UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Gercino José de Araújo Júnior

Aplicações da Lei de Reciprocidade Quadrática e Equações Diofantinas Não Lineares no Contexto Olímpico

Campina Grande - PB

Agosto/2026

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Gercino José de Araújo Júnior

Aplicações da Lei de Reciprocidade Quadrática e Equações Diofantinas Não Lineares no Contexto Olímpico

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientador: Dr. Luiz Antônio da Silva Medeiros

Campina Grande - PB
Agosto/2026

Universidade Federal de Campina Grande - UFCG
Sistema de Bibliotecas - SISTEMOTECA
Catalogação de Publicação na Fonte. UFCG - Biblioteca Central

A663a Araújo Júnior, Gercino José de.

Aplicações da lei de reciprocidade quadrática e equações diofantinas não lineares no contexto olímpico / Gercino José de Araújo Júnior. – 2026.

85 f. : il. color.

Dissertação (mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Humanidades, 2026.

"Orientação: Prof. Dr. Luiz Antônio da Silva Medeiros".

Referências.

1. Olimpíadas de Matemática. 2. Aritmética. 3. Equações Diofantinas. 4. Resolução de Problemas. 5. Heurística de Pólya. I. Medeiros, Luiz Antônio da Silva. II. Título.

UFCG/BC CDU 51(043.3)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA ITAPUANA SOARES DIAS GONÇALVES CRB-15/93

Gercino José de Araújo Júnior

Aplicações da Lei de Reciprocidade Quadrática e Equações Diofantinas Não Lineares no Contexto Olímpico

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Trabalho aprovado. Campina Grande - PB, 21 de Agosto de 2026:

gov.br Documento assinado digitalmente
LUIZ ANTONIO DA SILVA MEDEIROS
Data: 16/09/2026 21:17:52-0300
Verifique em https://validar.iti.gov.br

Dr. Luiz Antônio da Silva Medeiros
Orientador - UFCG

gov.br Documento assinado digitalmente
PAULO CESAR CAVALCANTE DE OLIVEIRA
Data: 16/09/2026 18:33:15-0300
Verifique em https://validar.iti.gov.br

Dr. Paulo César Cavalcante de Oliveira
Examinador externo(a) URCA

gov.br Documento assinado digitalmente
RENAN JACKSON SOARES ISNERI
Data: 17/09/2026 17:14:08-0300
Verifique em https://validar.iti.gov.br

Dr. Renan Jackson Soares Isneri
Examinador interno - UFCG

Campina Grande - PB
Agosto de 2026

Dedico este trabalho aos meus filhos Pedro e Bento. Que são a fonte de motivação dos meus esforços.

Agradecimentos

Agradeço imensamente à minha mãe, que é a minha grande motivadora nos estudos e é a responsável por ser professor, obrigado mãe! A meu pai, que sempre nos deu o sustento para que nada faltasse, só tenho a agradecer. Agradeço a nosso senhor e salvador Jesus Cristo, que acalmou minha mente e meu coração em momentos de dificuldade neste percurso. Agradeço a colaboração e ótimo convívio com os colegas de turma e de viagem até a UFCG, e também aos colegas de fora do mestrado que me apoiaram. Agradeço os meus professores, não somente os atuais professores do mestrado, mas também cada um que fez parte da minha trajetória. Acima de tudo, agradeço pelo ensinamento que me deram. Meu eterno agradecimento! A todos os funcionários do UAMAT. Obrigado por tudo!

"A matemática é a poesia das ideias lógicas."
Albert Einstein

Resumo

Diante da crescente expansão das olimpíadas de Matemática no país, o preparo de estudantes para conteúdos que transcendem o currículo tradicional constitui um desafio relevante. Nesse contexto, o presente trabalho apresenta uma abordagem detalhada da Lei da Reciprocidade Quadrática (LRQ) e das Equações Diofantinas Não Lineares, utilizando a perspectiva de resolução de problemas de (Pólya, 1945) para evidenciar a importância de ampliar o arsenal estratégico dos estudantes diante de questões complexas. A partir da seleção e da resolução de problemas de nível olímpico, busca-se estabelecer uma ponte direta entre esses conceitos matemáticos avançados e a sua aplicação prática, demonstrando que o domínio de ferramentas robustas enriquece a compreensão e possibilita a simplificação de problemas mais rebuscados. Como produto educacional decorrente desta pesquisa, foi elaborado um livreto instrucional autossuficiente que compila uma miscelânea de questões olímpicas e exemplos ilustrativos referentes aos temas abordados. Esse material tem como objetivo fornecer um suporte teórico e prático aprofundado, servindo como ferramenta de apoio tanto para a prática docente quanto para a preparação de estudantes.

Palavras-chave: Olimpíadas de Matemática; Aritmética; Equações Diofantinas; Resolução de Problemas; Heurística de Pólya.

Abstract

Given the growing expansion of mathematics olympiads in the country, preparing students for contents that transcend the traditional curriculum constitutes a relevant challenge. In this context, the present work presents a detailed approach to the Law of Quadratic Reciprocity (LQR) and Non-Linear Diophantine Equations, using (Pólya, 1945) problem-solving perspective to highlight the importance of expanding students' strategic arsenal when facing complex questions. Based on the selection and resolution of olympiad-level problems, this study seeks to establish a direct bridge between these advanced mathematical concepts and their practical application, demonstrating that mastering robust tools enriches comprehension and enables the simplification of intricate problems. As an educational product resulting from this research, a self-sufficient instructional booklet was developed, compiling a miscellany of olympiad questions and illustrative examples related to the covered topics. This material aims to provide in-depth theoretical and practical support, serving as a tool for both teaching practice and student preparation.

Keywords: Mathematics Olympiads; Arithmetic; Diophantine Equations; Problem Solving; Pólya's Heuristics.

