiv 1 \mod m,\ y^{\lambda(m)} \equiv 1 \mod m,$$

$$y^{\Phi(m)} \equiv 1 \mod m,\ z^{\lambda(m)} \equiv 1 \mod m \text{ e } z^{\Phi(m)} \equiv 1 \mod m.$$

3.5 EXISTÊNCIA DE SOLUÇÕES NÃO TRIVIAIS PARA CERTOS PRIMOS p

A busca por soluções não triviais para $X^n + Y^n \equiv Z^n \mod p$, com $p, n \in \mathbb{N}$, analisando para cada número primo p é impossível. Entretanto, é possível provar que, para cada $n \in \mathbb{N}$, existe um número primo p para o qual a congruência apresenta solução.

Para apresentarmos os casos em que a congruência em estudo possui solução não trivial, vamos nos apoiar nos *Teoremas de Ramsey e de Schur*, os quais serão apresentados detalhadamente na seção a seguir. O desenvolvimento da Seção 3.5 é baseado em [13] e [6].

3.5.1 *Teorema de Ramsey e Teorema de Schur*

O desenvolvimento desta seção é iniciado com alguns conceitos sobre grafos.

Definição 3.3. *Um grafo é qualquer conjunto de pontos, chamados vértices, e possíveis arestas ligando-os. Um grafo completo de n pontos, denotado por K_n, é um grafo de n pontos com a propriedade de que todos os seus pares de vértices são conectados por uma aresta.*

Exemplo 3.4. *A Figura 1 mostra os grafos completos K_3, K_4 e K_5, respectivamente (note que todos os vértices estão conectados por uma aresta).*

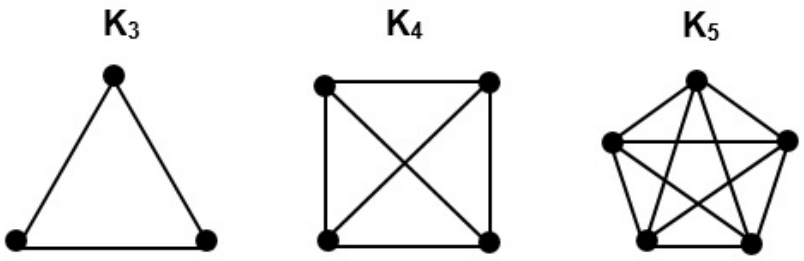

Figura 1: exemplo de grafos completos.

Exemplo 3.5. *Os grafos apresentados na Figura 2 não são completos, pois existem vértices que não estão ligados entre si por uma aresta.*

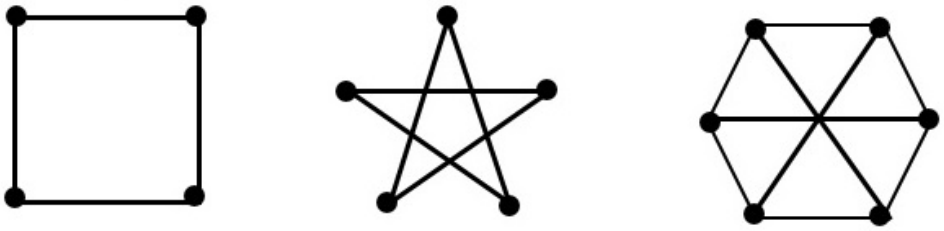

Figura 2: exemplos de grafos.

Definição 3.6. *Uma k-coloração de arestas de um grafo completo é uma atribuição de até k cores distintas ($k \in \mathbb{N}$ para as arestas do grafo. Um grafo é dito monocromático se todas as suas arestas são da mesma cor.*

Exemplo 3.7. *A Figura 3 mostra exemplos de uma 2-coloração de K_4, onde o primeiro e o último grafo exemplificam grafos monocromáticos.*

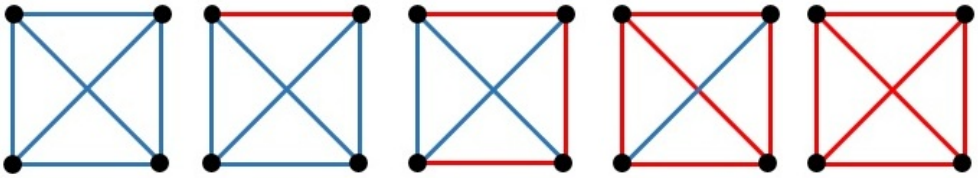

Figura 3: exemplos de 2-coloração de K_4.

