UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

IZABELLA VIANNA GOMES

QUADRADOS PERFEITOS E NÚMEROS p-ÁDICOS: APLICAÇÕES AO ENSINO E À QUESTÃO 6 DA IMO DE 1988

CURITIBA

2025

IZABELLA VIANNA GOMES

QUADRADOS PERFEITOS E NÚMEROS p-ÁDICOS: APLICAÇÕES AO ENSINO E À QUESTÃO 6 DA IMO DE 1988

Perfect squares and p-adic numbers: applications to teaching and to IMO 1988 Problem 6

Dissertação apresentada como requisito para obtenção do título de Mestre em Matemática, Área de Concentrção: Matemática na Educação Básica, no Programa Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Técnológica Federal do Paraná - UTFPR.
Linha de pesquisa: Formação de Professores de Matemática da Educação Básica.
Orientador(a): Dr. Ronie Peterson Dario

CURITIBA

2025

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

IZABELLA VIANNA GOMES

QUADRADOS PERFEITOS E NÚMEROS P-ÁDICOS: APLICAÇÕES AO ENSINO E À QUESTÃO 6 DA IMO DE 1988

Trabalho de pesquisa de mestrado apresentado como requisito para obtenção do título de Mestre Em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR). Área de concentração: Matemática.

Data de aprovação: 25 de Novembro de 2025

Dr. Ronie Peterson Dario, Doutorado - Universidade Tecnológica Federal do Paraná

Dra. Mael Sachine, Doutorado - Universidade Federal do Paraná (Ufpr)

Dra. Mari Sano, Doutorado - Universidade Tecnológica Federal do Paraná

Documento gerado pelo Sistema Acadêmico da UTFPR a partir dos dados da Ata de Defesa em 25/11/2025.

RESUMO

Este trabalho propõe um método para resolver problemas de olimpíadas de matemática que envolvem quadrados perfeitos, de forma a superar a limitação inerente ao método da contradição modular, o qual apenas verifica a não existência de soluções. Desenvolvemos uma abordagem baseada no princípio local-global, utilizando números p-ádicos e o Teorema de Grunwald-Wang para estabelecer condições que garantam quando um número inteiro é um quadrado perfeito. O método é aplicado à histórica Questão 6 da IMO de 1988, oferecendo uma solução alternativa às abordagens tais como Vieta Jumping e Descida Infinita de Fermat . Além das contribuições teóricas, o trabalho inclui propostas didáticas para o ensino básico, com atividades investigativas sobre números 2-ádicos e datas pitagóricas, mostrando como conceitos matemáticos avançados podem ser acessíveis a estudantes da educação básica. Os resultados indicam a viabilidade de integrar teoria dos números com educação matemática, apontando caminhos para aplicações em outros problemas olímpicos.

Palavras-chave: Números p-ádicos; Quadrados Perfeitos; Datas Pitagóricas; Olimpíadas de Matemática.

ABSTRACT

This dissertation proposes a method for solving mathematical olympiad problems involving perfect squares, aiming to overcome the inherent limitation of the modular contradiction method, which only verifies the non-existence of solutions. We developed an approach based on the local–global principle, using p-adic numbers and the Grunwald–Wang theorem to establish conditions that guarantee when an integer is a perfect square. The method is applied to the historic Problem 6 of the 1988 IMO, offering an alternative solution to approaches such as Vieta Jumping and Fermat's Infinite Descent. Beyond the theoretical contributions, the work includes didactic proposals for basic education, with investigative activities on 2-adic numbers and Pythagorean dates, demonstrating how advanced mathematical concepts can be made accessible to basic education students. The results indicate the feasibility of integrating number theory with mathematics education, pointing toward applications in other olympiad problems.

Keywords: p-adic Numbers; Perfect Squares; Pythagorean dates; Mathematical Olympiads.

SUMÁRIO

1 INTRODUÇÃO

Por permitirem uma grande variedade de aplicações e contextualizações, problemas envolvendo equações diofantinas são comuns em olimpíadas de matemática. Trata-se de equações cujos coeficientes são números inteiros e para as quais somente se admitem soluções formadas também por números inteiros. São tipicamente equações polinomiais, embora também se estude alguns tipos de equações exponenciais.

Há diversas abordagens e métodos, dependendo da equação. Na formação de professores de matemática, em especial no Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, considera-se inicialmente (HEFEZ, 2022) a equação linear (ou afim) em duas variáveis

$$aX + bY = c, \quad a, b, c \in \mathbb{Z}, \tag{1.1}$$

onde $\mathbb{Z}$ representa o conjunto dos números inteiros. Esta equação também é abordada na preparação de estudantes para competições de matemática, como a Olimpíada Internacional de Matemática (IMO), a Olimpíada Brasileira de Matemática (OBM), entre outras, e já foi utilizada até mesmo numa aplicação ao mercado financeiro (DARIO, 2022), em problemas de otimização de carteiras de investimento que demandam aquisições de quantidades inteiras de ativos financeiros.

As possíveis soluções da Equação 1.1 são pares (x, y) de números inteiros tais que $ax+by = c$ e são completamente descritas através do Algoritmo de Euclides Estendido (HEFEZ, 2022, Capítulo 5), que não apenas verifica a existência de soluções através da divisibilidade do número c pelo máximo divisor comum entre a e b, mas também mostra como gerar todas as soluções a partir de uma solução particular.

Equações mais complicadas obviamente demandam técnicas mais sofisticadas. Uma estratégia bem conhecida e popular em olimpíadas de matemática é "mudar o ambiente" em que se estuda a equação, transferindo o problema original para uma equação sobre corpos finitos com p elementos, onde p é um número primo. A ideia é que trabalhando módulo p, a existência de soluções pode ser analisada com maior facilidade, pois trata-se de um conjunto finito em que todo elemento não nulo possui inverso multiplicativo. Para melhor explicar essa estratégia, precisamos recordar algumas definições e resultados básicos da Aritmética (HEFEZ, 2022, Capítulo 8).

Iniciamos lembrando que dois números inteiros a e b são congruentes módulo p quando deixam o mesmo resto na divisão por p e denotamos $a \equiv b \mod p$. A relação de congruência produz uma relação de equivalência em $\mathbb{Z}$, sendo que uma classe de equivalência $\overline{r}$, com $0 \leq r \leq p-1$, reúne todos os números inteiros que deixam resto r na divisão por p. Assim, mostra-se que o conjunto quociente

$$\mathbb{Z}/p\mathbb{Z} = \left\{\overline{0},\ \overline{1},\ \ldots,\ \overline{p-1}\right\}$$

formado pelas classes residuais $\overline{a} = a + p\mathbb{Z}$ e dotado das operações usuais de soma e produto de classes é um corpo com p elementos, usualmente denotado por $\mathbb{F}_p$.

A projeção canônica $\pi : \mathbb{Z} \longmapsto \mathbb{F}_p$, associa o inteiro s à sua classe residual $\overline{s}$ e tem a propriedade fundamental de preservar as operações de soma e produto. Desta forma, a projeção π é a ferramenta que permite a tradução do problema algébrico original (sobre $\mathbb{Z}$) para o ambiente sobre $\mathbb{F}_p$. Na prática, trabalha-se somente com as congruências, ao invés da notação de classes residuais.

Por exemplo, em (HEFEZ, 2022), este método é introduzido através do estudo de congruências lineares e quadráticas, que correspondem às equações polinomiais de grau 1 e 2 em uma variável, respectivamente, dadas por

$$aX \equiv b \mod p \quad \text{e} \quad aX^2 + bX + c \equiv 0 \mod p,$$

e obtidas a partir das equações de grau 1 e 2 sobre os inteiros.

De maneira geral, para ilustrar a situação, temos

$$f(X_1, \ldots, X_n) = a \quad \twoheadrightarrow \quad f(X_1, \ldots, X_n) \equiv a \mod p.$$

O conhecido **Método da Contradição Modular** para equações diofantinas utiliza o fato de que a possível existência de solução para a equação original é preservada pela projeção sobre $\mathbb{F}_p$. Por exemplo, se o par de inteiros (x, y) é solução da Equação 1.1, tem-se $ax + by = c$. Aplicada a projeção, segue que $\overline{a}\,\overline{x} + \overline{b}\overline{y} = \overline{c}$, ou seja, $(\overline{x}, \overline{y})$ é solução de $\overline{a}X + \overline{b}Y = \overline{c}$ sobre $\mathbb{F}_p$.

Podemos então concluir, pela contra-positiva, que a não existência da solução modular para algum número primo p implica que a equação original também não tem solução. Ainda mais, esta conclusão pode ser obtida analisando a equação módulo um único número primo p. É claro que este número primo deve ser escolhido de forma conveniente para a equação. Em resumo, obtêm-se um método para mostrar que a equação original não tem solução, bastando para isso encontrar um único número primo p para o qual a equação não tenha solução, módulo p.

No Capítulo 3 vamos estudar brevemente o Método da Contradição Modular e apresentar algumas aplicações a problemas de olimpíadas de matemática. Na Seção 3.1 vamos abordar uma generalização natural, trocando o número primo p por um número inteiro $m > 1$. De particular interesse será o caso $m = 8$, que mostra-se muito útil em olimpíadas (veja os Problemas 16 e 17), devido a particularidades relacionadas aos quadrados módulo 8, conforme a Proposição 14.

Ocorre que a estratégia que expomos é basicamente unidirecional, ou seja, é útil para mostrar que o problema original **não possui solução**, ou, na melhor das hipóteses, para determinar alguma restrição sobre o conjunto solução. A direção contrária é muito mais complicada. Em geral, obter soluções modulares, mesmo que para todo número primo p, não garante a existência de solução racional. Um exemplo clássico é o polinômio $f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34)$, que possui raiz quando considerado sobre o corpo finito com p elementos (para qualquer p), mas não possui raiz racional (SERRE, 1973).

Na segunda parte deste trabalho, avançamos alguns passos na direção oposta, explorando meios para que a partir da solução de uma equação módulo p, para **todo primo** p, se possa deduzir a existência da solução sobre $\mathbb{Z}$. Vamos usar esta abordagem para lidar com equações diofantinas envolvendo quadrados perfeitos. Um número inteiro a é chamado de um **quadrado perfeito** quando a equação polinomial

$$X^2 - a = 0 \tag{1.2}$$

possui solução em $\mathbb{Z}$, isto é, existe um inteiro x tal que $a = x^2$. De maneira geral, se a pertence a um anel comutativo com unidade (por exemplo, $\mathbb{Q}$ e $\mathbb{F}_p$) diz-se que a é um **quadrado** quando a mesma equação possui solução neste anel. Um caso particular importante é sobre $\mathbb{R}$, o corpo dos números reais, em que todo número real positivo é um quadrado.

O caminho a ser percorrido passa por um breve estudo dos corpos de números p-ádicos ($\mathbb{Q}_p$), no Capítulo 4. Estes corpos fornecem um ambiente local e completo para cada primo p, análogo ao papel de $\mathbb{R}$ como completamento de $\mathbb{Q}$, mas na métrica p-ádica (GOUVÊA, 2020).

Na sequência, utilizamos um princípio do tipo local-global, conhecido como Teorema de Grunwald-Wang (Teorema 22), e uma versão quadrática do clássico Lema de Hensel (Teorema 23), para obtermos o **Método Local - Global** (Teorema 29), que estabelece condições para que um número inteiro positivo a seja um quadrado perfeito quando for um quadrado em $\mathbb{F}_p$, para todo número primo $p > 2$ e satisfizer uma condição extra para $p = 2$.

Aplicamos este método à histórica Questão 6 da IMO de 1988, que envolve a estrutura de quadrados perfeitos em uma equação diofantina não trivial. Este problema é considerado o mais difícil (ao menos de Teoria dos Números) já proposto em uma olimpíada de matemática.