Sumário

Sumário 8

Lista de ilustrações 10

Lista de tabelas 11

1 INTRODUÇÃO 12
1.1 Equações diofantinas 14
1.1.1 Quem foi Diofanto 14
1.1.2 Equações Diofantinas na resolução de problemas 15
1.2 A Aritmética em Olimpíadas Globais 15

2 OBJETIVOS 17
2.1 Objetivo geral 17
2.2 Objetivos específicos 17

3 FUNDAMENTAÇÃO TEÓRICA 18
3.1 A Metodologia de Resolução de Problemas 18
3.2 Lei da reciprocidade quadrática 20
3.3 Divisibilidade 21
3.4 Algoritmo da Divisão 22
3.5 Congruências Modulares 30
3.6 Resíduos Quadráticos 38
3.6.1 Suplementos à Lei de Reciprocidade Quadrática 47
3.7 A Lei de Reciprocidade Quadrática 50

4 EQUAÇÕES DIOFANTINAS 60
4.1 Equações diofantinas lineares 60
4.2 Equações diofantinas não lineares 61
4.3 Equações Diofantinas Quadráticas 63
4.4 O Método da Descida Infinita 64

5 APLICAÇÃO: QUESTÕES OLÍMPICAS 66
5.1 Apoio a docentes 66
5.2 Desafios e Potencialidades da Teoria dos Números Avançada no Treinamento Olímpico 66

5.3 Exemplos Clássicos 67
5.3.1 Aplicações da Lei da Reciprocidade Quadrática 67
5.3.2 Equações Diofantinas Não Lineares 68
5.4 Questões Olímpicas 69
5.4.1 Questões sobre resíduos quadráticos e Lei da reciprocidade quadrática . 70
5.4.2 Questões que envolvem equações diofantinas não lineares 73

6 CONSIDERAÇÕES FINAIS 84
Referências 85

Lista de ilustrações

Figura 1 – Demonstração da LRQ 53

Lista de tabelas

Tabela 1 – Números da OBMEP - 1ª Edição (2005) 13
Tabela 2 – Números da OBMEP - 20ª Edição (2025) 13
Tabela 3 – Como resolver um problema 19

1 Introdução

A participação de estudantes em olimpíadas de Matemática tem se tornado uma constante no cenário educacional contemporâneo, atuando como um catalisador para a descoberta de talentos e para o aprofundamento do saber científico nas escolas. Esse fenômeno impulsiona, de forma análoga, uma demanda por materiais didáticos especializados e por docentes qualificados para mediar uma jornada de aprendizagem de alto desempenho. O ecossistema das competições científicas não apenas estimula o raciocínio lógico, mas também desafia as fronteiras tradicionais do currículo da educação básica.

A visibilidade e o alcance das competições científicas no cenário educacional brasileiro consolidaram-se por meio do engajamento crescente de estudantes e instituições ao longo das últimas décadas. Nesse contexto, conquanto esta dissertação analise as olimpíadas de conhecimento em sua totalidade, os indicadores da OBMEP detalhados a seguir atuam como um recorte amostral, evidenciando, na prática, o processo de democratização e capilaridade dessas iniciativas. Nesse contexto, dados divulgados pelo Ministério da Ciência, Tecnologia e Inovação (MCTI) ilustram a amplitude alcançada pela competição:

> Em 2025, a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) comemora vinte edições da maior competição científica do país com um marco histórico. A 20ªOBMEP chegará em 57.222 escolas de 5.566 municípios garantindo uma cobertura de 99,93% das cidades do país, o maior número de instituições de ensino e de municípios inscritos desde a criação da Olimpíada. Este ano, a competição reunirá 18,6 milhões de estudantes do 6ºano do Ensino Fundamental ao 3ºano do Ensino Médio de instituições públicas e privadas (BRASIL. Ministério da Ciência, Tecnologia e Inovação, 2025).

Para ilustrar a magnitude dessa expansão ao longo de mais de duas décadas, é pertinente comparar os indicadores da primeira edição, realizada em 2005, com os dados da 20ª edição, de 2025. O contraste entre os períodos evidencia o engajamento contínuo das escolas e a massiva participação estudantil que o projeto conquistou ao longo do tempo. As Tabelas 1 e 2 apresentam um panorama quantitativo dessa evolução.

A análise comparativa das tabelas evidencia um salto substancial não apenas no número absoluto de alunos inscritos, mas principalmente na capilaridade do projeto, que passou a abranger a quase totalidade dos municípios brasileiros. Esse crescimento vertiginoso demonstra o sucesso e a consolidação da OBMEP como uma política educacional perene, capaz de identificar jovens talentos e de democratizar o estímulo ao estudo da matemática e das ciências em todas as regiões do país.

Tabela 1 – Números da OBMEP - 1ª Edição (2005)

OBMEP 2005 - Inscrições 1ª Fase	
Escolas	31.031
Alunos	10.520.831
Municípios	93,5%

Fonte: Dados extraídos de (OBMEP, 2026).

Tabela 2 – Números da OBMEP - 20ª Edição (2025)

20ª OBMEP 2025 - Inscrições 1ª Fase			
	Públicas	**Privadas**	**Todos**
Escolas	51.428	5.794	57.222
Alunos	17.691.812	925.554	18.617.336
Municípios	99,93%	24,36%	99,93%

Fonte: Dados extraídos de (OBMEP, 2026).

As questões olímpicas de nível avançado destacam-se por sua estrutura multifacetada: sob enunciados frequentemente minimalistas e elegantes, ocultam-se camadas de complexidade analítica que exigem do estudante estratégias criativas e o domínio de ferramentas abstratas. Muitas dessas ferramentas, embora aplicadas a problemas olímpicos de nível médio, são restritas aos currículos de cursos de graduação e pós-graduação. Essa disparidade cria um hiato pedagógico desafiador para os professores do ensino fundamental e médio, que muitas vezes carecem de referenciais teóricos e metodológicos direcionados para a preparação dessas competições.

Diante desse panorama, este trabalho propõe a elaboração de um livreto de apoio teórico e metodológico voltado a professores da educação básica que orientam estudantes em olimpíadas de Matemática com foco em questões envolvendo congruências não lineares. O material concentra-se em dois pilares fundamentais e interligados da Teoria dos Números: a **Lei de Reciprocidade Quadrática (LRQ)** e o estudo de **Equações Diofantinas Não Lineares**. A LRQ é tratada como uma ferramenta indispensável para determinar a solubilidade de congruências de segundo grau da forma $x^2 \equiv a \pmod{p}$, permitindo uma análise profunda sobre a distribuição dos resíduos quadráticos.

No âmbito das equações diofantinas não lineares, o trabalho transcende as técnicas elementares de fatoração e análise modular, incorporando o rigoroso **Método da Descida ao Infinito** de Fermat. Baseado no princípio do bom ordenamento dos números inteiros positivos, este método de demonstração por contradição desempenha um papel crucial na comprovação da insolubilidade de equações de graus superiores — como a célebre equação $x^4 + y^4 = z^2$ — e serve de alicerce para o estudo de estruturas mais complexas, como a Equação de Pell ($x^2 - Dy^2 = 1$) e curvas elíticas elementares. Dessa

forma, esta dissertação visa instrumentalizar o docente, oferecendo-lhe um arcabouço matemático robusto que o capacite a guiar os discentes rumo à autonomia cognitiva em ambientes competitivos de alta performance.