Definição 3.8. *Dados $r_1, \ldots, r_k \in \mathbb{N}$, o número de Ramsey da k-upla $(r_1, \ldots, r_k)$, é o menor número inteiro positivo $n = R(r_1, \ldots, r_k)$ tal que qualquer k-coloração do grafo K_n admite um subgrafo monocromático K_{r_i} da cor i para algum $1 \leq i \leq k$.*

Exemplo 3.9. *Seja $(r_1, r_2) = (3, 3)$. A 2-coloração do grafo K_5 na Figura 4 a seguir apresenta uma coloração que não contém um subgrafo K_3 monocromático. Portanto, $R(3, 3) > 5$. Por outro lado, pode-se verificar que qualquer 2-coloração de um grafo K_6 contém um subgrafo K_3 monocromático, como o K_6 ilustrado também na Figura 4, então $R(3, 3) = 6$.*

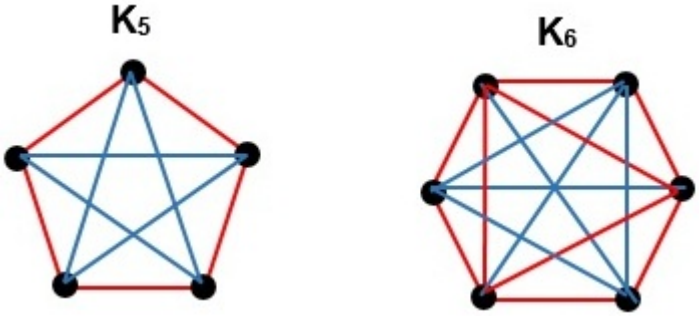

Figura 4: exemplo e contraexemplo de $R(3, 3)$.

A garantia da existência do número de Ramsey é um teorema atribuído a Ramsey:

Teorema 3.10. *(Ramsey) Para quaisquer k números naturais, $r_1, r_2, \ldots, r_k$, existe um número natural, $n = R(r_1, r_2, \ldots, r_k)$, tal que qualquer grafo completo K_n colorido com k cores distintas, deve conter um subgrafo K_{r_i} da cor i para algum $1 \leq i \leq k$. Em outras palavras, o número de Ramsey existe.*

Demonstração. A prova deste resultado requer uma análise imediata de três casos e uma estrutura indutiva:

1. $R(r_{\alpha_{(1)}}, r_{\alpha_{(2)}}, \ldots, r_{\alpha_{(k)}}) = R(r_1, r_2, \ldots, r_k)$ para $r_1, r_2, \ldots, r_k \geq 2$ e qualquer permutação α de $\{1, 2, \ldots, k\}$ uma vez que para cada coloração de um grafo exite uma outra com as cores permutadas.

2. $R(r_1, r_2, \ldots, r_{k-1}, 1) = 1$ para todos $r_1, r_2, \ldots, r_{k-1} \geq 2$, pois, uma vez que K_1 não possui arestas, não há aresta para colorir. Assim, qualquer K_1 colorido sempre conterá um K_1 monocromático;

3. $R(r_1, r_2, \ldots, r_{k-1}, 2) = R(r_1, r_2, \ldots, r_{k-1})$ para $r_1, r_2, \ldots, r_{k-1} \geq 2$, pois, por definição, $R(r_1, r_2, \ldots, r_{k-1})$ é a menor quantidade de vértices que um grafo completo deve conter para se obter um K_{r_1} da cor 1 ou K_{r_2} da cor 2 ou, assim por diante, um $K_{r_{k-1}}$ da cor $k-1$. Entretanto, podemos escolher aleatoriamente qualquer uma das suas arestas e pintá-la de uma cor, digamos r, obtendo, assim, um K_2 da cor r. As arestas restantes permanecem todas coloridas ou da cor 1 ou da cor 2 ou, sucessivamente, até a cor $r-1$. De uma maneira ou de outra, sempre teremos um K_{r_1} da cor 1 ou um K_{r_2} da cor 2 ou, sucessivamente, um K_{r-1} da cor $r-1$ ou um K_2 da cor r;

4. $R(r_1, ..., r_k) \leq R(r_1, ..., r_{k-2}, R(r_{k-1}, r_k))$, para todos $r_1, r_2, \ldots, r_k \geq 2$.