Iniciamos com o Capítulo 2, no qual revisamos os resultados básicos sobre resíduos quadráticos, em especial o Critério de Euler, que permite determinar completamente quais classes em $\mathbb{F}_p$ correspondem a resíduos quadráticos. No Capítulo 6 finalizamos o trabalho com duas aplicações ao ensino. A primeira trata de obter uma forma de explicar a natureza de um número 2-ádico de forma suficientemente elementar para que seja entendida por um estudante do ensino básico. A segunda trata de datas pitagóricas, motivada pelo próprio ano de $2025 = 45^2$ já ser um quadrado perfeito. Desenvolvemos uma sequência didática que explora o caso 16 de setembro de 2025 $(9/16/25)$, onde 9, 16 e 25 são quadrados perfeitos que formam o terno pitagórico $(3, 4, 5)$. A proposta inclui atividades investigativas sobre propriedades dos ternos pitagóricos primitivos e restrições do calendário gregoriano.

Acreditamos que a iniciativa deste trabalho possa beneficiar os estudantes tanto do PROFMAT, quanto dos cursos preparatórios para olimpíadas, pois os tópicos citados consistem em uma continuação natural nos assuntos de Aritmética trabalhados nestes cursos. Em especial, acreditamos que os métodos aqui tratados possam levar a abordagens alternativas em problemas de olimpíadas de matemática.

2 RESÍDUOS QUADRÁTICOS IN A NUTSHELL

Neste capítulo estudaremos a estrutura dos quadrados no corpo finito com p elementos ($\mathbb{F}_p$), onde p é um número primo. Introduziremos o conceito de resíduo quadrático, exploraremos critérios para determiná-los, como o Critério de Euler (Teorema 3) e o fato de que exatamente metade dos elementos do conjunto $\{1, 2, \ldots, p-1\}$ correspondem à quadrados em $\mathbb{F}_p$, para $p > 2$.

A Teoria Elementar dos Números (HEFEZ, 2022; SANTOS, 2003) tem como principal objeto de estudo o anel dos números inteiros, denotado por $\mathbb{Z}$. Também são importantes os anéis quocientes $\mathbb{Z}/p\mathbb{Z}$ de $\mathbb{Z}$ por seus ideais primos $p\mathbb{Z} = \{p\alpha \mid \alpha \in \mathbb{Z}\}$.

Um elemento de $\mathbb{Z}/p\mathbb{Z}$ é uma classe $\bar{r}$, com $0 \leq r \leq p-1$, composta por todos os números inteiros que deixam resto r na divisão por p. Desta forma, $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$. Veja o Capítulo 8 de (HEFEZ, 2022) para uma abordagem mais detalhada.

Sendo $\bar{r} \neq \bar{0}$ em $\mathbb{Z}/p\mathbb{Z}$, através da clássica Identidade de Bezout (HEFEZ, 2022, Teorema 5.7), mostra-se que existe $s \in \mathbb{Z}$, com $1 \leq s \leq p-1$, tal que $\bar{r}\bar{s} = \bar{1}$. Isto implica que no anel (comutativo e com unidade) das classes residuais $\mathbb{Z}/p\mathbb{Z}$, todo elemento não nulo possui inverso multiplicativo, e portanto, $\mathbb{Z}/p\mathbb{Z}$ é um corpo. Vamos denotá-lo por

$$\mathbb{F}_p = \left\{\bar{0}, \bar{1}, \ldots, \overline{p-1}\right\},$$

e o chamá-lo de **corpo finito com p elementos**. O grupo multiplicativo de $\mathbb{F}_p$, formado pelos seus elementos não nulos, é denotado por

$$\dot{\mathbb{F}}_p = \mathbb{F}_p \setminus \{\overline{0}\}.$$

Definição 1. *Um **quadrado** em $\mathbb{F}_p$ é um elemento $\bar{a} \in \mathbb{F}_p$ para o qual existe $\bar{x} \in \mathbb{F}_p$ tal que $\bar{x}^2 = \bar{a}$. Se $\overline{a}$ é um quadrado em $\mathbb{F}_p$, dizemos que a é um **resíduo quadrático** módulo p.*

Note que a é um resíduo quadrático módulo p se, e somente se, a congruência $X^2 \equiv a \mod p$ possui solução. Denotamos o conjunto dos quadrados não nulos em $\mathbb{F}_p$ por

$$(\dot{\mathbb{F}}_p)^2 = \left\{\overline{a}^2 \mid \overline{a} \in \mathbb{F}_p^{\times}\right\}.$$

Por abuso de notação, denotaremos, quando ficar claro no contexto, a classe $\overline{a}$ simplesmente por a. Por exemplo, $(\dot{\mathbb{F}}_{11})^2 = \{1, 3, 4, 5, 9\}$. Em $\mathbb{F}_{11}$, temos $3 = 5^2$ e $5 = 7^2$, pois $5^2 \equiv 3 \mod 11$ e $7^2 \equiv 5 \mod 11$. Por sua vez, 2, 6, 7 e 8 não são resíduos quadráticos módulo 11, pois se a é um destes números, verifica-se diretamente que a congruência $X^2 \equiv a \mod 11$ não possui solução.

Como sugere este exemplo, é possível mostrar que para p primo ímpar, há exatamente $\dfrac{p-1}{2}$ resíduos quadráticos e $\dfrac{p-1}{2}$ não-resíduos quadráticos módulo p entre os números $1, \ldots, p-1$. Isso

divide $\dot{\mathbb{F}}_p$ em $\dfrac{p-1}{2}$ pares, cada um contribuindo com um único quadrado. O principal resultado para definir se um número é um resíduo quadrático é o Critério de Euler (Teorema 3), que veremos na sequência. Para estudá-lo, precisamos antes do clássico resultado a seguir, cuja demonstração (HEFEZ, 2022, Teorema 8.3.1) utiliza o Binômio de Newton e indução matemática.

Teorema 2 (Pequeno Teorema de Fermat)**.** *Seja a um número inteiro e p um número primo que não divide a. Então*

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

Apenas para ilustrar a grande utilidade do Pequeno Teorema de Fermat, vejamos como calcular 6^n em $\mathbb{F}_{13}$, para $n \in \mathbb{N}$. Pela Divisão Euclidiana, temos $n = 12q + r$, para algum quociente $q \in \mathbb{Z}$ e algum resto $r \in \{0, \ldots, 11\}$. Como 13 não divide 6, Pelo Pequeno Teorema de Fermat temos que $6^{12} \equiv 1 \mod 13$. Obtemos assim a seguinte redução da potência n:

$$6^n = (6^{12})^q \cdot 6^r \equiv 6^r \mod 13,$$

e agora só precisamos calcular 6^r módulo 13, para $r \in \{0, \ldots, 11\}$. Vamos utilizar este cálculo no Problema 10 (a frente).

Agora suponha que p é um número primo ímpar. Pelo Teorema 2, temos que p divide

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Como p é primo, temos que p divide $a^{\frac{p-1}{2}} - 1$ ou p divide $a^{\frac{p-1}{2}} + 1$. Isto motiva o seguinte resultado.

Teorema 3 (Critério de Euler)**.** *Seja p um número primo ímpar e a um número inteiro não divisível por p. Então*

(1) *p divide $a^{\frac{p-1}{2}} - 1$ se, e somente se, a é um resíduo quadrático módulo p.*

(2) *p divide $a^{\frac{p-1}{2}} + 1$ se, e somente se, a não é um resíduo quadrático módulo p.*

A demonstração completa pode ser encontrada em (HEFEZ, 2022, Capítulo 8) e (SERRE, 1973, Capítulo I), mas para ilustrar, note que para a recíproca da parte (1), temos que existe $\alpha \in \mathbb{Z}$, tal que $a \equiv \alpha^2 \mod p$ e p não divide α. Assim,

$$a^{\frac{p-1}{2}} \equiv \alpha^{p-1} \equiv 1 \mod p.$$

Como aplicação do Teorema 3, temos que -1 é resíduo quadrático módulo p se, e somente se, $(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$. Como $\dfrac{p-1}{2}$ é par se $p = 4n+1$ e ímpar se $p = 4n+3$, segue o seguinte resultado, devido a Fermat:

Proposição 4 (Fermat)**.** *Se p é um número primo da forma $p = 4n + 1$, então -1 é resíduo quadrático módulo p. Por outro lado se $p = 4n + 3$, então -1 não é resíduo quadrático módulo p.*

3 O MÉTODO DA CONTRADIÇÃO MODULAR PARA RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS EM PROBLEMAS OLÍMPICOS

Neste capítulo exploramos o Método da Contradição Modular, que como explicamos na Introdução, permite concluir que uma equação diofantina não possui solução em $\mathbb{Z}$ a partir da não existência de solução da equação correspondente módulo p.

Uma **equação diofantina polinomial** é uma equação da forma

$$f(X_1, \ldots, X_n) = 0, \tag{3.1}$$

onde f é um polinômio em n variáveis com coeficientes inteiros, e as possíveis soluções são n-uplas $(x_1, \ldots, x_n)$, também compostas por números inteiros. Por exemplo, a equação diofantina

$$x^2 - 61y^2 = 1$$

possui uma história interessante porque sua solução foi um desafio, envolvendo frações contínuas, proposto por Fermat e resolvida de forma geral por Lagrange em 1766. Contudo, a menor solução natural possível, dada por $x = 1.766.319.049$, $y = 226.153.980$, já era conhecida por Bhaskara, muitos séculos antes! (STILLWELL, 2002).

Entre as equações diofantinas polinomiais, um caso de grande importância é a equação pitagórica (Exemplo 3.1), cujas soluções inteiras positivas são conhecidas como ternos pitagóricos. Esta equação será retomada no Capítulo 6 no contexto das datas pitagóricas, em que abordaremos estratégias educacionais aplicáveis.

Exemplo 3.1 (Equação Pitagórica)**.** *A equação $X^2 + Y^2 = Z^2$ admite infinitas soluções inteiras não triviais. Exemplos bem conhecidos são os ternos $(3, 4, 5)$, $(5, 12, 13)$ e $(8, 15, 17)$. O terno (x, y, z) corresponde à uma solução primitiva, isto é, $\mathrm{mdc}(x, y, z) = 1$, se e somente se, existem números inteiros positivos m e n, com $m > n$, $\mathrm{mdc}(m, n) = 1$ e de paridades opostas, tais que*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Exemplo 3.2 (Somas de Quadrados)**.** *Dizemos que o número inteiro a é uma **soma de quadrados** quando a equação diofantina*

$$X_1^2 + X_2^2 + \ldots + X_n^2 = a \tag{3.2}$$

possui solução, isto é, existem $x_1, \ldots, x_n \in \mathbb{Z}$, tais que $x_1^2 + x_2^2 + \ldots + x_n^2 = a$.

Há vários resultados bem conhecidos sobre somas de quadrados. Citamos aqui o Teorema de Legendre e o Teorema de Lagrange sobre somas de três e quatro quadrados, respectivamente (HEFEZ, 2022).

Teorema 5 (Teorema de Legendre)**.** *Seja $n = 4^k m$ um número inteiro positivo, com $k \geq 0$ e $m \not\equiv 0 \mod 4$. Então existem $a, b, c \in \mathbb{Z}$ tais que $n = a^2 + b^2 + c^2$, se, e somente se, $m \not\equiv 7 \mod 8$.*

Teorema 6 (Teorema de Lagrange (ou Teorema dos Quatro Quadrados))**.** *Todo número inteiro não negativo pode ser expresso como a soma de, no máximo, quatro quadrados perfeitos.*

Equações diofantinas estão associadas a outras funções além de polinomiais. Por exemplo, destacamos o Problema 374 de (PARVARDI, 2019), que reúne problemas olímpicos de matemática de diversas competições internacionais. Trata-se de determinar todos os inteiros positivos n para os quais a expressão

$$4^n + 6^n + 9^n$$

resulta num quadrado perfeito. Veremos a resolução no Problema 10.