Para que o denso arcabouço matemático apresentado não se reduza a demonstrações herméticas ou resoluções mecânicas, a estrutura didática do livreto fundamenta-se nos pressupostos teóricos da Resolução de Problemas, cujas bases modernas foram consolidadas por George Pólya em sua obra seminal *How to Solve It* (Pólya, 1945). Publicada originalmente em 1945, a obra estabelece quatro fases heurísticas fundamentais para a abordagem de qualquer desafio matemático: (1) a compreensão do problema, (2) a concepção de um plano, (3) a execução do plano e, por fim, (4) o retrospecto. Ao adotar essa arquitetura, a elaboração das questões olímpicas no material proposto transcende a mera exposição de gabaritos secos, assumindo o papel de um roteiro investigativo que orienta o professor sobre como mediar o raciocínio do aluno diante de impasses analíticos.

1.1 Equações diofantinas

1.1.1 Quem foi Diofanto

Diofanto de Alexandria viveu por volta do ano 250 d.C. e é uma das figuras mais enigmáticas da história da matemática. Pouco se sabe sobre sua vida pessoal, origens ou nacionalidade exata, embora historiadores sugerem que ele era um egípcio que recebeu uma forte educação grega (Zawaira A.; Hitchcock, 2009). O seu grande legado histórico reside no fato de ter sido o autor de três obras fundamentais: *Sobre Números Poligonais*, *Porismas* (hoje perdida) e a sua obra-prima *Arithmetica*. Esta última é frequentemente considerada o primeiro grande tratado sobre álgebra, onde Diofanto inovou ao introduzir o uso sistemático de notação matemática para representar incógnitas, igualdades e subtrações (Koshy, 2007).

Ironicamente, quase tudo o que se sabe sobre a biografia de Diofanto provém de um famoso enigma matemático (um epigrama) preservado na *Antologia Grega*, uma coleção de poemas e textos da antiguidade. O enigma descreve as fases da sua vida em forma de frações:

> "A infância de Diofanto durou um sexto de sua vida; sua juventude, um doze avos; e ele passou mais um sétimo de sua vida como solteiro. Cinco anos após o seu casamento, nasceu-lhe um filho. O filho viveu exatamente a metade da idade que seu pai viria a ter. Diofanto faleceu quatro anos após a morte de seu filho." (Koshy, 2007)

A partir deste curioso epigrama, é possível formular uma equação diofantina linear ($\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$), cuja resolução revela que Diofanto se casou aos 33 anos, teve seu filho aos 38, perdeu-o aos 80 e, finalmente, viveu até os 84 anos de idade (Koshy, 2007).

1.1.2 Equações Diofantinas na resolução de problemas

No contexto das competições científicas de matemática, a Teoria dos Números figura como um dos pilares fundamentais, exigindo dos estudantes um alto nível de abstração e criatividade. Nesse cenário, a introdução das equações diofantinas não lineares no treinamento olímpico assume um papel de grande relevância. Diferentemente das equações lineares que possuem algoritmos de resolução padronizados, como o Algoritmo de Euclides, os modelos não lineares exigem a articulação de diversas técnicas algébricas, como a fatoração, a análise de congruências (aritmética modular) e a limitação de variáveis.

O domínio dessas equações atua como uma poderosa ferramenta de resolução e simplificação de questões. Ao aplicar esses conceitos, o estudante desenvolve um raciocínio lógico-dedutivo capaz de reduzir enunciados aparentemente intratáveis a relações algébricas elementares. Sobre a importância dessa abordagem no ambiente competitivo, (Andreescu; Andrica, 2009) destacam que a resolução de equações diofantinas transcende a mera aplicação de fórmulas; ela se configura como um verdadeiro teste de maturidade matemática, no qual a capacidade de simplificar e reestruturar um problema é tão importante quanto encontrar a sua solução final. Assim, o ensino desse tópico não apenas fornece um repertório técnico robusto, mas também estimula o pensamento heurístico essencial para o sucesso nas olimpíadas.

1.2 A Aritmética em Olimpíadas Globais

A aritmética elementar, longe de se restringir a um mero conjunto de regras mecânicas de. A transição do pensamento puramente concreto para a manipulação abstrata de símbolos numéricos. De acordo com Dehaene (Dehaene, 2011), embora o cérebro humano possua um "senso numérico" biológico e intuitivo, é através do aprendizado formal da aritmética estruturada que o indivíduo consegue transcender as limitações evolutivas e construir andaimes cognitivos complexos. Essa alfabetização numérica simbólica reorganiza o córtex parietal, permitindo que a mente processe relações abstratas de causa, proporção e simetria com maior velocidade e profundidade.

Em competições de alto nível como a *International Mathematical Olympiad* (IMO), os conceitos aritméticos fundamentais, frequentemente expandidos e formalizados sob

o domínio da Teoria dos Números, constituem um dos pilares mais desafiadores das provas.

Conforme apontam (Andreescu; Andrica, 2009), os problemas de aritmética em cenários competitivos raramente dependem de algoritmos exaustivos ou cálculos puramente mecânicos; pelo contrário, eles exigem uma aplicação engenhosa e profunda de propriedades fundamentais, tais como a divisibilidade, a aritmética modular, o Princípio das Gavetas de Dirichlet e a decomposição em fatores primos. Dessa forma, a presença massiva e transversal da aritmética nas olimpíadas de todo o mundo reforça o seu papel não apenas como base histórica da matemática, mas como o terreno mais fértil e refinado para avaliar a criatividade e a pura intuição lógica dos estudantes.

2 Objetivos

2.1 Objetivo geral

Descrever de forma didática os conceitos matemáticos envolvendo a Lei da Reciprocidade Quadrática (LRQ) e as equações diofantinas não lineares, utilizando as etapas de resolução de problemas de Pólya (1945) para fundamentar a importância de ampliar o repertório estratégico dos estudantes diante de questões olímpicas mais rebuscadas. O trabalho tem foco nos professores de Matemática que atuam na preparação para olimpíadas, e o resultado final, além desta dissertação, será a produção de um livreto instrucional autossuficiente sobre tais conteúdos.