O item (1) garante que não há relevância na ordem dos números $r_1, \ldots, r_k$. Assim, tendo em vista os itens (2) e (3), ao estabelecer uma cota superior para $R(r_1, r_2)$ em termos de $R(r_1 - 1, r_2)$ e $R(r_1, r_2 - 1)$, completa-se um argumento indutivo utilizando o item (4). Para isso, verificaremos que

$$R(r_1, r_2) \leq R(r_1 - 1, r_2) + R(r_1, r_2 - 1),$$

o que concluirá a demonstração. De fato, considere uma coloração com duas cores, digamos azul e vermelho, em K_n com $n = R(r_1 - 1, r_2) + R(r_1, r_2 - 1)$. Escolhamos um dos vértices de K_n, digamos v, e consideremos V_v e A_v sendo, respectivamente, o conjunto dos vértices ligados a v por uma aresta vermelha e por uma aresta azul. Como temos $R(r_1 - 1, r_2) + R(r_1, r_2 - 1)$ vértices neste grafo, existem $R(r_1 - 1, r_2) + R(r_1, r_2 - 1) - 1$ outros vértices e um dos seguintes casos deve ocorrer:

- a partir de v tem-se, ao menos, $R(r_1 - 1, r_2)$ arestas azuis e, neste caso, por definição de $R(r_1 - 1, r_2)$, dentre esses $R(r_1 - 1, r_2)$ vértices existem r_2 que estão conectados

entre si por arestas vermelhas ou $r_1 - 1$ que estão conectados entre si por arestas azuis, de modo que juntando v a estes $r_1 - 1$ vértices, obtemos r_1 vértices que estão conectados entre si por arestas azuis;

- a partir de v tem-se, ao menos, $R(r_1, r_2 - 1)$ arestas vermelhas e, neste caso, por definição de $R(r_1, r_2 - 1)$, dentre esses $R(r_1, r_2 - 1)$ vértices existem r_1 que estão conectados entre si por arestas azuis ou $r_2 - 1$ que estão conectados entre si por arestas vermelhas e, juntando v a estes $r_2 - 1$ vértices, obtemos r_2 vértices que estão conectados entre si por arestas vermelhas.

Com isso, um grafo completo bicolorido de ordem $R(r_1 - 1, r_2) + R(r_1, r_2 - 1)$ deve conter um K_{r_1} azul ou um K_{r_2} vermelho, provando que $R(r_1, r_2) \leq R(r_1 - 1, r_2) + R(r_1, r_2 - 1)$. □

O teorema a seguir é fundamental para a demonstração do resultado principal deste trabalho. Para o seu contexto, observe que uma k-coloração de um conjunto $A \neq \emptyset$ pode ser vista como uma função $f : A \to R$, onde $R = \{1, 2, \ldots, k\}$. Dizemos que cada número de $R = \{1, 2, \ldots, k\}$ é uma cor e, ainda, dizemos que $a \in A$ está colorido com a cor $i \in R$ se $f(a) = i$.

Teorema 3.11. *(Schur) Dado $k \in \mathbb{N}$, existe $N \in \mathbb{N}$ tal que se $n \geq N$, então para toda k-coloração C de $\{1, 2, \ldots, n\}$ existem $x, y, z \in \{1, 2, \ldots, n\}$ de mesma cor e que satisfazem $x + y = z$.*

Demonstração. Consideremos um grafo K_n, com $n \geq R(\overbrace{3, \ldots, 3}^{k \text{ vezes}})$. Tomemos dois vértices i, j de K_n, com $i, j \in \{1, \ldots, n\}$ e $i < j$, e definamos uma k-coloração f do conjunto das arestas de K_n por $f(a) = f(i, j) = C(j - i)$, onde indicamos uma aresta a entre os vértices i e j pelo par (i, j). Pelo Teorema 3.10, existe, em particular, um subgrafo K_3 monocromático. Assim, existem a, b e c, com $a < b < c$, de modo que $b - a$, $c - b$ e $c - a$ são todos da mesma cor. Com isso, escrevendo $x = b - a$, $y = c - b$ e $z = c - a$, teremos que (x, y, z) é uma trinca monocromática ordenada. □

Exemplo 3.12. *No conjunto*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$$

podemos fazer uma 3-coloração na qual temos x, y e z com a mesma cor e que não satisfazem $x + y = z$, por exemplo

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}.$$

Portanto, $R(3, 3, 3) > 16$.

3.5.2 *As soluções não triviais para* $X^n + Y^n \equiv Z^n \mod p$

Finalmente, estamos aptos a apresentar o teorema que estabelece, para cada $n \in \mathbb{N}$, a existência de soluções não triviais para a congruência $X^n + Y^n \equiv Z^n \mod p$, para certos números primos $p \in \mathbb{N}$:

Teorema 3.13. *Dado $n \in \mathbb{N}$, existe um número primo p_0 tal que para todo primo $p \geq p_0$, a congruência $X^n + Y^n \equiv Z^n \mod p$ admite uma solução inteira não trivial.*

Demonstração. Seja p um número primo. Consideremos o conjunto

$$A_{n,p} = \{a^n \mod p \mid a \in \{1, 2, \ldots, p-1\}\}$$

e definamos a seguinte relação de equivalência:

$$x \sim y \Leftrightarrow x \equiv yt \mod p,$$

para algum $t \in A_{n,p}$. Denotemos as classes de equivalências distintas por

$$a_i A_{n,p} = \{a_i t \mod p \mid t \in A_{n,p}\},$$

onde $a_1, \ldots, a_k \in \{1, \ldots, p-1\}$. Lembrando que as classes de equivalência em um conjunto formam uma partição deste conjunto[1], temos

$$\{1, 2, \ldots, p-1\} = a_1 A_{n,p} \cup \cdots \cup a_k A_{n,p}$$

e cada elemento do conjunto $\{1, 2, \ldots, p-1\}$ pertence a uma (e apenas uma) dessas classes de equivalência.