Esse problema é um exemplo que pode ser formulado em termos de uma **equação diofantina exponencial**, que definiremos como equações do tipo

$$g(X_1, \ldots, X_n) = a \tag{3.3}$$

com $g(X_1, \ldots, X_n) = a_1^{X_1} + a_2^{X_2} + \ldots + a_n^{X_n}$, sendo $a, a_1, \ldots, a_n \in \mathbb{N}$ e as soluções em $\mathbb{N}$.

Conforme citado na Introdução, a ideia do método estudado neste capítulo é tratar equações dos tipos (3.1) e (3.3) sobre um corpo finito com p elementos, fazendo uso da projeção canônica

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{F}_p \\ r &\longmapsto \bar{r} = r + p\mathbb{Z}. \end{aligned}$$

Esta função é um homomorfismo de anéis, isto é, para todos $r, s \in \mathbb{Z}$, tem-se que $\overline{r+s} = \overline{r} + \overline{s}$ e $\overline{r \cdot s} = \overline{r} \cdot \overline{s}$. Isto permite considerar equações diofantinas originalmente sobre $\mathbb{Z}$, como equações sobre $\mathbb{F}_p$. Por exemplo, para a Equação 3.3, a correspondente equação reduzida é dada por

$$\overline{g}(X_1, \ldots, X_n) = \overline{a}$$

com $\overline{g}(X_1, \ldots, X_n) = \overline{a_1}^{X_1} + \overline{a_2}^{X_2} + \ldots + \overline{a_n}^{X_n}$.

A ideia central do método é que a não existência de soluções em $\mathbb{F}_p$, para algum número primo p, implica na não existência de soluções em $\mathbb{Z}$. A seguir, formalizamos esse princípio.

Proposição 7 (Redução Modular de Soluções Diofantinas)**.** *Se a Equação 3.1 (respectivamente, a Equação 3.3), possui uma solução sobre $\mathbb{Z}$, então para todo número primo p, a equação reduzida*

$$\overline{f}(X_1, \ldots, X_n) = \overline{0} \ \ (\textit{resp. } \overline{g}(X_1, \ldots, X_n) = \overline{a}), \tag{3.4}$$

possui uma solução sobre $\mathbb{F}_p$.

Demonstração. Façamos o caso da equação exponencial (a polinomial é análoga). Sejam $x_1, \ldots, x_n \in \mathbb{N}$ tais que $a_1^{x_1} + \ldots + a_n^{x_n} = a$ e seja p um número primo. Aplicando a projeção $\pi : \mathbb{Z} \to \mathbb{F}_p$, temos $\overline{a_1^{x_1} + \ldots + a_n^{x_n}} = \overline{a}_1^{x_1} + \ldots + \overline{a}_n^{x_n} = \overline{a}$. Assim, a equação reduzida também possui solução. □

O Corolário 8 segue imediatamente por contraposição da Proposição 7.

Corolário 8 (Método da Contradição Modular)**.** *Se existir um número primo p tal que a equação reduzida* (3.4) *não possui solução sobre $\mathbb{F}_p$, então as equações originais* (3.1) *e* (3.3) *também não possuem solução sobre $\mathbb{Z}$.*

Os exemplos subsequentes ilustram a aplicação prática deste método.

Problema 9 (Olimpíada de Matemática de Singapura de 1998)**.** *Verifique se existem números inteiros x e y tais que*

$$x^3 + y^4 = 19^{19}.$$

Solução Suponha que (x, y) é solução e vamos trabalhar módulo 13. Vejamos que $19^{19} \equiv 7 \mod 13$. De fato, pelo Pequeno Teorema de Fermat (Teorema 2), temos $19^{12} \equiv 1 \mod 13$. Assim, $19^{19} \equiv 19^{12} \cdot 19^7 \equiv 6^7 \equiv 7 \mod 13$. Agora note que $x^3 \equiv 0,\ 1,\ 5,\ 8$, ou $12 \mod 13$ e que $y^4 \equiv 0,\ 1,\ 3$ ou $9 \mod 13$. Desta forma, não se pode obter 7 nas possíveis somas residuais de x^3 com y^4. Logo, não há solução modular para $p = 13$. Portanto, a equação original também não possui solução.

Vamos agora resolver o problema mencionado antes da definição de equação exponencial (3.3). A estratégia é simples: para n ímpar, um argumento módulo 13 mostra que a expressão não pode ser quadrado; para n par, módulo 5 já é suficiente.

Problema 10. *Encontre os inteiros positivos n tais que $4^n + 6^n + 9^n$ seja um quadrado perfeito.*

Solução Iniciamos com o caso em que n é impar, examinando $A = 4^n + 6^n + 9^n$ módulo 13. Como $9 \equiv -4 \mod 13$, segue que

$$A \equiv 4^n + 6^n + (-4)^n \equiv 6^n \mod 13.$$

Basta então verificar que as potências ímpares de 6 módulo 13 não resultam em resíduos quadráticos. Temos $n = 12q + r$, para algum $q \in \mathbb{Z}$ e algum $r \in \{1, 3, 5, 7, 11\}$. Pelo Pequeno Teorema de Fermat, temos $6^n \equiv 6^r \mod 13$. Para $r = 1$, 3, 5, 7 e 11, temos $6^r \equiv 6$, 8, 2, 7 e $11 \mod 13$, respectivamente. Note que nenhum destes casos resulta em um resíduo quadrático módulo 13 (1, 3, 4, 9, 10 e 12). Assim, para n ímpar, concluímos que A não pode ser quadrado perfeito.
Para o caso em que n é par, temos $4 \equiv -1$, $6 \equiv 1$ e $9 \equiv -1 \mod 5$. Fazendo $n = 2k$, segue que

$$A \equiv (-1)^{2k} + 1^{2k} + (-1)^{2k} \equiv 3 \mod 5.$$

Como 3 é não-resíduo quadrático módulo 5, a expressão não pode ser quadrado perfeito.

Há um importante refinamento do Corolário 8 para o caso de equações homogêneas. Dizemos que a equação diofantina polinomial

$$f(X_1, \ldots, X_n) = 0 \tag{3.5}$$

é **homogênea de grau** α, onde α é um número inteiro ≥ 1, quando

$$f(tX_1, \ldots, tX_n) = t^\alpha f(X_1, \ldots, X_n),$$

para todo número inteiro $t \geq 0$. Note que esta equação sempre admite a solução trivial (composta somente de zeros). Um exemplo é uma equação do tipo $a_1X_1^2 + \ldots + a_nX_n^2 = 0$, com $a_1, \ldots, a_n \in \mathbb{Z}$, que é homogênea de grau 2.

Corolário 11 (Método da Contradição Modular para Equações Homogêneas)**.** *Considere a equação diofantina polinomial e homogênea de grau α dada em (3.5). Se existir um número primo p tal que a congruência $f(X_1, \ldots, X_n) \equiv 0 \mod p$ não possui solução* ***não trivial*** *sobre $\mathbb{F}_p$, então a Equação 3.5 também não possui solução* ***não trivial*** *sobre $\mathbb{Z}$.*

Demonstração. Suponha que os números inteiros $x_1, \ldots, x_n$ formam uma solução não trivial para a Equação 3.5. Então existe pelo menos um índice k tal que $x_k \neq 0$. Se $p \nmid x_k$, então $\overline{x}_k \neq \overline{0}$ em $\mathbb{F}_p$, garantindo a não trivialidade da solução reduzida. Se $p \mid x_k$ para todo k, então a homogeneidade garante que $(x_1/p, \ldots, x_n/p)$ também é solução. Fazendo $y_i = x_i/p$, reobtemos a mesma equação original, agora nas variáveis $Y_1, \ldots, Y_n$. Poderíamos então repetir o processo, caso p divida y_k, para todo k. Contudo, este processo não pode seguir indefinidamente, pois, caso contrário, os números que compõe a solução original poderiam ser fatorados indefinidamente, contradizendo o Teorema Fundamental da Aritmética (HEFEZ, 2022, Teorema 1.3.1). Desta forma, há solução não trivial sobre $\mathbb{F}_p$. □

O Corolário 11 pode ser utilizado no caso da equação homogênea do Problema 12.

Problema 12. *Determine, se existirem, as soluções não triviais da equação diofantina quadrática*

$$3X^2 + 5Y^2 - 7Z^2 = 0.$$

Solução Note que a equação é homogênea de grau 2. Se os números inteiros x, y e z formam uma solução, então a redução módulo 3 nos dá:

$$2y^2 \equiv z^2 \mod 3.$$

Se $z \not\equiv 0 \mod 3$, então $z^2 \equiv 1 \mod 3$ e temos $y^2 \equiv 2 \mod 3$. Mas isto é impossível, pois 2 não é resíduo quadrático módulo 3. Por outro lado, se $z \equiv 0 \mod 3$, então $y \equiv 0 \mod 3$. Segue que $y \equiv z \equiv 0 \mod 3$ e como consequência, a única solução módulo 3 é a trivial $x \equiv y \equiv z \equiv 0 \mod 3$. Pelo Corolário 11, a equação original não possui soluções não triviais.

3.0.1 UMA GENERALIZAÇÃO NATURAL

Nesta seção generalizamos o método da seção anterior substituindo o número primo p por um número inteiro $m > 1$. Neste caso, o quociente

$$\mathbb{Z}/m\mathbb{Z} = \left\{\overline{0},\ \ldots,\ \overline{m-1}\right\}$$

de $\mathbb{Z}$ pelo ideal $m\mathbb{Z} = \{m\alpha,\ |\ \alpha \in \mathbb{Z}\}$ é um anel comutativo com unidade.

As Equações 3.2 e 3.3 também podem ser consideradas em $\mathbb{Z}/m\mathbb{Z}$, por meio do homomorfismo dado pela projeção canônica

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ r &\longmapsto \bar{r} = r + m\mathbb{Z} \end{aligned}$$

ou seja, passamos a considerar as equações

$$f(X_1, \ldots, X_n) \equiv 0 \mod m \tag{3.6}$$

$$g(X_1, \ldots, X_n) \equiv a \mod m \tag{3.7}$$

onde f corresponde à equação polinomial (3.1) e g à equação exponencial (3.3).

O Corolário 8 pode ser estendido diretamente para este caso, ou seja, a não existência da solução módulo m, implica na não existência da solução da equação original.

Corolário 13 (Método da Contradição Modular Generalizado)**.** *Se existir um número inteiro $m > 1$ tal que a Equação 3.6 (resp. Equação 3.7) não possui solução módulo m, então a Equação 3.1 (resp. a Equação 3.3) também não possui solução sobre $\mathbb{Z}$.*

Um caso de particular interesse para resolução de problemas é $m = 8$, devido à grande utilidade do seguinte resultado elementar e seu corolário.

Proposição 14. *Seja a um número inteiro.*

(1) *Se a é ímpar, então $a^2 \equiv 1 \mod 8$.*

(2) *Se a é par, temos*

(2.1) $a^2 \equiv 4 \mod 8$, *se* $a \equiv 2 \mod 4$.

(2.2) $a^2 \equiv 0 \mod 8$, *se* $a \equiv 0 \mod 4$.

Demonstração. Para (1), se a é ímpar então a é da forma $4k + 1$ ou $4k + 3$. Assim, basta analisar módulo 8 o quadrado destes números. O item (2) é imediato. □

Segue uma primeira aplicação utilizando a Proposição 14.

Problema 15. *Determine, se existirem, todos os números inteiros ímpares a para os quais existe um número racional x tal que*

$$x^2 + ax + a = 0.$$

Solução A equação tem solução racional se, e somente se, seu discriminante Δ é um quadrado perfeito, ou seja, precisa existir um número inteiro positivo k tal que

$$\Delta = a^2 - 4a = k^2.$$

Sendo a ímpar, pela Proposição 14[1], temos $\Delta \equiv -3 \equiv 5 \mod 8$, assim Δ não é um quadrado perfeito, o que implica que não existe o número a requerido.