2.2 Objetivos específicos

- Apresentar e estruturar os conceitos matemáticos da Lei da Reciprocidade Quadrática (LRQ) e das Equações Diofantinas Não Lineares, focando em suas aplicações no contexto de competições matemáticas;
- Utilizar a perspectiva de resolução de problemas de George Pólya (1945) para demonstrar a relevância de incorporar ferramentas matemáticas avançadas, enriquecendo a capacidade de compreensão e planejamento por parte dos estudantes;
- Demonstrar que o domínio da LRQ e de Equações Diofantinas atua como um facilitador, permitindo abordagens mais maduras ou simplificadas na resolução de problemas complexos de olimpíadas;
- Produzir um livreto educativo autossuficiente, como forma de produto educacional, direcionado a professores de Matemática da educação básica;
- Promover a divulgação do conhecimento matemático, instrumentalizando os professores a utilizarem ferramentas matemáticas robustas para expandir as estratégias de resolução de seus alunos.

3 Fundamentação Teórica

Neste capítulo apresentaremos os fundamentos aritméticos e algébricos essenciais que sustentam o estudo avançado da Teoria dos Números, estabelecendo o arcabouço matemático indispensável para a compreensão da Lei da Reciprocidade Quadrática e para a abordagem de equações diofantinas não lineares. Inicialmente, revisitaremos as propriedades relacionadas aos números inteiros ($\mathbb{Z}$), enfatizando a teoria da divisibilidade, os critérios de primalidade e o Teorema Fundamental da Aritmética. Em seguida, formalizaremos os conceitos de aritmética modular e o estudo dos corpos finitos $\mathbb{Z}/p\mathbb{Z}$, que fornecem o ambiente algébrico natural para o desenvolvimento de congruências de ordens superiores. Por fim, introduziremos a teoria dos resíduos quadráticos e o símbolo de Legendre $\left(\frac{a}{p}\right)$, ferramentas que desempenham um papel central tanto na determinação da solubilidade de equações polinomiais de segundo grau quanto na caracterização de soluções inteiras para curvas e sistemas não lineares, mapeando assim o percurso teórico que guiará as seções subsequentes.

3.1 A Metodologia de Resolução de Problemas

A estruturação do raciocínio matemático voltado para a resolução de problemas ganhou contornos definitivos com a publicação da obra seminal *How to Solve It*, de George Pólya (Pólya, 1945). Neste trabalho, o autor propõe que o ato de resolver um problema matemático não é um evento de inspiração fortuita, mas um processo heurístico que pode ser sistematizado em quatro etapas fundamentais. A primeira etapa, a *compreensão do problema*, consiste na identificação clara da incógnita, dos dados fornecidos e das condições impostas. A segunda fase é a *concepção de um plano*, o momento criativo em que o solucionador busca conexões entre os dados e a incógnita, frequentemente recorrendo a problemas auxiliares ou conhecimentos prévios. A terceira etapa trata da *execução do plano*, na qual os passos idealizados são postos em prática com rigor, verificando-se a exatidão de cada dedução. Por fim, a quarta etapa, o *retrospecto*, envolve a revisão crítica da solução obtida, a verificação dos argumentos e a investigação sobre a possibilidade de generalização do resultado para outros contextos.

No âmbito desta dissertação, a interface entre a segunda e a terceira etapas do modelo de Pólya assume um protagonismo central. Em problemas olímpicos envolvendo a Lei da Reciprocidade Quadrática ou o Método da Descida ao Infinito em equações diofantinas, a *concepção do plano* raramente se apoia em algoritmos diretos. Ela exige do estudante a habilidade de articular intuições e testar hipóteses como analisar parida-

Tabela 3 – Como resolver um problema

Primeiro Passo	**Compreender o Problema**
É preciso compreender o problema	Qual a incógnita? Quais são os dados? Qual é a condição? É possível satisfazer a condição? A condição é suficiente para determinar a incógnita? Ou é insuficiente? Ou redundante? Ou contraditória? Trace uma figura. Adote uma notação adequada. Separe as diversas partes da condição. É possível escrevê-las?
Segundo Passo	**Estabelecer um Plano**
Encontre a conexão entre os dados e a incógnita. É possível que seja obrigado a considerar problemas auxiliares se não puder encontrar. É preciso chegar afinal a um plano para resolução.	Já viu o problema antes? Ou já viu o mesmo problema apresentado sob forma ligeiramente diferente? Conhece um problema relacionado com este? Conhece um problema que lhe pode ser útil? Considere a incógnita! E procure pensar num problema conhecido que tenha a mesma incógnita ou outra semelhante. Eis um problema correlato e já antes resolvido. É possível utilizá-lo? É possível utilizar seu resultado? É possível utilizar o seu método. Deve-se introduzir algum elemento auxiliar para tornar possível a sua solução? É possível reformular o problema? É possível reformulá-lo ainda de outra maneira? Volte as definições. Se não puder resolver o problema proposto, procure antes resolver algum problema correlato. É possível imaginar um problema correlato mais acessível? Um problema mais genérico? Um problema mais específico? Um problema análogo? É possível resolver uma parte do problema? É possível obter dos dados alguma coisa útil? Utilizou todos os dados? Utilizou toda a condicionante?
Terceiro Passo	**Executar o Plano**
Execute seu plano	Ao executar o seu plano de resolução, *verifique cada passo*. É possível verificar claramente que o passo está correto? É possível demonstrar que ele está correto?
Quarto Passo	**Refletir Sobre o Trabalho**
Examine a solução obtida	É possível verificar o resultado? É possível verificar o argumento? É possível chegar ao resultado por um caminho diferente? É possível utilizar o resultado, ou o método, em algum outro problema?

FONTE: adaptado de (Pólya, 1995), p. XII-XIII, 1995.

des, investigar congruências em módulos específicos ou buscar contradições. O livreto proposto atua exatamente como um mediador nesta fase, revelando ao leitor as heurísticas ocultas por trás do planejamento de uma solução avançada. Simultaneamente, o material dá suporte à *execução do plano*, uma etapa que, na Teoria dos Números de alto nível, não tolera imprecisões. A transição entre o planejamento abstrato e a execução rigorosa é detalhada nas resoluções do livreto, demonstrando como a manipulação algébrica deve ser conduzida para garantir a validade formal da prova, sem perder de vista a estratégia global traçada no plano inicial.

Para consolidar essa abordagem na formulação do livreto como um material de apoio para professores e alunos, este trabalho ampara-se também nas expansões teóricas propostas por Schoenfeld (Schoenfeld, 1985). Schoenfeld argumenta que o sucesso na resolução de problemas complexos depende não apenas do conhecimento matemático de base, mas crucialmente do uso de estratégias heurísticas e do controle metacognitivo isto é, a capacidade do indivíduo de monitorar, avaliar e reorientar o próprio pensamento durante a resolução. O livreto desenvolvido materializa essa premissa ao não se limitar a apresentar o passo a passo definitivo de uma questão olímpica. O produto educacional transcende a exposição de resultados, transformando-se em um manual de treinamento do raciocínio e do controle cognitivo exigidos no ambiente de alta performance das olimpíadas de matemática.