Agora, para cada número primo p, tomemos a k-coloração

$$c : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, k\}$$

definida por $c(x) = i$, se $x \in a_i A_{n,p}$. Pelo Teorema 3.11, se tomarmos

$$p_0 \geq R\overbrace{(3, \ldots, 3)}^{n \text{ vezes}} \text{ e } p \geq p_0 \text{ com ambos primos,}$$

podemos encontrar uma solução não trivial (a, b, c) com $a, b, c \in \{1, 2, \ldots, p-1\}$ tais que $a, b, c \in a_i A_{n,p}$, ou seja, são de mesma cor, para algum $i \in \{1, \ldots k\}$, de modo que $a = a_i x^n$, $b = a_i y^n$ e $c = a_i z^n$, para certos $x, y, z \in \{1, 2, \ldots, p-1\}$ e $a_i x^n + a_i y^n \equiv a_i z^n \mod p$. Como a_i e p são coprimos, pela Proposição 1.7, $a_i x^n + a_i y^n \equiv a_i z^n \mod p$ equivale a $x^n + y^n \equiv z^n \mod p$.

□

[1] Termos encontrados em livros de Álgebra e Aritmética, por exemplo, em [5].

O exemplo a seguir traz uma ilustração sobre como encontrar k e $a_1, \ldots, a_k$ conforme a notação deste Teorema. No entanto, a determinação de p_0 depende da determinação de $R\underbrace{(3, \ldots, 3)}_{n \text{ vezes}}$, o qual não é um assunto explorado neste trabalho.

Exemplo 3.14. *Considere $n = 4$ e $p = 17$. Neste caso,*

$$\begin{aligned} A_{4,17} &= \{a^4 \mod 17 \mid a \in \{1, 2, \ldots, 16\}\} \\ &= \{1, 16, 13, 1, 13, 4, 4, 16, 16, 4, 4, 13, 1, 13, 16, 1\} \\ &= \{1, 4, 13, 16\}. \end{aligned}$$

Logo,

$$1A_{4,17} = \{1, 4, 13, 16\}, \quad 2A_{4,17} = \{2, 8, 9, 15\},$$

$$3A_{4,17} = \{3, 5, 12, 14\} \quad e \quad 6A_{4,17} = \{6, 7, 10, 11\},$$

de onde concluímos que $k = 4$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ e $a_4 = 6$, pois

$$1A_{4,17} \cup 2A_{4,17} \cup 3A_{4,17} \cup 6A_{4,17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}.$$

Finalmente, a condição existencial para p vem ao encontrar um primo p_0 tal que $p_0 \geq R(3, 3, 3, 3)$. Considerando que $R(3, 3, 3, 3) \leq 62$, conforme Richard L.Kramer[2], podemos tomar, por exemplo, $p_0 = 67$.

[2] Revista Colombiana de Matemáticas, Volume 39 (2005).

4

PROPOSTA DIDÁTICA

A sociedade vive em constante transformação e, com isso, se faz necessário reflexões sobre as práticas docentes com intuito de buscar inovações na metodologia de ensino para que se possa formar cidadãos críticos e influentes, capazes de acompanhar com sensatez e criticidade os desafios propostos por essas mudanças.

Saber matemática é muito mais do que o domínio dos conteúdos. De acordo com os Parâmetros Curriculares Nacionais (PCNs) [2], para que um aluno saiba matemática é necessário que seja hábil para levantar ideias, desenvolva um raciocínio lógico e estabeleça conexões entre tópicos da Matemática e, também, conectá-los com outras áreas.

Assim, pesquisas buscando inovação da prática docente, afim de tornar as aulas mais propícias às necessidades da sociedade atual, vem ganhando destaque e, consequentemente, novas tendências de ensino ganham espaço uma vez que abrangem diferentes enfoques e são consideradas relevantes quando aplicadas às práticas vivenciadas em sala de aula.

Podemos dizer que uma tendência no ensino de Matemática é caracterizada por fatores tais como as finalidades atribuídas ao ensino de Matemática e a perspectiva em relação ao processo ensino-aprendizagem com vistas à melhoria do ensino de Matemática.