O próximo problema é um caso particular do Teorema de Legendre (Teorema 5).

Problema 16. *Verifique se* 2023 *é a soma de três quadrados.*

Solução Temos $2023 \equiv 7 \mod 8$. Pela Proposição 14, se a é um número inteiro então $a^2 \equiv 0,\ 1$ ou $4 \mod 8$. Considerando todas as somas $x^2 + y^2 + z^2$, módulo 8, com $x^2, y^2, z^2 \in \{0, 1, 4\}$, não ocorre a soma igual a 7. Consequentemente, para quaisquer inteiros x, y, z, temos $x^2+y^2+z^2 \not\equiv 7 \mod 8$. Pelo Corolário 13, 2023 não é soma de três quadrados.

Problema 17 (Questão 4, Fase Regional da Olimpíada Austríaca de Matemática de 2025)**.** *Seja z um inteiro positivo não divisível por* 8 *e um inteiro $n \geq 2$. Mostre que nenhum dos números*

$$z^n + z + 1$$

é um quadrado perfeito.

Solução: Suponha, por contradição, que $N = z^n + z + 1$ é um quadrado perfeito e vamos analisar $N \mod 8$. Pela Proposição 14, os quadrados módulo 8 correspondem a 0, 1 ou 4. No entanto, para $z \not\equiv 0 \mod 8$, verifica-se diretamente que $N \equiv 3$, 5, ou $7 \mod 8$, exceto no caso em que $z \equiv 7 \mod 8$ e n é par, onde $N \equiv 1 \mod 8$. Para os casos em que $N \equiv 3,\ 5,\ 7 \mod 8$, temos uma contradição, pois esses valores não são quadrados módulo 8. No caso excepcional $z \equiv 7 \mod 8$ com n par, temos $N \equiv 1 \mod 8$. Aqui, z é ímpar, e escrevendo $z = 2k + 1$, obtemos $N = (2k + 1)^n + (2k + 1) + 1$. Para n par, $(2k + 1)^n \equiv 1 \mod 4$, logo $N \equiv 2k + 3 \mod 4$. Se k é par, $N \equiv 3 \mod 4$, o que é impossível para um quadrado (já que quadrados são 0 ou $1 \mod 4$). Assim, restamos com k ímpar, onde $N \equiv 1 \mod 4$. Analisamos agora módulo 3. Como $z \equiv 7 \equiv 1 \mod 3$, temos $z^n \equiv 1 \mod 3$ e $z \equiv 1 \mod 3$, logo $N \equiv 1 + 1 + 1 = 3 \equiv 0 \mod 3$. Portanto, $3 \mid N$. Para N ser um quadrado, devemos ter $9 \mid N$. No entanto, para $z \equiv 1 \mod 3$, temos $z = 3t + 1$, e então $N = z^n + z + 1 \equiv 1 + 1 + 1 = 3 \mod 9$, uma vez que $z^n \equiv 1 \mod 9$ para n par pelo Teorema 3. Assim, $N \not\equiv 0 \mod 9$, contradizendo a condição necessária para que N seja um quadrado perfeito. Concluímos que N não pode ser um quadrado perfeito em nenhum caso.

4 O TEOREMA DE GRUNWALD-WANG E O LEMA DE HENSEL

Neste capítulo estudamos o corpo dos números p-ádicos e exploramos suas principais propriedades. Manteremos a abordagem o mais elementar possível e restrita ao necessário para os objetivos do nosso trabalho. Detalhes e demonstrações omitidas podem ser encontradas no livro de Gouvêa (GOUVÊA, 1989), que será nossa principal referência.

O propósito principal deste capítulo é estudar dois resultados essenciais para o nosso método a ser explorado no Capítulo 5. Primeiro, veremos o Teorema de Grunwald-Wang para o caso de quadrados, que estabelece que um número racional é um quadrado, se e somente se, é um quadrado no corpo dos números p-ádicos, para todo número primo p, e em $\mathbb{R}$. Na sequência, estudamos o Lema de Hensel, que permitirá, sob certas condições, reduzir o problema de calcular quadrados de inteiros p-ádicos para o cálculo de resíduos quadráticos módulo p.

4.0.1 OS NÚMEROS p-ÁDICOS E O TEOREMA DE GRUNWALD-WANG PARA QUADRADOS

Os números p-ádicos foram concebidos, por volta de 1897, pelo matemático alemão Kurt Hensel. Ele estava, junto com Weierstress, em busca de métodos para desenvolver funções em séries de potências. Já nessa época, ele usou os números p-ádicos para resolver vários problemas de teoria dos números.

Na Teoria Elementar dos Números (HEFEZ, 2022, Capítulo 1), temos que a representação de um número inteiro positivo x na base p (p primo) é dada por:

$$x = a_0 + a_1 p + \ldots + a_n p^n$$

onde $a_0, \ldots, a_n \in \{0, 1, \ldots, p-1\}$ e $a_n \neq 0$. Denota-se $x = (a_n \ldots a_1 a_0)_p$.

Para $m \geq n+1$, tem-se $a_m = 0$ e obtemos a expressão

$$x = a_0 + a_1 p + \ldots + a_n p^n + 0p^{n+1} + 0p^{n+2} + \ldots$$

que chamaremos de expansão p-ádica de x na base p. Séries formais deste tipo, em que também podem aparecer infinitos coeficientes não nulos, são conhecidas na literatura como inteiros p-ádicos (GOUVÊA, 1989, Capítulo 2), conforme a seguinte definição.

Definição 18. *Seja p um número primo. Um **inteiro p-ádico** é uma soma formal*

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \ldots$$

onde cada dígito a_i é um número inteiro satisfazendo $0 \leq a_i \leq p-1$. O conjunto de todos os inteiros p-ádicos é denotado por $\mathbb{Z}_p$. Desta forma,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, \ldots, p-1\} \right\}.$$

As operações de adição e multiplicação em $\mathbb{Z}_p$ seguem as operações com inteiros escritos na base p. Por exemplo, para $p = 3$, $17 + 25 = (122)_3 + (221)_3 = (1120)_3 = 42$ e $17 \times 25 = (122)_3 \times (221)_3 = (202021)_3 = 425$. De maneira mais intuitiva:

$$\begin{array}{cccc} & 1 & 2 & 2 \\ + & 2 & 2 & 1 \\ \hline 1 & 1 & 2 & 0 \end{array} \qquad \begin{array}{cccccc} & & & 1 & 2 & 2 \\ & & \times & 2 & 2 & 1 \\ \hline & & & 1 & 2 & 2 \\ & 1 & 0 & 2 & 1 & \\ 1 & 0 & 2 & 1 & & \\ \hline 1 & 2 & 0 & 2 & 0 & 2 \end{array}$$

Estas operações conferem a $\mathbb{Z}_p$ uma estrutura de anel comutativo com unidade, onde:

- O elemento neutro aditivo é $0 = 0 + 0p + 0p^2 + \ldots$
- A unidade multiplicativa é $1 = 1 + 0p + 0p^2 + \ldots$

Conforme (GOUVÊA, 1989), a representação p-ádica de -1 é $\sum_{i=0}^{\infty}(p-1)p^i$ e o inverso aditivo de $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ é dado por

$$-x = (p - a_0) + \sum_{i=1}^{\infty}(p - 1 - a_i)p^i.$$

Pode-se ainda mostrar que o anel $\mathbb{Z}_p$ é um domínio de integridade: se $x, y \in \mathbb{Z}_p$ e $xy = 0$, então $x = 0$ ou $y = 0$. Finalmente, as unidades de $\mathbb{Z}_p$ (elementos invertíveis) podem ser caracterizadas de forma simples através de sua representação p-ádica:

Proposição 19. *Um elemento $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ é uma unidade se, e somente se, $a_0 \neq 0$.*

Demonstração. Se x é uma unidade, então existe $y = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ tal que $xy = 1$. Reduzindo esta igualdade módulo p, obtemos $a_0 b_0 \equiv 1 \mod p$, o que implica $a_0 \neq 0$. Reciprocamente, se $a_0 \neq 0$, podemos construir o inverso multiplicativo $y = \sum_{i=0}^{\infty} b_i p^i$ de x definindo recursivamente os dígitos b_i

através das condições:

$$\begin{aligned} a_0 b_0 &\equiv 1 \mod p \\ a_0 b_1 + a_1 b_0 &\equiv 0 \mod p \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &\equiv 0 \mod p \\ &\vdots \end{aligned}$$

Cada equação pode ser resolvida unicamente para b_i pois a_0 é invertível módulo p. □

Para obter um corpo a partir do anel $\mathbb{Z}_p$, estende-se este último para incluir potências negativas de p, seguindo a construção apresentada em (GOUVÊA, 1989) e (QUADROS, 2019).

Definição 20. *Um **número p-ádico** é uma soma formal*

$$\sum_{i=-m}^{\infty} a_i p^i = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$$

onde $m \in \mathbb{N}$, $0 \leq a_i \leq p-1$ para todo $i \geq -m$ e $a_{-m} \neq 0$. O conjunto de todos os números p-ádicos é denotado por $\mathbb{Q}_p$. Assim,

$$\mathbb{Q}_p = \left\{ \sum_{i=-m}^{\infty} a_i p^i,\ m \in \mathbb{N},\ \ a_i \in \mathbb{Z} \ \ \textit{e} \ \ 0 \leq a_i \leq p-1 \right\}.$$

Exemplo 4.1. *Em $\mathbb{Q}_3$, o número racional $\frac{1}{3}$ se escreve como:*

$$\frac{1}{3} = 1 \cdot 3^{-1} + 0 + 0 \cdot 3 + 0 \cdot 3^2 + \cdots = (0,1)_3$$

enquanto que $\frac{1}{2}$ em $\mathbb{Q}_3$ possui a expansão:

$$\frac{1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots = (2,1,1,1,\ldots)_3.$$

Em geral, todo número racional $\dfrac{a}{b},\ b \neq 0$, pode ser expresso como uma soma formal em $\mathbb{Q}_p$ (GOUVÊA, 1989). Desta forma, há uma inclusão natural $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ do corpo dos números racionais em cada corpo p-ádico, que simplesmente associa um número racional à sua expansão p-ádica. Conforme o teorema a seguir, $\mathbb{Q}_p$ é um corpo. De fato, o corpo $\mathbb{Q}_p$ é o completamento, na norma p-ádica, do corpo dos números racionais (GOUVÊA, 1989).

Teorema 21. *O conjunto $\mathbb{Q}_p$ é um corpo sob as operações de adição e multiplicação estendidas de $\mathbb{Z}_p$ e contém $\mathbb{Z}_p$ como subanel. Ainda mais, todo elemento não nulo $x \in \mathbb{Q}_p$ pode ser escrito unicamente na forma*

$$x = p^m u \tag{4.1}$$

onde $m \in \mathbb{Z}$ e u é uma unidade em $\mathbb{Z}_p$. Por fim,

$$\mathbb{Z}_p = \Big\{ x \in \mathbb{Q}_p : x = p^m u, \textit{ para alguma unidade } u \textit{ e algum } m \geq 0 \Big\}.$$

A demonstração completa por ser vista em (GOUVÊA, 1997, Teorema 3.2.3). A existência da representação $x = p^m u$ decorre do fato de que para qualquer $x = \sum_{i=-m}^{\infty} a_i p^i$ com $a_{-m} \neq 0$, temos

$$x = p^{-m}\left(a_{-m} + a_{-m+1}p + a_{-m+2}p^2 + \cdots\right) = p^{-m}u$$

onde $u = \sum_{j=0}^{\infty} a_{j-m}p^j$ é uma unidade em $\mathbb{Z}_p$, pois $a_{-m} \neq 0$. A unicidade segue da própria construção da representação p-ádica.