3.2 Lei da reciprocidade quadrática

A **Lei da Reciprocidade Quadrática** é um dos pilares da Teoria dos Números. Demonstrada rigorosamente por (Gauss, 1801), ela estabelece uma conexão profunda entre a solubilidade de congruências quadráticas módulo números primos distintos.

Em competições de alto nível (IMO, OBM, Putnam), a Reciprocidade Quadrática é frequentemente o "divisor de águas" entre uma solução parcial e uma prova completa. Suas principais funções no contexto olímpico incluem:

- **Análise de Divisores Primos:** Permite caracterizar a forma dos divisores primos de expressões como $n^2 + k$. Por exemplo, provar que qualquer divisor primo de $n^2 + 1$ deve ser 2 ou da forma $4k + 1$.
- **Provas de Inexistência:** Ao encontrar um primo p tal que um lado de uma equação é um resíduo quadrático e o outro não, o competidor pode demonstrar de forma elegante que a equação original não possui soluções inteiras.
- **Simplificação Algorítmica:** Reduz o cálculo de símbolos de Legendre complexos a operações aritméticas simples, evitando a necessidade de testar todos os valores possíveis para x em $x^2 \equiv a \pmod{p}$.

Em seguida, seguiremos com a base teórica que fundamenta a Lei da reciprocidade quadrática. Para tanto, usamos como fonte de pesquisa teórica o livro de Teoria dos Números, de (Santos, 2015). No III Colóquio de Matemática da Região Norte, (Costa Júnior, 2014) apresenta a demonstração da Lei da reciprocidade quadrática, em uma sequência teórica que utilizamos de base para seguir com a nossa demonstração.

3.3 Divisibilidade

O conceito de divisibilidade ganha papel fundamental para as próximas seções. E sua importância é essencial para resolver vários problemas de contagem e definir a relação de congruência modular no conjunto dos números inteiros. Apesar de estar bem consolidado, adotamos a definição de (Santos, 2015) abaixo por incluir o caso em que o zero é divisor dele mesmo.

Definição 3.3.1. *Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$. Diz-se que a divide b se existir $c \in \mathbb{Z}$ tal que $b = ac$. Neste caso, usaremos a notação $a|b$ para indicar que a divide b. Quando não existe $c \in \mathbb{Z}$ tal que $b = ac$, diz-se que a não divide b e escreve-se $a \nmid b$.*

Notoriamente, dizer a divide b é o mesmo que falar b é divisível por a ou b é um múltiplo de a.

Exemplo 3.3.1. *Notemos que $7|42$, $4|36$ e $8|24$, pois $42 = 7 \cdot 6$, $36 = 4 \cdot 9$ e $24 = 3 \cdot 8$, respectivamente. Temos ainda que $5 \nmid 12$, $6 \nmid 20$ e $9 \nmid 25$, pois não existem inteiros a, b, c tais que $12 = 5a$, $20 = 6b$ ou $25 = 9c$.*

O próximo teorema estabelece as propriedades do conceito de divisibilidade e sua demonstração é bastante simples. Neste sentido, convidamos ao leitor tentar demonstrá-las para se familiarizar e consolidar a base da teoria.

Teorema 3.3.1 (Principais propriedades)**.** *Da definição, decorre que, para quaisquer $a, b, c, d \in \mathbb{Z}$, em que a divisão esteja definida, tem-se:*

1. *$a|a$, $1|a$ e $a|0$;*
2. *se $a|b$ e $b|c$, então $a|c$;*
3. *se $a|b$ e $c|d$ então $ac|bd$;*
4. *se $ab|ac$ e $a \neq 0$, então $b|c$;*
5. *se $a|b$ e $b \neq 0$, então $|a| \leq |b|$;*
6. *$a|1 \Leftrightarrow a = \pm 1$;*

7. $a|b$ *e* $b|a \Rightarrow |a| = |b|$;

8. *se* $c|a$ *e* $c|b$, *então* $c|(ma + nb)$, *para quaisquer* $m, n \in \mathbb{Z}$;

9. *se* $a \mid (b \pm c)$, *então* $a \mid b \iff a \mid c$.

3.4 Algoritmo da Divisão

Nesta seção, apresentamos os principais resultados da teoria de divisibilidade, que servem como arcabouço para a Lei de Recíprocidade Quadrática e os estudos de algumas equações diofantinas não lineares a ser desevolvidos nos próximos capítulos. Entre estes, destacamos o Algoritmo da Divisão de Euclides e o Teorema Fundamental da Aritmética.

Teorema 3.4.1 (Algoritmo da Divisão)**.** *Dados* $a \in \mathbb{Z}$ *e* $b \in \mathbb{N}$, *existem únicos* $q, r \in \mathbb{Z}$ *tais que* $a = qb + r$, *com* $0 \leq r < b$.

Demonstração: A demonstração deste teorema crucial da Teoria dos Números será dividida de forma didática em duas partes independentes: primeiro provaremos a *existência* dos inteiros q e r, e em seguida a sua *unicidade*, seguindo a abordagem clássica de Hefez (Hefez, Abramo, 2002).

1. Existência: Queremos encontrar um múltiplo de b que esteja o mais próximo possível de a por baixo, de modo que o resto r seja não-negativo e estritamente menor que b. Para isso, consideremos o conjunto S de todos os restos não-negativos possíveis do tipo $a - xb$:

$$S = \{a - xb \mid x \in \mathbb{Z} \text{ e } a - xb \geq 0\}.$$

Para aplicarmos as propriedades dos números inteiros, precisamos garantir que S não é vazio. Vamos analisar dois casos para o número a:

- Se $a \geq 0$, podemos escolher $x = 0$, o que nos dá $a - 0 \cdot b = a \geq 0$. Logo, $a \in S$.
- Se $a < 0$, como $b \in \mathbb{N}$ (logo $b \geq 1$), multiplicando ambos os lados por $-a$ (que é positivo), temos $-ab \geq -a$, o que implica $a - ab \geq 0$. Escolhendo $x = a$, temos que $a - ab \in S$.

Em ambos os casos, $S \neq \emptyset$. Como S é um subconjunto não vazio de inteiros não-negativos ($\mathbb{Z}_{\geq 0}$), pelo **Princípio da Boa Ordenação**, S possui um menor elemento. Vamos denotar esse elemento mínimo por r.