Atualmente, há várias tendências em educação Matemática, mas este trabalho apresenta apenas duas delas com o intuito de aplicá-las na proposta didática sugerida em seguida. Estas tendências são *o ensino de Matemática por meio da sua história e através da resolução de problemas.*

4.1 HISTÓRIA DA MATEMÁTICA

Para muitos alunos do ensino fundamental, a Matemática não passa de um conjunto de procedimentos e regras sem vínculo com o seu cotidiano, restringindo a sua capacidade de compreender seus conceitos, suas representações e aplicações a um emaranhado de contas sem sentido. Desse modo, os alunos criam aversão por esta disciplina, questionando aos professores, com frases como: “para que serve?” ou “onde vou usar isso?”.

Entender o contexto histórico que originou determinado conteúdo matemático pode contribuir, de forma significativa, para sua compreensão, já que, deste modo, é possível entender o motivo pelo qual cada conceito foi introduzido e que esse processo se deu de forma natural na ocasião.

O ensino de Matemática entrelaçado com seu contexto histórico também pode contribuir na construção do conhecimento matemático, auxiliando o aluno na compreensão dos métodos e fórmulas que lhe são apresentadas na sala de aula. Além disso, pode provocar

no aluno o interesse pelo aprofundamento do assunto, expondo-lhe o sentido de como os problemas eram resolvidos antes da formalização que hoje é apresentada.

Através do estudo da história da Matemática, o aluno percebe que a Matemática é um conteúdo em contínua evolução e que também foram desafios para outras mentes algumas das dificuldades apresentadas pelos alunos hoje, mostrando que os conceitos que atualmente são apresentados, bem estruturados e sequenciais, são resultados de grande esforço e respostas aos desafios que diversos matemáticos enfrentaram.

De acordo com os PCNs (cf. [2]), quando conectamos os conteúdos matemáticos com a sua história, podemos estabelecer vínculos com a informação cultural, sociológica e antropológica da humanidade e, nesse sentido, a história da Matemática constitui-se um instrumento de resgate da própria identidade cultural, fazendo com que o aluno perceba que avanço tecnológico de hoje não seria possível sem a herança cultural de gerações passadas.

Ainda podemos afirmar que a história da Matemática permite constituir pontes com diversas outras disciplinas como a História, a Filosofia, a Geografia e com parâmetros culturais.

A relação entre a Matemática e sua história não é apoiada apenas pelo PCNs. No campo da Educação Matemática é amplamente divulgada e defendida por diversos pesquisadores. De acordo com [10], estes defendem que a história da Matemática deve ser utilizada em todas as séries visto que esta aflora no discente uma visão crítica e reflexiva, desmistificando a ideia de que a Matemática é uma disciplina sem ligações com a realidade.

4.2 RESOLUÇÃO DE PROBLEMAS

A ideia do que significa "problema" é algo intuitivo, mas, mesmo sem uma definição formal, todos sabemos que problema é um obstáculo a ser superado e que exige o exercitar do pensamento para fazê-lo. No entanto, para o ensino de Matemática, os PCNs trazem uma definição formal para problema, a saber *"uma situação que demanda a realização de uma sequência de ações ou operações para obter um resultado. Ou seja, a solução não está disponível de início, no entanto é possível construí-la."*.

Resolver problemas é inerente a atividade humana. Desde os tempos mais remotos os homens buscam resolver situações que desafiam os seus conhecimento e isso não é diferente na Matemática. Ainda consoante com os PCNs, um dos objetivos do ensino de Matemática nas séries fundamentais é a resolução de problemas matemáticos.

A importância da resolução de problemas no ensino de Matemática é notória e, assim, pesquisas sobre este tema no Brasil vêm ganhando espaço e esta metodologia caracteriza-se como uma tendência na educação. O pioneiro na pesquisa sobre *Resolução de Problemas* foi *George Pólya*, considerado o "pai" da metodologia que se apoia na resolução de problemas, ao publicar um livro sobre o tema, em 1945, traduzido para o português como "A

Arte de Resolver Problemas" [7]. Aqui no Brasil, estudos sobre essa metodologia ganharam forças na segunda metade da década de 80. Essa tendência é amplamente apoiada e divulgada entre os pesquisadores na área de Educação Matemática, tal como podemos destacar o educador matemático *Luiz Roberto Dante* [3].

A Resolução de Problemas trata-se de uma metodologia educacional, em que o professor propõe aos alunos situações-problemas, procurando instigar o aluno a investigar e explorar novos conceitos. Essa prática pedagógica baseia-se numa interação professor-aluno e entre os próprios alunos, onde a mediação ocorre por meio de questionamentos direcionados. Nessa metodologia, a Matemática não é sempre o objeto central de estudo, mas sempre é uma ferramenta útil, destacando seu papel nas atividades cotidianas do educando e não apenas como uma disciplina a ser assimilada nas salas de aulas.