Conforme citamos após o Exemplo 4.1, há uma inclusão natural de $\mathbb{Q}$ em $\mathbb{Q}_p$, para todo número primo p. Juntando com a inclusão natural $\mathbb{Q} \hookrightarrow \mathbb{R}$, obtemos uma aplicação

$$i : \mathbb{Q} \longrightarrow \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3 \times \cdots = \mathbb{R} \times \prod_{p \text{ primo}} \mathbb{Q}_p \tag{4.2}$$

pela qual identificamos um número racional x com sua expansão p-ádica, para todo primo p.

Finalmente, podemos enunciar o Teorema de Grunwald-Wang para o caso que nos interessa.

Teorema 22 (Teorema de Grunwald-Wang para Quadrados)**.** *Um número racional é um quadrado em $\mathbb{Q}$ se, e somente se, é um quadrado em $\mathbb{R}$ e em $\mathbb{Q}_p$, para todo primo p.*

Cabe ressaltar que este teorema tem uma versão mais geral (WANG, 1950) que trata de potências n-ésimas de números racionais (ao invés de somente quadrados) e também permite a exclusão de um número finito de primos na aplicação i.

Demonstração. (do Teorema 22) Suponha que $r \in \mathbb{Q}$ é um quadrado em $\mathbb{Q}$, ou seja, existe $s \in \mathbb{Q}$ tal que $r = s^2$. Como $\mathbb{Q} \subset \mathbb{R}$, temos $s \in \mathbb{R}$, logo $r = s^2$ é um quadrado em $\mathbb{R}$. Analogamente, para todo primo p, temos $\mathbb{Q} \subset \mathbb{Q}_p$, portanto $s \in \mathbb{Q}_p$ e $r = s^2$ é um quadrado em $\mathbb{Q}_p$. Para a outra direção, suponha que $r \in \mathbb{Q}$, $r \neq 0$, e que $x^2 = r$ tem solução em $\mathbb{R}$ e em $\mathbb{Q}_p$ para todo primo p. Vejamos que r é um quadrado em $\mathbb{Q}$. Seja $\text{ord}_p(r)$ o expoente de p na fatoração de r (pode ser positivo, negativo ou zero). Como r é um quadrado em $\mathbb{Q}_p$, existe $u_p \in \mathbb{Q}_p$ tal que $r = u_p^2$. Então:

$$\text{ord}_p(r) = \text{ord}_p(u_p^2) = 2 \cdot \text{ord}_p(u_p).$$

Logo, $\text{ord}_p(r)$ é divisível por 2 para todo primo p. Segue que na fatoração de r em produto de números primos, todos os expoentes são múltiplos de 2. Isso significa que podemos escrever r como o produto abaixo, no qual só aparecem os números primos p para os quais $\text{ord}_p(r) \neq 0$ (e portanto, é um produto finito):

$$r = \prod_p p^{2 \cdot k_p} = \left(\prod_p p^{k_p}\right)^2.$$

□

4.0.2 O LEMA DE HENSEL E OS QUADRADOS EM $\mathbb{Z}_p$

O Lema de Hensel, formulado por Kurt Hensel em 1897, constitui uma das ferramentas mais poderosas da aritmética p-ádica, permitindo o levantamento de soluções aproximadas de equações polinomiais para soluções exatas em $\mathbb{Z}_p$. Para enunciá-lo, definimos a **derivada formal** do polinômio $f(X) = a_0 + a_1X + \ldots + a_nX^n$ como o novo polinômio

$$f'(X) = a_1 + a_2X + \ldots + na_nX^{n-1}.$$

Teorema 23 (Lema de Hensel)**.** *Seja $f(X)$ um polinômio com coeficientes em $\mathbb{Z}_p$. Se existe $\alpha_0 \in \mathbb{Z}_p$ tal que:*

(1) $f(\alpha_0) \equiv 0 \mod p$ *e*

(2) $f'(\alpha_0) \not\equiv 0 \mod p$*,*

então existe um único $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ e $\alpha \equiv \alpha_0 \mod p$.

Demonstração. (ideia) (GOUVÊA, 1997, Teorema 3.4.1). Define-se uma sequência de aproximações $\{\alpha_n\}$ recursivamente por

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}.$$

Utilizando a hipótese $f'(\alpha_0) \not\equiv 0 \mod p$, demonstra-se por indução que $f(\alpha_n) \equiv 0 \mod p^{n+1}$, $f(\alpha_n) \equiv 0 \mod p^{n+1}$ e $\alpha_{n+1} \equiv \alpha_n \mod p^{n+1}$, para todo inteiro $n \geq 1$. Na métrica p-ádica, a sequência $\{\alpha_n\}$ converge para um limite $\alpha \in \mathbb{Z}_p$ que satisfaz $f(\alpha) = 0$. □

Conforme sugere a demonstração, o Lema de Hensel representa o análogo p-ádico do método de Newton do cálculo real e apresenta aplicações profundas em Teoria dos Números, incluindo o estudo de resíduos quadráticos e formas quadráticas.

Como um primeiro exemplo, vamos mostrar que 2 é um quadrado em $\mathbb{Z}_7$.

Exemplo 4.2. *Considere o polinômio $f(X) = X^2 - 2 \in \mathbb{Z}_7[X]$. Dado que $3^2 \equiv 2 \mod 7$ e $f'(3) = 6 \not\equiv 0 \mod 7$, o Lema de Hensel garante a existência de uma raiz quadrada de 2 em $\mathbb{Z}_7$. Efetivamente,*

$$\sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \ldots$$

em $\mathbb{Z}_7$.

O argumento principal do Exemplo 4.2 pode ser generalizado de maneira direta. Na Proposição 24 temos uma aplicação importante do Lema de Hensel, que permite o levantamento das raízes de um polinômio da forma $X^2 - a$.

Proposição 24. *Seja p um número primo ímpar. Sendo u uma unidade em $\mathbb{Z}_p$ e $\bar{u}$ sua classe em $\mathbb{F}_p$, tem-se que u é um quadrado em $\mathbb{Z}_p$ se, e somente se, u é um resíduo quadrático módulo p.*

Demonstração. A implicação é imediata, pois se $u = \alpha^2$ para algum $\alpha \in \mathbb{Z}_p$, então reduzindo módulo p, temos $\overline{u} = \overline{\alpha}^2$ em $\mathbb{F}_p$. Para a recíproca, aplica-se o Lema de Hensel (Teorema 23) ao polinômio $f(X) = X^2 - u$, cuja derivada formal é $f'(X) = 2X$. Sendo u um resíduo quadrático módulo p, existe $\overline{\alpha_0} \in \mathbb{F}_p$ tal que $u \equiv \alpha_0^2 \mod p$. Como p é ímpar, $2\alpha_0 \not\equiv 0 \mod p$. Logo, $f'(\alpha_0) \not\equiv 0 \mod p$. Pelo Lema de Hensel, existe $\alpha \in \mathbb{Z}_p$ tal que $\alpha^2 = u$. □

Vimos no Teorema 21 que todo elemento não nulo $z \in \dot{\mathbb{Q}}_p$ possui uma representação única da forma $z = p^m u$, onde $m \in \mathbb{Z}$ e u é uma unidade em $\mathbb{Z}_p$. Portanto, z é um quadrado em $\mathbb{Q}_p$ se, e somente se, m é par e u é um quadrado em $\mathbb{Z}_p$. Segue o seguinte resultado.

Corolário 25. *Seja p um número primo ímpar e $z \in \dot{\mathbb{Q}}_p$. Temos*

$$z \in \dot{\mathbb{Q}}_p^2 \iff z = p^{2n}u,$$

para algum número natural $n \geq 1$ e alguma unidade $u \in \mathbb{Z}_p$.

Observe que o Lema de Hensel, argumento principal na demonstração da Proposição 24, só pode ser aplicado ao polinômio $X^2 - u$ porque o primo p foi escolhido diferente de 2. Caso contrário, teríamos a derivada igual a zero. Para o caso $p = 2$, os quadrados são caracterizados na Proposição 26, cuja demonstração completa pode ser encontrada em (GOUVÊA, 1997). Faremos somente a implicação.

Proposição 26. *Uma unidade $u \in \mathbb{Z}_2$ é um quadrado em $\mathbb{Z}_2$ se, e somente se, $u \equiv 1 \mod 8$.*

Demonstração. Para a implicação, suponha que u seja um quadrado em $\mathbb{Z}_2$, ou seja, existe $v \in \mathbb{Z}_2$ tal que $u = v^2$. Como u é uma unidade, v também é uma unidade, e portanto $v \equiv 1 \mod 2$. Podemos escrever v na forma $v = 1 + 2a$, onde $a \in \mathbb{Z}_2$. Elevando ao quadrado, obtemos:

$$u = v^2 = (1 + 2a)^2 = 1 + 4a + 4a^2 = 1 + 4a(a + 1).$$

Como $a(a + 1)$ é par, temos $4a(a + 1) \equiv 0 \mod 8$ e portanto, $u \equiv 1 \mod 8$. □

Corolário 27. *Um elemento não nulo $z \in \mathbb{Q}_2$ é um quadrado se, e somente se, é da forma*

$$z = 2^{2n}u,$$

onde $n \in \mathbb{Z}$ e u é uma unidade em $\mathbb{Z}_2$ tal que $u \equiv 1 \mod 8$.

5 O MÉTODO LOCAL-GLOBAL - UMA PROPOSTA PARA PROBLEMAS OLÍMPICOS

Neste capítulo compilamos os principais resultados explorados no capítulo anterior para obter o Método Local-Global (Teorema 29) e exibir a aplicação à Questão 6 da IMO de 1998. Em resumo, o método estabelece que um número inteiro é um quadrado perfeito quando é um resíduo quadrático módulo p, para todo número primo ímpar p e satisfaz uma condição extra para $p = 2$. Apesar de usar conceitos como números p-ádicos, a aplicação do método pode ser feita de maneira elementar. Essa é sua principal vantagem para uso em olimpíadas de matemática.

Iniciamos com um caso particular do Lema de Hensel (Teorema 23). Basta aplicar o Teorema 23 ao polinômio $X^2 - a$, conforme fizemos no Exemplo 4.2.

Teorema 28 (Lema de Hensel - Versão Quadrática)**.** *Seja p um número primo ímpar. Se $x \in \mathbb{Z}$ e existe um inteiro r tal que*

$$x \equiv r^2 \mod p \quad \textit{e} \quad p \nmid r,$$

então existe um inteiro p-ádico $\tilde{r}$ tal que $\tilde{r} \equiv r \mod p$ e $x = \tilde{r}^2$ em $\mathbb{Z}_p$.

Pelo Corolário 27, uma condição suficiente para que o inteiro x seja um quadrado em $\mathbb{Q}_2$ é que

(a) Existe um inteiro $n \geq 1$ tal que $x \equiv 4^n \mod 8$, se x é par, ou

(b) $x \equiv 1 \mod 8$, se x é ímpar.

Juntando todos os resultados, nosso método é o seguinte:

Teorema 29 (Método Local-Global)**.** *Seja x um número inteiro positivo. Suponha que*

(1) $x \equiv 1 \mod 8$ *ou* $x \equiv 4^n \mod 8$*, para algum $n \geq 1$, e*

(2) *Para todo número primo ímpar p, existe $r \in \mathbb{Z}$, tal que p não divide r e $x \equiv r^2 \mod p$.*

Então, x é um quadrado perfeito.