Como $r \in S$, existem duas conclusões imediatas por definição:

1. Existe algum inteiro q tal que $r = a - qb$ que implica $a = qb + r$.

2. Como $r \in S$, temos garantido que $r \geq 0$.

Resta-nos mostrar que $r < b$. Suponhamos, por absurdo, que $r \geq b$. Se subtrairmos b de ambos os lados da equação, teremos:

$$r - b = (a - qb) - b = a - (q + 1)b.$$

Dado que supusemos $r \geq b$, então $r - b \geq 0$. Isso significa que o número $a - (q + 1)b$ cumpre os requisitos para pertencer ao conjunto S. No entanto, como $b > 0$, é evidente que $r - b < r$.

Chegamos a uma contradição: encontramos um elemento $(r - b)$ pertencente a S que é estritamente menor do que r, que havia sido definido como o *menor* elemento de S. Portanto, a nossa suposição inicial está errada, e devemos ter $r < b$. Isso conclui a prova da existência de q e r tais que $0 \leq r < b$.

2. Unicidade: Suponhamos agora que existam dois pares de inteiros (q_1, r_1) e (q_2, r_2) que satisfaçam simultaneamente as condições do teorema:

$$a = q_1 b + r_1, \quad \text{com } 0 \leq r_1 < b$$

e

$$a = q_2 b + r_2, \quad \text{com } 0 \leq r_2 < b.$$

Igualando as duas expressões para a, obtemos:

$$q_1 b + r_1 = q_2 b + r_2 \implies (q_1 - q_2)b = r_2 - r_1.$$

Sem perda de generalidade, podemos assumir que $r_2 \geq r_1$, o que implica que $r_2 - r_1 \geq 0$. Como ambos os restos são estritamente menores que b, a diferença máxima possível entre eles deve ser estritamente menor que b. Ou seja, temos o seguinte intervalo para a diferença:

$$0 \leq r_2 - r_1 < b.$$

Da equação $(q_1 - q_2)b = r_2 - r_1$, vemos que o número $r_2 - r_1$ é um múltiplo inteiro de b. Contudo, o único múltiplo inteiro de b que reside no intervalo $[0, b)$ é o próprio zero. Portanto:

$$r_2 - r_1 = 0 \implies r_2 = r_1.$$

Substituindo $r_2 - r_1 = 0$ de volta na equação dos múltiplos, encontramos:

$$(q_1 - q_2)b = 0.$$

Como $b \in \mathbb{N}$ (logo $b \neq 0$), a única forma do produto ser zero é se:

$$q_1 - q_2 = 0 \implies q_1 = q_2.$$

Isso prova que os valores de q e r são estritamente únicos, finalizando completamente a demonstração. ■

Aqui está a continuação do material, estendendo o Algoritmo da Divisão para abranger qualquer divisor inteiro não nulo. A demonstração se apoia diretamente no teorema anterior, mantendo o rigor e a didática clássica de Abramo Hefez (Hefez, Abramo, 2002).

Corolário 3.4.2 (Caso geral)**.** *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que $a = qb + r$, com $0 \leq r < |b|$.*

Demonstração: Como este é um corolário, utilizaremos o resultado já provado no Teorema do Algoritmo da Divisão (onde o divisor era estritamente positivo) para expandir o conceito para qualquer inteiro $b \neq 0$. Dividiremos a análise da *existência* em dois casos, dependendo do sinal de b, e em seguida provaremos a *unicidade*.

1. Existência:

Caso 1: $b > 0$. Se b é positivo, então $|b| = b$. Neste caso, o corolário recai exatamente no enunciado do teorema anterior. Logo, a existência de q e r tais que $a = qb + r$ com $0 \leq r < b = |b|$ já está garantida.

Caso 2: $b < 0$. Se b é negativo, então o seu módulo é positivo, isto é, $|b| = -b > 0$. Como $|b| \in \mathbb{N}$, podemos aplicar o teorema anterior aos inteiros a e $|b|$. Pelo Teorema do Algoritmo da Divisão, existem inteiros q' e r' tais que:

$$a = q'|b| + r', \quad \text{com } 0 \leq r' < |b|.$$

Como $b < 0$, sabemos que $|b| = -b$. Substituindo isso na equação acima, obtemos:

$$a = q'(-b) + r' \implies a = (-q')b + r'.$$

Agora, basta definirmos $q = -q'$ e $r = r'$. Como q' e r' são inteiros, q e r também o são. Assim, reescrevemos a equação como:

$$a = qb + r, \quad \text{com } 0 \leq r < |b|.$$

O que conclui a prova da existência para qualquer $b \neq 0$.

2. Unicidade: O argumento de unicidade segue uma lógica muito semelhante à do teorema principal. Suponha que existam dois pares de inteiros (q_1, r_1) e (q_2, r_2) que satisfaçam as condições do corolário:

$$a = q_1 b + r_1, \quad \text{com } 0 \leq r_1 < |b|$$

e

$$a = q_2 b + r_2, \quad \text{com } 0 \leq r_2 < |b|.$$

Igualando as expressões para a, temos:

$$q_1 b + r_1 = q_2 b + r_2 \implies (q_1 - q_2)b = r_2 - r_1.$$

Aplicando o valor absoluto (módulo) em ambos os lados da igualdade, obtemos:

$$|q_1 - q_2||b| = |r_2 - r_1|.$$

Como r_1 e r_2 estão ambos no intervalo $[0, |b|)$, a distância máxima entre eles deve ser estritamente menor que o comprimento do intervalo, que é $|b|$. Logo:

$$0 \leq |r_2 - r_1| < |b|.$$

Substituindo na equação dos módulos:

$$|q_1 - q_2||b| < |b|.$$

Como $b \neq 0$, temos que $|b| > 0$, então podemos dividir ambos os lados da desigualdade por $|b|$:

$$|q_1 - q_2| < 1.$$

Sendo q_1 e q_2 números inteiros, a diferença entre eles também é inteira. O único número inteiro não-negativo (pois é um módulo) estritamente menor que 1 é o zero. Portanto:

$$|q_1 - q_2| = 0 \implies q_1 - q_2 = 0 \implies q_1 = q_2.$$

Se $q_1 = q_2$, voltando à equação inicial $(q_1 - q_2)b = r_2 - r_1$, obtemos:

$$0 \cdot b = r_2 - r_1 \implies 0 = r_2 - r_1 \implies r_1 = r_2.$$

Logo, q e r são únicos. ■

Exemplo 3.4.1. *Numa divisão por -6, os possíveis restos são os números pertencentes ao conjunto $X = \{r \in \mathbb{Z} : 0 \leq r < |-6|\}$, ou seja, $X = \{0, 1, 2, 3, 4, 5\}$.*