Para Pólya, a resolução de problemas se baseia em quatro etapas principais, que são: compreender o problema; elaborar um plano de ação fazendo conexões entres as informações fornecidas e o que é solicitado; executar o plano traçado; e fazer a verificação, onde pode rever todo o caminho trilhado e averiguar se não houve algum equívoco. Essa etapa é extremamente importante pois, após resolver o problema, é necessário que haja uma reflexão com o intuito de pôr à prova os resultados obtidos, os caminhos percorridos, e as habilidades desenvolvidas uma vez que nessa metodologia o processo de resolução ganha maior enfoque do que uma resposta correta.

Vale ressaltar que essas etapas não são rígidas, fixas e infalíveis. O processo de resolução de um problema é algo mais complexo e rico, que não se limita a seguir instruções passo a passo que levarão a uma solução como se fosse um algoritmo. Entretanto, de modo geral, elas orientam durante o processo.

Há diversas vantagens no ensino através da resolução de problemas em sala de aula. Esta prática contribui para que o aluno desenvolva um pensamento produtivo e estimule o desenvolvimento do raciocínio ao fazer uso inteligente dos recursos à sua disposição; capacita para enfrentar situações novas e nas tomadas de decisão; torna as aulas mais interessantes e desafiadoras; prepara o aluno para investigar estratégias; e ainda amplia a percepção para que as pessoas possam entender o mundo matematicamente organizado.

Assim, essa tendência deve ser amplamente explorada, uma vez que o dever da escola de hoje é formar cidadãos para a sociedade que está em rápida evolução cientifica e tecnológica, onde ocorrem mudanças abruptas, as quais geram a necessidade de uma capacitação dos alunos para que possam acompanhá-la.

Cabe esclarecer que, embora buscássemos autores que apontassem pontos de vistas diferentes sobre o assunto, isto é, que apresentassem situações em que não fossem favoráveis a aplicação desta metodologia ou razões que opusessem essa prática, não encontramos.

4.3 SEQUÊNCIA DIDÁTICA

Conteúdo:

- Divisão de números inteiros e suas propriedades.
- Resolução de equações com uma, duas e três incógnitas.
- Congruências.
- Resolução de equações envolvendo congruências.

Objetivos:

- Compreender e aplicar a relação fundamental da divisão de números naturais (i.e., algoritmo da divisão euclideana).
- Resolver equações no conjunto dos números inteiros.
- Apresentar um pouco da história de Pierre de Fermat e algumas de suas contribuições para a Matemática.
- Introduzir a noção de congruência de números inteiros e identificar soluções para equações envolvendo congruências.

Público alvo: Alunos dos 8º e 9º ano do Ensino Fundamental e do Ensino Médio.

Tempo estimado: 4 aulas de 1h30 de duração cada uma.

Planejamento
Aula 1

Objetivos específicos:

- Revisar divisão de números inteiros e suas propriedades.
- Escrever um número inteiro por meio da relação fundamental da divisão.
- Apresentar o conceito de congruência de números inteiros.

Desenvolvimento

Inicie a aula apresentando o seguinte problema:

Qual é o resto da divisão do número 6^{2015} ***por*** 10***?***

Com auxílio de uma calculadora, peça aos alunos que calculem as primeiros potências de 6 e anote as respostas apresentadas pelos alunos. Faça-os perceber que seria inviável efetuar o cálculo solicitado manualmente ou até mesmo com uma calculadora escolar. Em seguida, utilize os resultados apresentados para as potências e estimule-os a observar que o algarismo da unidade sempre será 6 e conclua que o resto da divisão proposta será 6, assim como o de qualquer potência desse número.

Em seguida, leve os alunos a uma biblioteca e solicite que procurem sobre a divisão de números inteiros e suas propriedades anotando os pontos relevantes. Em seguida, inicie um debate sobre as informações obtidas com o intuito de verificar se os alunos compreendem as informações que obtiveram. Faça alguns questionamentos, como por exemplo:

- O que significa elemento “neutro” e “nulo”?
- Sempre é possível efetuar a divisão com os inteiros?
- A divisão de números inteiros sempre é um número inteiro?
- O que significa uma divisão “exata”?
- Quais os possíveis restos da divisão de um número inteiro?

Se necessário, use exemplos numéricos para esclarecer as características da divisão e solicite aos alunos que também apresentem exemplos para as propriedades encontradas. Em seguida, destaque a relação fundamental da divisão: dividendo é igual ao produto do divisor pelo quociente adicionado ao resto e solicite que escreva alguns números dessa forma.