Demonstração. Pelo Teorema de Grunwald-Wang (Teorema 22) temos que $x = \alpha^2$, para algum número racional α, se x é um quadrado em $\mathbb{R}$ e em $\mathbb{Q}_p$, para todo número primo p. Como x é positivo, ele já é um quadrado real. Conforme citado antes do enunciado, o item (1) garante que x é um quadrado em $\mathbb{Q}_2$. Para $p > 2$, a versão quadrática do Lema de Hensel (Teorema 28) garante que

x é um quadrado em $\mathbb{Z}_p$ (e portanto em $\mathbb{Q}_p$). Desta forma, $x = \alpha^2$, com $\alpha \in \mathbb{Q}$. Para ver que α tem que ser inteiro, provaremos que

$$\mathbb{Q}^2 \cap \mathbb{Z} = \mathbb{Z}^2 = \{m^2 \mid m \in \mathbb{Z}\}.$$

A inclusão $\mathbb{Z}^2 \subseteq \mathbb{Q}^2 \cap \mathbb{Z}$ é imediata. Seja $\alpha = \dfrac{a}{b} \in \mathbb{Q}$, com $b \neq 0$ e $\text{mdc}(a, b) = 1$, tal que $\alpha^2 = \dfrac{a^2}{b^2} \in \mathbb{Z}$, ou seja, b^2 divide a^2. Como $\text{mdc}(a, b) = 1$, temos que $\text{mdc}(a^2, b^2) = 1$. Mas b^2 divide a^2 e $\text{mdc}(a^2, b^2) = 1$, implica que $b^2 = 1$. Portanto, $\alpha = a^2$. □

5.0.1 APLICAÇÃO À CLÁSSICA QUESTÃO 6 DA IMO DE 1988

A Olimpíada Internacional de Matemática (IMO) de 1988 foi realizada em Canberra, Austrália, e contou com a participação de 49 países.

A competição ficou marcada pela Questão 6 da prova do segundo dia do evento, até hoje considerada uma das mais difíceis e famosas da história da competição.

Antes de decidir incluir a questão na prova e marcá-la com duplo asterisco, a banca submeteu a questão a matemáticos australianos, que trabalham com teoria dos números, e deu-lhes 6 horas para resolver o problema. Nenhum foi capaz de fazê-lo.

Assim, a Questão 6 entrou para a história não apenas por sua notória dificuldade, mas pelo seleto grupo de jovens mentes brilhantes que conseguiram desvendá-la. Entre os 268 participantes daquele ano, onze alcançaram a solução completa.

Muitos competidores tentaram abordagens algébricas diretas, como fatoração ou análise de casos particulares com números pequenos, mas não conseguiram avançar. Alguns perceberam que a equação lembrava a desigualdade de Cauchy-Schwarz ou relações de recorrência, mas não sabiam como estruturar uma prova rigorosa.

Segue o enunciado, em tradução direta da prova.

Problema 30 (Questão 6 - IMO-1998)**.** *Sejam a e b números inteiros positivos tais que $1 + ab$ divide $a^2 + b^2$. Mostre que*

$$\frac{a^2 + b^2}{1 + ab}$$

é o quadrado de um número inteiro.

A solução clássica utiliza o método de Vieta Jumping (VOELZ; DARIO, 2019). Assume-se que existe um contra-exemplo de tal forma que a soma $a+b$ seja mínima e, na sequência, encontra-se uma solução cuja soma é menor, obtendo-se uma contradição com a minimalidade. Outra abordagem utiliza de maneira semelhante a Descida Infinita de Fermat (VOELZ; DARIO, 2019). Estes métodos ficaram conhecidos em competições de matemática por causa de sua aplicação à Questão 6.

Uma solução alternativa foi apresentada em termos geométricos por Sanchez Alfaro (ALFARO, 2011).

Uma generalização foi apresentada em (CAMPBELL, 1988). Foi demonstrado por indução que se k é um inteiro tal que $(1+ab)k = a^2+b^2$, então $k = \mathrm{mdc}(a,b)^2$. Introduz-se um inteiro $c = ak - b$, com $0 \leq c < b$, e mostra-se que $\mathrm{mdc}(a,b) = \mathrm{mdc}(a,c)$, permitindo reduzir o problema a um caso com soma menor e concluir a indução.

Contudo, até hoje não foi apresentada uma solução utilizando somente as técnicas clássicas da Teoria Elementar dos Números, como congruências e resíduos quadráticos. Apresentamos nesta seção uma solução utilizando o nosso método (Teorema 29). Na nossa abordagem utilizaremos parcialmente o argumento indutivo citado acima, mas sem a necessidade de verificar que k deva ser o máximo divisor comum de a e b.

Estudando soluções particulares do problema, percebemos que só aparecem determinados números primos na fatoração do número $1+ab$. Por exemplo, sendo k o quociente do enunciado, alguns pares de soluções são $(2,8)$, $(30,8)$ e $(3,27)$, com $k = 4$, 4 e 9, respectivamente. Note que nas fatorações

$$\underbrace{(1+2\times 8)}_{17}\ k = \underbrace{2^2+8^2}_{4\times 17}$$

$$\underbrace{(1+30\times 8)}_{241}\ k = \underbrace{30^2+8^2}_{4\times 241}$$

$$\underbrace{(1+3\times 27)}_{41\times 2}\ k = \underbrace{3^2+27^2}_{9\times 82}$$

os fatores primos de $1+ab$ deixam resto 1 na divisão por 8, se ímpares. Isto motivou a Afirmação abaixo. Para a demonstração, lembramos que a **ordem** $\mod p$ de um número inteiro x é o menor número natural $\mathrm{ord}_p(x)$ tal que $x^{\mathrm{ord}_p(x)} \equiv 1 \mod p$, onde p é um número primo. Ainda, se n é um número natural tal que $x^n \equiv 1 \mod p$, então $n \mid \mathrm{ord}_p(x)$.

Afirmação Sejam a e b como no Problema 30. Seja $p > 2$ um número primo que divide $1+ab$. Então $p \equiv 1 \mod 8$. Consequentemente, se $1+ab$ é ímpar, então $1+ab \equiv 1 \mod 8$.
Demonstração Das hipóteses, $p \mid a^2+b^2$. Assim, $a^2 \equiv -b^2 \mod p$. Substituindo em $ab \equiv -1 \mod p$, temos que $a^4+1 \equiv 0 \mod p$, o que implica $a^4 \equiv -1 \mod p$. Elevando ambos os lados ao quadrado, obtemos $a^8 \equiv 1 \mod p$. Logo, a ordem de a módulo p é 8. Do Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \mod p$. Portanto, 8 divide $p-1$.

A partir desta Afirmação, podemos resolver a questão utilizando nosso método local-global para quadrados perfeitos.

Solução (do Problema 30). Seja k o número inteiro tal que

$$k = \frac{a^2 + b^2}{1 + ab}.$$

Dado que k é positivo, nosso método requer que provemos as duas condições do Teorema 29. Faremos:

Parte 1: $k \equiv 1 \mod 8$ ou $k \equiv 4^n \mod 8$, para algum $n \geq 1$.

Parte 2: Se $p > 2$ é primo, então $k \equiv \alpha^2 \mod p$ e $p \nmid \alpha$.

Para a Parte 1, assumiremos inicialmente que a ou b é par e faremos $a = 2^\alpha m$ e $b = 2^\beta n$, com $\alpha, \beta \geq 0$ e $2 \nmid mn$. Pela simetria, podemos também assumir $\alpha \leq \beta$. Então

$$(1 + ab)k = a^2 + b^2 \Rightarrow (1 + 2^{\alpha+\beta}mn)k = 4^\alpha m^2 + 4^\beta n^2.$$

Façamos $mn = 1 + 2t$, para algum inteiro t. Temos as seguintes possibilidades:

- **Caso 1**: $\alpha = 0$ e $\beta = 1$. Segue que $1+2^{\alpha+\beta}mn = (1+2(1+2t)) = 3+4t$, que é congruente a 3 ou 7 $\mod 8$, contradizendo a Afirmação. Desta forma, este caso não ocorre.
- **Caso 2**: $\alpha = \beta = 1$. Temos $1 + ab = 1 + 4mn \equiv 5 \mod 8$, que também não ocorre.
- **Caso 3**: $\alpha + \beta \geq 3$. Temos $1 + ab \equiv 1 \mod 8$ e

  $$k \equiv a^2 + b^2 \equiv 4^\alpha m^2 + 4^\beta n^2 \equiv 4^\alpha + 4^\beta \equiv 4^\alpha \mod 8,$$

  pois $m^2 \equiv n^2 \equiv 1 \mod 8$ e como $\alpha \leq \beta$, podemos assumir $\beta \geq 2$ ($\Rightarrow 4^\beta \equiv 0 \mod 8$).

Para concluir a Parte 1, ainda precisamos resolver o caso em que a e b são ímpares. Façamos $a = dm$ e $b = dn$, com $d =$mdc(a, b) e mdc$(m, n) = 1$. Temos $1 + ab \equiv 2 \mod 4$. Da Afirmação, segue que $1 + ab = 2c$, com $c \equiv 1 \mod 8$. Assim, $1 + ab \equiv 2 \mod 8$. Por outro lado,

$$a^2 + b^2 = d^2(m^2 + n^2).$$

Sendo $m = 2u + 1$ e $n = 2v + 1$, verifica-se diretamente que

$$m^2 + n^2 = (2u + 1)^2 + (2v + 1)^2 = 2((u + v + 1)^2 + (v - u)^2).$$

Juntando as informações na igualdade $(1 + ab)k = d^2(m^2 + n)^2$, temos

$$2ck = d^2 2(x^2 + y^2),$$

com $x = u + v + 1$ e $y = v - u$, possuindo paridades distintas. Lembrando que $c \equiv 1 \mod 8$, segue que

$$k \equiv d^2(x^2 + y^2) \mod 8. \tag{5.1}$$

Agora observe que:

- $x + y = n$
- $x - y = m$
- Temos $mn \equiv 1 \mod 8$ (o que implica que $m \equiv n \mod 8$).

Para verificar o último item note que $1 + ab \equiv 2 \mod 8$ implica em $d^2mn \equiv 1 \mod 8$, e temos $d^2 \equiv 1 \mod 8$, pois d é ímpar. Dos três itens acima, concluímos que $2y \equiv 0 \mod 8$, ou seja, $y \equiv 4 \mod 8$. Consequentemente,

$$k \equiv d^2(x^2 + 4^2) \equiv x^2 \equiv 1 \mod 8.$$

A última congruência segue do fato que x é ímpar (pois y é par e x e y possuem paridades distintas).

Parte 2: Seja p um número primo ímpar, a, b e k como no Problema 30. Podemos assumir $a \leq b$. Utilizaremos indução sobre ab para mostrar que existe $\alpha \in \mathbb{Z}$ tal que $k \equiv \alpha^2 \mod p$ e $p \nmid \alpha$. Para o caso-base da indução, assumimos que $ab = 1$. Como a única possibilidade é $a = b = 1$, substituindo na expressão de k módulo p, temos

$$2k \equiv 2 \mod p.$$

Como mdc$(2, p) = 1$, segue que $k \equiv 1^2 \mod p$ e é claro que p não divide 1. Agora suponha $ab > 1$ e o resultado válido para os produtos menores que ab (hipótese de indução). Seja

$$c = ak - b.$$

Vejamos que

(a) $(1 + ac)k = a^2 + c^2$.

(b) $0 < c < b$.

Para (a), a verificação é direta:

$$a^2 + c^2 = a^2 + b^2 - 2abk + a^2k^2 = (1 + ab)k + a^2k^2 - 2abk = (1 + (ak - b)a)k = (1 + ac)k.$$

Para (b), temos da definição de k que $1 + ac > 0$, o que implica em $c > -1/a$. Portanto, $c > 0$. Para ver que $c < b$, note que

$$k < \frac{a^2 + b^2}{ab} = \frac{a}{b} + \frac{b}{a},$$

o que nos dá $ak < \dfrac{a^2}{b} + b \leq \dfrac{b^2}{b} + b = 2b$. Logo, $ak - b < b$, ou seja, $c < b$.