Observação 3.4.1. *Dizemos que um número inteiro é par quando é divisível por 2 (deixa resto 0 na divisão por 2). Portanto, um número inteiro n é par se, e somente se, n é da forma $2 \cdot k$, para algum k inteiro . Caso contrário, diremos que um número é ímpar se deixa resto 1 na divisão por 2, isto é, um número inteiro n é ímpar se, e somente se, n é da forma $2 \cdot k + 1$, para algum k inteiro. Além disso, dizemos que dois inteiros têm a mesma paridade se são ambos pares ou ambos ímpares. Não é difícil verificar que:*

- *a soma de um número ímpar com um número par é um número ímpar;*
- *a soma de dois números ímpares é um número par;*

- *a soma de dois números pares é um número par.*

Definição 3.4.1 (Máximo Divisor Comum)**.** *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. O máximo divisor comum (MDC) de a e b, denotado por $mdc(a, b)$, é um inteiro positivo d que satisfaz:*

1. *$d|a$ e $d|b$;*
2. *se $\exists c \in \mathbb{Z}$ tal que $c|a$ e $c|b$, então $c|d$.*

O item 1 nos diz que mdc(a, b) é um divisor comum de a e b. Já o item 2 diz que d é o maior divisor comum de a e b.

Definição 3.4.2. *Quando $mdc(a, b) = 1$, diz-se que a e b são relativamente primos ou primos entre si.*

Exemplo 3.4.2. *Podemos verificar facilmente que, $mdc(3, 6) = 3$, $mdc(-5, -30) = 5$, $mdc(6, 0) = 6$, $mdc(13, 20) = 1$ e $mdc(4, -2) = 2$.*

A seguir, apresentamos um caracterização clássica do máximo divisor comum entre dois inteiros. Omitiremos a sua demonstração, buscando atingir com maior brevidade os objetivos desse trabalho.

Teorema 3.4.3 (Teorema de Bachet-Bézout)**.** *Sejam a e b inteiros não nulos. Então, $mdc(a, b) = 1$, se e somente se, existem inteiros x, y tais que*

$$a \cdot x + b \cdot y = 1.$$

Demonstração: A demonstração pode ser encontrada em (Hefez, Abramo, 2016, p. 82).

Teorema 3.4.4 (Lema de Gauss)**.** *Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração: Do Teorema 3.4.3 de Bézout, existem inteiros x, y tais $ax + by = 1$. Multiplicando a igualdade anterior por c, e usando o quociente d da divisão de bc por a, obtemos:

$$acx + bcy = c \implies a(cx) + (ad)y = c \implies a \cdot (cx + dy) = c \implies a \mid c.\blacksquare$$

Definição 3.4.3 (Números Primos)**.** *Um número $p \in \mathbb{Z} \setminus \{1, -1, 0\}$ diz-se primo se $a|p$ implicar $a = \pm 1$ ou $a = \pm p$. Um número composto é aquele que não é primo.*

Note que os números $-1, 0, 1$ não são primos e nem são compostos. Da definição, decorre que se d é um número composto, então existem inteiros r e s, com $1 < r \leq s < d$, tais que $d = rs$.

Como p é primo se, e somente se, $-p$ é primo, na maioria dos resultados que faremos, consideraremos $p > 1$. Além disso, definiremos agora os seguintes conjuntos, que serão para simplificar os enunciados:

$$P = \{p \in \mathbb{N} : p \text{ é primo}\}, \quad P^* = \{p \in \mathbb{N} : p \text{ é primo ímpar}\}$$

e

$$I_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}.$$

Teorema 3.4.5 (Lema de Euclides)**.** *Se $p \mid ab$ e p é primo, então $p \mid a$ ou $p \mid b$.*

Demonstração: Para demonstrarmos este resultado clássico, assumiremos por hipótese que p divide o produto ab. Isso significa que existe um inteiro k tal que:

$$ab = pk.$$

A nossa tese é provar que $p \mid a$ ou $p \mid b$. Ora, se $p \mid a$, a tese se verifica. Sendo assim, vamos assumir que p **não divide** a (ou seja, $p \nmid a$) e provaremos que, obrigatoriamente, p deve dividir b.
Como p é um número primo, os seus únicos divisores positivos são 1 e o próprio p. O máximo divisor comum entre a e p, denotado por $\text{mdc}(a, p)$, deve necessariamente ser um divisor de p. Logo, temos apenas duas possibilidades:

$$\text{mdc}(a, p) = 1 \quad \text{ou} \quad \text{mdc}(a, p) = p.$$

No entanto, se $\text{mdc}(a, p) = p$, isso implicaria por definição que p é um divisor de a, o que contraria a nossa suposição de que $p \nmid a$. Portanto, a única possibilidade viável é que:

$$\text{mdc}(a, p) = 1.$$

Isso significa que a e p são primos entre si. O resultado segue então do Lema de Gauss (Lema 3.4.4), onde se conclui que $p \mid b$.■

Teorema 3.4.6 (Teorema Fundamental da Aritmética - TFA)**.** *Todo $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ pode ser escrito da forma $a = up_1p_2 \cdots p_k$, com $p_1 \leq p_2 \leq \cdots \leq p_k$, onde $u = \pm 1$ e p_i é primo. Além disso, essa forma é única.*

Demonstração: A demonstração deste teorema pilar, como vemos em (Hefez, Abramo, 2016), divide-se naturalmente em duas partes: a prova de que a decomposição existe e a prova de que ela é estritamente única. Para simplificar, sem perda de generalidade,

focaremos nos inteiros positivos ($a \geq 2$), o que corresponde a fixar $u = 1$. (Para números negativos, basta usar $u = -1$ e aplicar o mesmo raciocínio sobre o módulo $|a|$).

1. Existência: Vamos provar a existência da fatoração utilizando o Princípio da Indução Forte sobre o número a.

Caso base: Para $a = 2$, o número já é primo. Sua decomposição é trivialmente ele mesmo, respeitando as condições do teorema.