Posteriormente, separe os alunos em pequenos grupos com 5 ou 6 alunos e solicite que escrevam alguns números inteiros por meio da relação fundamental da divisão em pedaços de papel separados, cada grupo dividindo por um inteiro diferente. Em seguida, peça para cada grupo separar os números que apresentam o mesmo resto. Nesse momento, apresente o conceito de *“congruência”* e seu símbolo.

Posteriormente, direcione os alunos para observarem que cada número inteiro é congruente a um dos números compreendidos entre zero e o módulo do divisor (que são os possíveis restos) e que para encontrarmos mais números que também sejam congruentes a este inteiro basta somarmos este número a múltiplos do divisor.

Por fim, retome o problema inicial e apresente sua solução por meio da congruência, ou seja, mostre para os alunos que as potências de 6 são congruentes a 6 módulo 10.

Aula 2

Objetivos específicos:

- Escrever uma situação-problema utilizando linguagem algébrica.
- Resolver equações com uma e duas incógnitas no conjunto dos números inteiros.
- Reconhecer que uma equação do 1º grau com duas variáveis pode possuir mais de uma solução no conjunto dos inteiros.

Desenvolvimento

Incie a aula apresentando o seguinte problema:

Francisca tinha certa quantia em dinheiro e ganhou de sua mãe o dobro do que tinha. Com isso, cada uma ficou com 186 reais. Quanto de dinheiro tinha cada uma no início?

Discuta o problema com os alunos estimulando-os a encontrarem sua solução. Em seguida, incentive os alunos a utilizar a linguagem algébrica para equacionar o problema e solucioná-lo. Após isso, revise o conteúdo de equações com uma incógnita; relembre-os de conceitos fundamentais como Conjunto Universo, Conjunto Solução, raiz, técnicas de resolução etc..

Em seguida, apresente outro problema:

Em uma partida de futebol, Lucas e Marcelo foram os únicos que marcaram gols pelo time anfitrião. Sabendo que o jogo foi vencido por 4 ***a*** 0***, quais as possibilidades na ordem de marcação dos gols nessa partida?***

Solicite aos alunos que apresentem as possíveis soluções para a situação e equacione-a juntamente com eles. De modo análogo ao anterior, relembre as equações com duas incógnitas e apresente algumas de suas características. Ressalte para eles que nessas equações poderão ser encontradas diversas soluções. Em seguida, estimule-os as escrever o conjunto solução, ressaltando a escrita matemática.

Para finalizar, proponha algumas situações problemas para que os alunos resolvam em grupos com o intuito de relembrarem esses conteúdo e, por fim, resolva juntamente com eles para que possam esclarecer possíveis dúvidas que surjam durante as resoluções.

Aula 3

Objetivos específicos:

- Estimular o uso da História da Matemática como recurso metodológico para o ensino de Matemática.
- Utilizar recursos tecnológicos para promover a aprendizagem.

Desenvolvimento

Em um laboratório de informática com acesso a internet apresente os seguintes vídeos do Youtube: "Os Simpsons - Homer 3D"[1] e "Pierre de Fermat fazendo prova - Matemática Rio"[2]. Após a apresentação, comente com os alunos que ambos os vídeos apresentam algo relacionado à Matemática e a um matemático e pergunte se eles sabem identificar. Identifique a eles o matemático e a equação que aparece.

Nos computadores disponíveis, peça que levantem informações sobre este matemático e oriente-os sobre a necessidade analisar as informações obtidas para que utilizem apenas as relacionadas com o tema solicitado pela pesquisa.

Em seguida, inicie uma roda de conversas sobre Fermat e suas contribuições. Nesse sentido, questione-os:

- Quem foi Pierre de Fermat?

[1] Disponível em https://www.youtube.com/watch?v=wEzj40FxQC0, acessado dia 16/08/2018
[2] disponível em https://www.youtube.com/watch?v=EEuzxuYGpUY, acessado dia 16/08/2018

- Qual era a profissão e porque ele estudava Matemática?
- Quais foram algumas de suas contribuições?

Nesse momento, seria interessante destacar que Fermat era advogado e que desfrutava da Matemática como hobby (assim como tantos outros matemáticos) para que com isso consiga mostrar que não é necessário que haja uma divisão determinística entre pessoas de exatas e humanas. Converse também como era a sociedade na época e estimule-os a observar que estudar era privilégio de alguns e não era acessível a todos como nos dias atuais. Se achar conveniente, levante mais questionamentos nesse sentido.

Espera-se que após a conversa os alunos saibam sobre o Último Teorema de Fermat e sua célebre frase deixada na margem em seu livro a respeito do seu teorema e assim possam fazer um paralelo com os filmes apresentados. Se for necessário, apresente os vídeos novamente para os alunos. Ressalte que este teorema recebe o nome de Último Teorema de Fermat por ser a última observação de uma lista de observações e comentários deixados por Fermat, sem as devidas demonstrações.