Assim, $0 < ac < ab$. Pela hipótese de indução, existe um inteiro α tal que $\dfrac{a^2 + c^2}{1 + ac} \equiv \alpha^2 \mod p$ e p não divide α. Mas este quociente é justamente k, o que nos dá direto a conclusão desejada.

6 PROPOSTA DE ATIVIDADES

Este capítulo apresenta duas propostas pedagógicas que mostram como os temas números p-ádicos, quadrados perfeitos e equações diofantinas podem ser abordados para diferentes níveis de ensino, desde a educação básica até a formação continuada de professores.

A primeira parte aborda o desafio de introduzir o conceito de números 2-ádicos para estudantes do sétimo ano do ensino fundamental. Através de uma abordagem elementar, mostramos como é possível construir a noção de número p-ádico a partir de uma equação simples, permitindo que os alunos compreendam a existência de estruturas numéricas além dos conjuntos tradicionais.

A segunda proposta desenvolve uma sequência didática explorando as datas pitagóricas no ano de 2025. Esta proposta conecta conceitos de teoria dos números com elementos do cotidiano dos estudantes, promovendo uma aprendizagem significativa através da investigação matemática. Através dessas aplicações, buscamos mostrar que tópicos avançados da matemática podem ser acessíveis e relevantes para a educação básica quando adequadamente contextualizados.

6.0.1 EXPLICANDO UM NÚMERO 2-ÁDICO PARA UM ESTUDANTE DO SÉTIMO ANO

Uma forma de elementar de construir um número 2-ádico particular, de forma que um estudante da educação básica possa entender, é através da equação

$$x + 1 = 0$$

sobre o conjunto dos números naturais. Como seria uma tentativa de resolver essa equação em $\mathbb{N}$?

Como 0 é um número par, o lado esquerdo da equação também tem que ser par. Desta forma, x deve ser ímpar. Denotando, $x = 2a_0 + 1$, para algum $a_0 \in \mathbb{N}$ e substituindo, temos

$$x + 1 = 0 \implies (2a_0 + 1) + 1 = 0 \implies a_0 + 1 = 0.$$

Iterando o raciocínio, temos que a_0 é ímpar, ou seja, $a_0 = 2a_1 + 1$, para algum $a_1 \in \mathbb{N}$. Substituindo novamente, temos $a_1 + 1 = 0$ e assim

$$x = 1 + 2a_0 = 1 + 2(2a_1 + 1) = 1 + 2 + 2^2 a_1.$$

Seguindo esse padrão, seria possível construir a solução

$$x = 1 + 2 + 2^2 + 2^3 + \ldots$$

que claramente não é um número natural, mas é construída a partir de números naturais. A ideia então seria construir um ambiente maior onde a expressão

$$-1 = 1 + 2 + 2^2 + 2^3 + \dots$$

faça sentido. Esta é exatamente a representação 2-ádica do número -1. Lembre que cada número é expresso como uma soma infinita de potências de 2. No contexto dos números 2-ádicos, a equação $x + 1 = 0$ possui solução.

6.0.2 ATIVIDADE COM DATAS DO ANO 2025

As datas pitagóricas representam um encontro fascinante entre a matemática pura e nossa experiência cotidiana com o calendário. Quando nos deparamos com uma data como 16 de setembro de 2025, podemos observar uma curiosidade matemática notável: na notação norte-americana (9/16/25), os números 9, 16 e 25 são quadrados perfeitos que satisfazem a relação pitagórica $3^2 + 4^2 = 5^2$.

Essa curiosidade numérica abre portas para investigarmos as propriedades dos ternos pitagóricos a partir de algo muito familiar, o nosso próprio calendário.

Na geometria euclidiana, o Teorema de Pitágoras estabelece que, em um triângulo retângulo, o quadrado da hipotenusa iguala a soma dos quadrados dos catetos. Quando três números inteiros positivos (a, b, c) satisfazem a equação $a^2 + b^2 = c^2$, dizemos que formam um terno pitagórico.

Um terno é considerado primitivo quando o máximo divisor comum entre a, b e c é igual a 1. Todo terno pitagórico primitivo pode ser gerado pelas fórmulas

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

onde m e n são inteiros positivos com $m > n$, mdc$(m, n) = 1$, e m e n possuem paridades opostas.

Uma data pitagórica é definida como uma data no formato $mm/dd/aa$ (onde aa representa os dois últimos dígitos do ano) em que os valores numéricos do mês, dia e ano formam um terno pitagórico. Quando esses três números são todos quadrados perfeitos, temos uma data pitagórica perfeita.

A investigação dessas datas envolve não apenas propriedades algébricas dos ternos pitagóricos, mas também as restrições impostas pelo calendário gregoriano: os meses variam de 1 a 12, os dias de 1 a 31 (com variações dependendo do mês), e os anos com dois dígitos de 0 a 99.

Esta sequência didática foi desenvolvida para ser aplicada em etapas, promovendo uma construção gradual do conhecimento. Sugere-se que na primeira aula seja feita a introdução ao conceito, utilizando a data 16/09/2025, com a realização da atividade 1 trabalhada em grupos. A segunda aula deve ser dedicada à exploração das relações numéricas e generalizações presentes na atividade 2, promovendo uma discussão coletiva para consolidar os entendimentos. Na terceira

aula, o trabalho avança para a geração de ternos e a investigação de datas futuras, conforme a atividade 3, sendo também o momento de introduzir a investigação avançada da atividade 4, voltada especialmente para os estudantes que já demonstram maior familiaridade com o conteúdo. Uma quinta aula, opcional, pode ser reservada para a socialização das soluções encontradas e uma discussão aprofundada das Considerações Finais, com o objetivo de enfatizar o processo investigativo vivenciado por toda a turma.

É esperado que os estudantes encontrem dificuldades específicas durante o percurso, principalmente na demonstração de propriedades, como na atividade 1 item 1, e no processo de generalização, exigido na atividade 2 item 3. Nesses momentos cruciais, recomenda-se que o professor conduza questionamentos estratégicos que guiem os alunos na percepção dos padrões por si mesmos, evitando fornecer as respostas diretamente. A resolução comentada, serve como um valioso apoio para o professor na condução dessas discussões, garantindo que a aprendizagem seja fruto de uma descoberta orientada.

6.0.2.1 ATIVIDADE 1

A data 16/09/25 (no formato 9/16/25) ilustra o conceito de data pitagórica perfeita, com $9 = 3^2$, $16 = 4^2$ e $25 = 5^2$ formando o terno pitagórico (3,4,5).

1. Demonstre que em qualquer terno pitagórico primitivo (a, b, c) com $a < b < c$, pelo menos um dos três números é múltiplo de 5. Com base nessa propriedade, explique por que é tão raro encontrar anos (com dois dígitos) que sejam quadrados perfeitos e que participem de uma data pitagórica com mês e dia também quadrados perfeitos.

2. Mostre que, para que uma data no formato $mm/dd/aa$ (com ano de dois dígitos) seja pitagórica e tenha mm, dd, aa como quadrados perfeitos, o valor de aa deve corresponder ao quadrado da hipotenusa de um terno pitagórico primitivo ou de seu múltiplo. Determine todos os valores possíveis para aa no século atual (2000–2099).

3. Encontre todas as datas pitagóricas perfeitas que ocorrerão no século XXI.

RESPOSTA COMENTADA

Na primeira questão, demonstramos que em qualquer terno pitagórico primitivo com $a < b < c$, pelo menos um dos três números é múltiplo de 5. Esta propriedade explica por que é tão raro encontrar anos com dois dígitos que sejam quadrados perfeitos e participem de uma data pitagórica com mês e dia também quadrados perfeitos.

A análise mostra que todo número ao quadrado é congruente a 0, 1 ou 4 módulo 5. Se nenhum de a, b, c fosse múltiplo de 5, então a^2 e b^2 pertenceriam ao conjunto $\{1, 4\}$ módulo 5.

As combinações possíveis seriam $1 + 1 = 2$, $1 + 4 = 0$ e $4 + 4 = 3$. A única que resulta em um quadrado perfeito módulo 5 é $1 + 4 = 0$, o que implica que c deve ser múltiplo de 5. Portanto, sempre há um múltiplo de 5 em qualquer terno pitagórico primitivo.

Para uma data pitagórica perfeita, o ano deve ser quadrado perfeito e múltiplo de 5. Os únicos quadrados perfeitos de dois dígitos múltiplos de 5 são 25. Assim, aa = 25 ocorre apenas uma vez por século, tornando essas datas extraordinariamente raras.

Para que uma data no formato $mm/dd/aa$ seja pitagórica e tenha mm, dd, aa como quadrados perfeitos, o valor de aa deve corresponder ao quadrado da hipotenusa de um terno pitagórico primitivo ou de seu múltiplo. Como $aa \leq 99$, então $c^2 \leq 99$ o que implica $c \leq 9$. Entre os ternos pitagóricos primitivos, apenas (3,4,5) satisfaz esta condição, pois o próximo terno (5,12,13) já tem $c^2 = 169 > 99$. Portanto, o único valor possível é $c^2 = 25$, tornando aa = 25 a única opção viável para o século XXI.

Combinando todas as condições $mm \leq 12$, $dd \leq 31$, $aa \leq 99$, e a necessidade de formar um terno pitagórico com quadrados perfeitos, chegamos a uma solução única: do terno (3,4,5) obtemos mês = $3^2 = 9$ (setembro), dia = $4^2 = 16$ e ano = $5^2 = 25$ (2025). Assim, apenas 16 de setembro de 2025 satisfaz todas as condições no século XXI. Para desenvolver esta questão com os estudantes, sugere-se iniciar com uma abordagem investigativa concreta apresentando diversos exemplos de ternos pitagóricos primitivos, como (3, 4, 5), (5, 12, 13) e (7, 24, 25), solicitando que os alunos identifiquem regularidades e padrões.

APLICAÇÃO DIDÁTICA

Organizar a turma em pequenos grupos, atribuindo a cada um a tarefa de verificar a presença de múltiplos de 5 em diferentes conjuntos de ternos gerados pela fórmula clássica. Durante essa investigação introduzir gradualmente o conceito de congruência módulo 5 de maneira intuitiva, focando o comportamento dos restos da divisão por 5.

Após o registro das observações, conduzir uma discussão coletiva onde os estudantes devem compartilhar suas descobertas e elaborar explicações para as datas pitagóricas. Para finalizar, pedir aos alunos que comparem a teoria matemática (que é exata) com as regras do calendário (que são cheias de exceções). Essa discussão mostrará como a matemática lida com limites reais.

6.0.2.2 ATIVIDADE 2

Observe as igualdades: $3^2 + 4^2 + 5^2 = 50$ e $45^2 = 2025$.

1. Demonstre algebricamente que $(3^2 + 4^2 + 5^2) \times 45^2 = (3 \times 45)^2 + (4 \times 45)^2 + (5 \times 45)^2$.
2. Utilize o resultado do item anterior para calcular o valor de $135^2 + 180^2 + 225^2$ sem calcular individualmente cada quadrado.

3. Generalize a propriedade demonstrada nos itens anteriores: Se $a^2 + b^2 + c^2 = S$ e k é um número inteiro, prove que $S \cdot k^2 = (ak)^2 + (bk)^2 + (ck)^2$.

4. Determine se existe algum inteiro k tal que k^2 represente um ano entre 2000 e 2100 e que $S \cdot k^2$ seja a soma de três quadrados que formem uma progressão aritmética.

RESPOSTA COMENTADA

Na segunda questão, exploramos relações numéricas e generalizações, partindo das igualdades $3^2 + 4^2 + 5^2 = 50$ e $45^2 = 2025$. Demonstramos algebricamente que $(3^2 + 4^2 + 5^2) \times 45^2 = (3 \times 45)^2 + (4 \times 45)^2 + (5 \times 45)^2$, revelando uma propriedade fundamental da homogeneidade em expressões polinomiais.

A demonstração mostra que quando multiplicamos uma soma de quadrados por um quadrado perfeito, o resultado pode ser reescrito como uma nova soma de quadrados. Esta propriedade reflete a escalabilidade das relações pitagóricas se multiplicamos todos os elementos de uma tripla por um mesmo fator, a relação pitagórica se mantém.

Aplicando este resultado, calculamos $135^2 + 180^2 + 225^2 = 50 \times 2025 = 101250$ sem necessidade de calcular individualmente cada quadrado, demonstrando o poder das generalizações algébricas para simplificar cálculos complexos.

A generalização desta propriedade nos permite afirmar que se $a^2 + b^2 + c^2 = S$ e k é um número inteiro, então $S \cdot k^2 = (ak)^2 + (bk)^2 + (ck)^2$.

Investigando a existência de um inteiro k tal que k^2 represente um ano entre 2000 e 2100 e que $S \cdot k^2$ seja a soma de três quadrados que formem uma progressão aritmética, descobrimos que apenas $k = 45$ (ano 2025) satisfaz a primeira condição. Porém, para a tripla $(135, 180, 225)$, verificamos que $2 \times 180^2 = 64800$ enquanto $135^2 + 225^2 = 68850$. Portanto, não formam uma progressão aritmética. Logo, não existe tal k para a tripla (3,4,5).

APLICAÇÃO DIDÁTICA

Iniciar com o exemplo numérico concreto, permitindo que os alunos constatem experimentalmente a validade das igualdades.

Em seguida, propor a exploração com outros conjuntos numéricos, sempre acompanhada de questionamentos que conduzam à percepção dos padrões. À medida que os estudantes ganhem confiança através da experimentação, introduzir progressivamente a linguagem matemática formal.

6.0.2.3 ATIVIDADE 3

Os ternos pitagóricos podem ser sistematicamente gerados usando as fórmulas: $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, com $m > n$ inteiros positivos.

1. Encontre todos os ternos pitagóricos (a, b, c) onde a^2, b^2 e c^2 são todos menores que 100, para que possam representar dias, meses ou anos com dois dígitos.

2. Dentre os ternos encontrados, identifique aqueles que permitem que dois de seus elementos sejam quadrados perfeitos que possam representar um mês válido (01–12) e um dia válido (01–31).

3. Investigue qual será a próxima data pitagórica perfeita após 2025, no formato $mm/dd/aa$, e justifique sua resposta.

RESPOSTA COMENTADA

Na terceira questão, utilizamos as fórmulas clássicas para gerar ternos pitagóricos sistematicamente. Encontramos que apenas o terno (3, 4, 5) satisfaz a condição de ter todos os quadrados menores que 100, necessário para representar dias, meses ou anos com dois dígitos. O próximo terno (6, 8, 10) já tem $c^2 = 100$, que não serve por não ser menor que 100.

Entre os meses válidos, apenas 1, 4 e 9 são quadrados perfeitos entre 1 e 12, enquanto os dias válidos são 1, 4, 9, 16 e 25. A única combinação viável do terno (3,4,5) é mês = 9 e dia = 16, resultando na data 16 de setembro.

Investigando datas futuras, descobrimos que após 2025, o próximo ano quadrado perfeito é $2116 = 46^2$. Porém, para $c = 46$, a equação $a^2 + b^2 = 2116$ com $a \leq 31$ e $b \leq 12$ é impossível, pois $31^2 + 12^2 = 1105 < 2116$. Portanto, não haverá outra data pitagórica perfeita no mesmo padrão após 2025.

APLICAÇÃO DIDÁTICA

Transformar esta questão em uma aula prática que combina rigor metodológico com criatividade. Disponibilizar uma tabela organizada com valores de parâmetros para preenchimento, estabelecendo claramente as restrições do problema.

Os estudantes formarão em duplas, utilizando ferramentas computacionais para agilizar os cálculos enquanto discutem entre si as características dos ternos gerados. O foco então se desloca para a aplicação prática no contexto do calendário, com o mapeamento de todas as combinações viáveis.

Por fim, os alunos usarão seus resultados para prever datas futuras, aplicando o poder de previsão da matemática. Em seguida, devem explicar por que algumas soluções que funcionam na teoria não são válidas na prática.

6.0.2.4 ATIVIDADE 4

Defina uma **data pitagórica perfeita completa** como aquela em que o dia, o mês e o ano (com 4 dígitos) são quadrados perfeitos e formam um terno pitagórico.

1. Verifique se existe alguma data pitagórica perfeita completa entre os anos 1000 e 3000.
2. Analise a data 9/16/2025. Demonstre que, embora 2025 seja 45^2, os números 9, 16 e 2025 não formam um terno pitagórico, e explique qual é a relação pitagórica verdadeira envolvida.
3. Desenvolva um problema original sobre a frequência com que ocorrem, em um milênio, datas em que o dia e o mês são os catetos de um terno pitagórico e o ano (com 4 dígitos) é o quadrado da hipotenusa.

RESPOSTA COMENTADA

Na quarta questão, definimos uma data pitagórica perfeita completa como aquela em que o dia, o mês e o ano com quatro dígitos são quadrados perfeitos e formam um terno pitagórico. Verificamos que não existe tal data entre os anos 1000 e 3000.

Para anos de quatro dígitos entre 1000 e 3000, precisamos de c^2 entre 1000 e 3000, o que implica c entre 32 e 54. Porém, com dia ≤ 31 e mês ≤ 12, temos $a^2 + b^2 \leq 31^2 + 12^2 = 1105$, limitando $c \leq 33$. A interseção entre $c \geq 32$ e $c \leq 33$ dá apenas $c = 32$ e $c = 33$, nenhum dos quais produz soluções inteiras dentro das restrições de dia e mês.

Analisando a data 9/16/2025, mostramos que embora 2025 seja 45^2, os números 9, 16 e 2025 não formam um terno pitagórico. A relação pitagórica verdadeira envolve apenas os últimos dois dígitos: $9 + 16 = 25$, não $9 + 16 = 2025$. Esta distinção é crucial para compreender a natureza matemática dessas datas especiais.

Propomos então investigar quantas vezes por milênio ocorre uma data onde dia e mês são catetos de um terno pitagórico e o ano de quatro dígitos é o quadrado da hipotenusa. A análise mostra que a resposta é zero, pois c^2 deve estar entre 1000 e 9999, mas $a^2 + b^2 \leq 1105$, criando um intervalo viável muito estreito ($c \leq 33$) que não contém números cujos quadrados estejam no milênio.

APLICAÇÃO DIDÁTICA

Iniciar assegurando a compreensão profunda do conceito central, utilizar exemplos e contra-exemplos para solidificar o entendimento.

Conduzir os estudantes através de uma exploração sistemática de casos limites, orientando-os na descoberta independente das restrições naturais do problema. A busca por soluções é organizada metodologicamente, enfatizando estratégias de registro e organização.

Quando alcançarmos a conclusão sobre a inexistência de soluções, promover uma reflexão profunda sobre o valor matemático das demonstrações de impossibilidade. A atividade se encerra com a criação de variações do problema original, desenvolvendo tanto a criatividade quanto o rigor matemático.

7 CONCLUSÃO

A abordagem complementar para problemas de olimpíadas de matemática envolvendo quadrados perfeitos integra o método clássico da contradição modular com a teoria dos números p-ádicos e princípios locais-globais. Através do desenvolvimento do Método Local-Global (Teorema 29), este trabalho demonstrou como é possível concluir que um número inteiro é um quadrado perfeito a partir de verificações modulares, de tal forma que a limitação do método tradicional seja superada.

A aplicação deste método à Questão 6 da IMO de 1988 (Problema 30) que combina análise modular elementar com resultados como o Teorema de Grunwald-Wang e o Lema de Hensel, mostrou-se uma alternativa viável às soluções clássicas baseadas em Vieta Jumping ou Descida Infinita.

Do ponto de vista pedagógico, as propostas apresentadas no Capítulo 6 demonstram a versatilidade dos temas abordados e como eles se adaptam a diferentes níveis de ensino. A exploração de números p-ádicos através de equações simples e a investigação de datas pitagóricas no contexto do calendário revelam como conceitos matemáticos avançados podem se tornar acessíveis e significativos para estudantes da educação básica. A construção de números 2-ádicos através da equação $x + 1 = 0$ introduz a noção de completamento não-arquimediano de forma intuitiva, enquanto a investigação das datas pitagóricas em $2025 = 45^2$ explora a interação entre teoria dos números e estruturas cotidianas, revelando que a única data pitagórica perfeita no século XXI - 16 de setembro de 2025 - emerge necessariamente do terno primitivo $(3, 4, 5)$.

As aplicações desenvolvidas contribuem para a formação tanto de professores de matemática quanto de estudantes olímpicos, oferece uma ponte entre a aritmética elementar e tópicos avançados da teoria dos números, ferramentas para abordar problemas desafiadores de equações diofantinas, estratégias pedagógicas para contextualizar conceitos abstratos em situações concretas e exemplos de como princípios profundos da matemática podem ser aplicados de forma elementar. As atividades propostas destacam o valor pedagógico das "não-soluções"e limitações matemáticas. A escassez de datas pitagóricas perfeitas ilustra como restrições aparentemente simples como os limites de dias (≤ 31) e meses (≤ 12) impõem condições que tornam tais datas excepcionalmente raras.

REFERÊNCIAS

ALFARO, L. G. S. **Another perspective on a famous problem, IMO 1988: The equation** $\frac{x^2+y^2}{xy+1} = n^2$. 2011. 143-152 p. Disponível em: <https://pt.scribd.com/document/387695378/BAMV-XVIII-2-p143-152-pdf>. 25

CAMPBELL, J. **A Solution to 1988 IMO Question 6**. 1988. 29-32 p. 25

DARIO, R. P. **Equações diofantinas e alocação otimizada de recursos financeiros de pequenos investidores no mercado acionário brasileiro**. 2022. e3007 p. Disponível em: <https://periodicos.ifrs.edu.br/index.php/REMAT/article/view/5674>. 6

GOUVÊA, F. Q. p**-adic numbers: an introduction**. Springer, 2020. 3rd edition. Disponível em: <https://link.springer.com/book/10.1007/978-3-030-47295-5>. 8

GOUVÊA, F. Q. **Primeiros passos p-ádicos**. Rio de Janeiro: IMPA, 1989. 17, 18, 19

GOUVÊA, F. Q. **p-adic numbers: an introduction**. Berlin: Springer, 1997. 282 p. (Universitext). 20, 21, 22

HEFEZ, A. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2022. 6, 7, 9, 10, 11, 14, 17

PARVARDI, A. H. **1220 Number Theory Problems (The J29 Project)**. 2019. Disponível em: <https://www.academia.edu/29934442/1220_Number_Theory_Problems_J29_Project_>. 12

QUADROS, F. B. **Primeiros Passos no Universo p-ádico**. São Bernardo do Campo: Editora da Universidade Federal do ABC, 2019. 19

SANTOS, J. P. O. **Introdução à Teoria Elementar dos Números**. Rio de Janeiro: Editora, 2003. 9

SERRE, J.-P. **A Course in Arithmetic**. New York: Springer-Verlag, 1973. (Graduate Texts in Mathematics, v. 7). 7, 10

STILLWELL, J. **Mathematics and Its History**. New York: Springer, 2002. 72-76 p. 11

VOELZ, M. E.; DARIO, R. P. **Sobre o método Vieta Jumping: cuidado para não errar o pulo e cair numa descida infinita**. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rtr/article/viewFile/12312/7442>. 24

WANG, S. **On Grunwald's theorem**. 1950. 471-484 p. Disponível em: <https://www.jstor.org/stable/1969335>. 20