Em seguida, enuncie o Último Teorema de Fermat de acordo com suas palavras, ou seja, *"Dividir um cubo em dois cubos, uma quarta potência ou, em geral uma potência qualquer em duas potências da mesma denominação acima da segunda é impossível"*, conforme [3]. Em seguida, interprete-o com os alunos equacionando-o, ou seja, $X^n + Y^n = Z^n$, com $n \in \mathbb{N}$, $n \geq 3$, só admite soluções inteiras triviais. Após apresentar a expressão e estimule os alunos a estudá-la com exemplos numéricos.

Aula 4

Objetivos específicos:

- Apresentar o Último Teorema de Fermat módulo um inteiro.
- Utilizar os conhecimentos algébricos para encontrar algumas soluções do Último Teorema de Fermat módulo um inteiro em casos pequenos e específicos de m e n.

Desenvolvimento

Inicie a aula revisando os conteúdos vistos nas aulas anteriores, ou seja, o conceito de congruência, o Último Teorema de Fermat e resolução de equações.

Em seguida, apresente o Último Teorema de Fermat módulo um inteiro, ou seja, $X^n + Y^n \equiv Z^n \mod m$ com $X, Y, Z \in \mathbb{N}$ e $n \in \mathbb{N}$ e $m \in \mathbb{N}$ e instigue-os na busca de suas soluções, por tentativa e erro, para pequenos valores de n e m. Nesse sentido, questione-os:

- Será possível encontrar uma solução para a congruência quando:

  $n = 1$ e para algum valor de m?

  $n = 2$ e para algum valor de m?

- Sabemos que o Último Teorema de Fermat não admite soluções não triviais quando $n \geq 3$. Será que a congruência terá soluções se $n = 3$?

- Há alguma solução da equação apresentada no teorema de Fermat que não é solução da congruência?

- Há alguma solução da congruência que não é solução da equação proposta pelo teorema de Fermat?

Posteriormente, peça aos alunos para apresentarem algumas soluções encontradas, incentivando-os a encontrar mais soluções a partir das que foram apresentadas.

Reflita com os alunos, caso não tenham observado ainda, que todas as soluções para a equação também são soluções para congruência, porém a recíproca não é válida. Outra observação, relevante a se destacar junto com os alunos, é que independente do valor atribuído a m a congruência possui infinitas soluções para $n = 1$ que podem ser obtidas a partir das soluções da equação e elabore o conjunto solução para esta situação. Induza-os a concluir que a congruência nem sempre apresenta soluções para o caso $n = 2$ e, se for conveniente, exiba os casos em que isso acontece. Por fim, apresente algumas soluções para o caso $n = 3$ e verifique com os alunos que estas não validam a equação de Fermat.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Andrade, J., Tópicos Especiais de Álgebra, SMB, Rio de Janeiro, 2013.

[2] Brasil. Secretaria de Educação Fundamental. Parâmetros curriculares nacionais: Matemática/Secretaria de Educação Fundamental. Brasília: MEC/SEF, 1998.

portal.mec.gov.br/seb/arquivos

[3] Dante, L., Formulação e Resolução de Problemas de Matemática, Ática, São Paulo, 2010.

[4] Eves, H., Introdução à História da Matemática, Unicamp, Campinas, 2011.

[5] Hefez, A., Iniciação à Aritmética, IMPA, Rio de Janeiro, 2015.

[6] Amini, N., Fermat's Last Theorem (mod p), 2013.

https://bit.ly/2WtOTB8

[7] Pólya, G., A arte de resolver problemas. Rio de Janeiro: Interciência, 1995.

[8] Ribas, S., Infinitos Números de Carmichael. Dissertação. UFMG, 2013.

[9] Ribenboim, P., 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York, 1979.

[10] Santos, C., A História da Matemática como Ferramenta no Processo de Ensino-Aprendizagem da Matemática, Dissertação do Mestrado Profissional em Ensino de Matemática, PUC-SP, 2007.

[11] Schur, I., *Über die Kongruenz* $x^m + y^m = z^m \mod p$. Jahresber. Deutsche Math.-Verein. 25, 114–116, 1916.

[12] Singh, S., O Último Teorema de Fermat, Bestbolso, Rio de Janeiro, 2014.

[13] Soares, G., O Teorema de Ramsey e outros resultados de combinatória que não são de contagem, Dissertação de Mestrado, IMPA, 2014.

[14] Yaun, Q., Ramsey Theory and Fermat's Last Theorem, 2010.

https://bit.ly/2OAwQ9C