Passo indutivo: Suponha por hipótese de indução que todo inteiro n, no intervalo $2 \leq n < a$, possa ser escrito como um produto de números primos. Nosso objetivo é mostrar que a também pode. Temos duas possibilidades para a:

- **Se a for primo:** A demonstração está terminada, pois a é a sua própria fatoração prima (um produto de um único fator).
- **Se a for composto:** Por definição, a possui divisores próprios. Isso significa que podemos escrevê-lo como $a = bc$, onde $1 < b < a$ e $1 < c < a$. Como b e c são estritamente menores que a, a nossa hipótese de indução se aplica a ambos. Logo, podemos escrevê-los como produtos de primos:

  $$b = p_1 p_2 \cdots p_r \quad \text{e} \quad c = q_1 q_2 \cdots q_s.$$

  Substituindo essas decomposições na equação de a, obtemos:

  $$a = bc = (p_1 p_2 \cdots p_r)(q_1 q_2 \cdots q_s).$$

  O que mostra que a é um produto de primos. Reordenando os fatores em ordem crescente, chegamos exatamente à forma exigida pelo teorema.

Isso conclui a prova da existência.

2. Unicidade: A prova da unicidade dependerá fortemente do Lema de Euclides, provado na seção anterior. Suponhamos que o inteiro a possua duas decomposições em números primos, ambas já ordenadas de forma crescente:

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m.$$

Observe que o primo p_1 obviamente divide o lado esquerdo da igualdade, logo, deve dividir o lado direito:

$$p_1 \mid (q_1 q_2 \cdots q_m).$$

Pelo **Lema de Euclides**, se um número primo divide um produto, ele tem que dividir pelo menos um dos fatores. Portanto, $p_1 \mid q_j$ para algum índice j. Porém, como

q_j também é primo, os seus únicos divisores são 1 e ele mesmo. Sendo $p_1 > 1$, a única conclusão possível é que $p_1 = q_j$.

Como as sequências estão em ordem crescente, sabemos que $q_1 \leq q_j$. Substituindo q_j por p_1, temos $q_1 \leq p_1$. Se fizermos o raciocínio simétrico (partindo de q_1 dividindo o lado esquerdo), concluiremos analogamente que $p_1 \leq q_1$. Se $q_1 \leq p_1$ e $p_1 \leq q_1$, obrigatoriamente:

$$p_1 = q_1.$$

Sendo iguais, podemos cancelar p_1 e q_1 de ambos os lados da nossa igualdade original, restando:

$$p_2 \cdots p_k = q_2 \cdots q_m.$$

Repetindo esse mesmo argumento lógico de forma sucessiva (o que rigorosamente constitui uma nova indução), concluiremos que $p_2 = q_2$, $p_3 = q_3$, e assim por diante.

Se a quantidade de fatores fosse diferente, digamos $k < m$, após cancelar todos os k fatores, o lado esquerdo ficaria igual a 1, enquanto o lado direito seria um produto de números primos:

$$1 = q_{k+1} \cdots q_m.$$

O que é um absurdo, visto que todos os primos são maiores ou iguais a 2. Conclui-se, portanto, que a quantidade de fatores tem que ser a mesma ($k = m$) e que $p_i = q_i$ para todo i. A decomposição é, de fato, estritamente única. ■

Corolário 3.4.7. *(TFA, caso geral)*
Todo $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ *pode ser escrito de modo único na forma*

$$a = up_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \quad com \quad p_1 < p_2 < \cdots < p_n,$$

onde $u = \pm 1$ *e* p_i *é primo para todo* $i \in I_n$.

Exemplo 3.4.3. *Decomponha os números 60, 124 e 500 como produtos de fatores primos.*

Solução:

i) $60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$;

ii) $124 = 2 \cdot 62 = 2 \cdot 2 \cdot 31 = 2^2 \cdot 31$;

iii) $500 = 5 \cdot 100 = 5 \cdot 4 \cdot 25 = 2^2 \cdot 5^3$;

iv) $666 = 2 \cdot 3 \cdot 111 = 2 \cdot 3 \cdot 3 \cdot 37 = 2 \cdot 3^2 \cdot 37$.

3.5 Congruências Modulares

Definição 3.5.1. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Dizemos que a é congruente a b módulo n e escrevemos $a \equiv b \pmod{n}$ se, e somente se, $a - b$ é um múltiplo de n, ou seja, se existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Se n não divide $a - b$, dizemos que a é incongruente a b e denotamos $a \not\equiv b \pmod{n}$.*

Percebamos que, ao considerar $n \in \mathbb{N}$, dizer que $a \equiv b \pmod{n}$, para $a, b \in \mathbb{Z}$, equivale a dizer que $n \mid (a - b)$.

Se $n = 1$, então a congruência $a \equiv b \pmod{1}$ é trivialmente verdadeira, pois todo número inteiro é múltiplo de 1 (basta tomar $k = a - b$ na definição). Se $n = 0$, então a congruência $a \equiv b \pmod{0}$ equivale à igualdade $a = b$, obviamente.

Se, por acaso, $n < 0$, na congruência $a \equiv b \pmod{n}$, podemos avaliar o caso equivalente $a \equiv b \pmod{-n}$. Por definição, o caso $n \leq 0$ é desconsiderado. Além disso, não consideraremos também o caso em que $n = 1$ nos enunciados e demonstrações dos teoremas que se sucederão.

Exemplo 3.5.1. *Obsere que $12 \equiv 2 \pmod{5}$, pois $12 - 2 = 10$ e $5 \mid 10$. Também é verdade que $13 \equiv -2 \pmod{5}$, pois $5 \mid [13 - (-2)]$. Porém, $42 \not\equiv 13 \pmod{2}$, pois $42 - 13 = 29$ e $2 \nmid 29$, e, como $9 \nmid 11$ e $11 = 13 - 2$, $13 \not\equiv 2 \pmod{9}$.*

Proposição 3.5.1 (Relação de Equivalência)**.** .

Sejam $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$. A congruência é uma relação reflexiva, simétrica e transitiva, isto é, as seguintes sentenças são verdadeiras:

1. *$a \equiv a \pmod{n}$;*
2. *se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;*
3. *se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$.*

Exemplo 3.5.2. *Como $8 \equiv -2 \pmod{5}$ e $-2 \equiv 3 \pmod{5}$, por transitividade, $8 \equiv 3 \pmod{5}$.*

Proposição 3.5.2 (Operações com $\equiv$)**.** *Se $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:*

1. *$a + c \equiv b + d \pmod{n}$, em particular, $a + k \equiv b + k \pmod{n}$;*
2. *$a - c \equiv b - d \pmod{n}$, em particular, $a - k \equiv b - k \pmod{n}$;*
3. *$ac \equiv bd \pmod{n}$, em particular, $ak \equiv bk \pmod{n}$.*

Exemplo 3.5.3. *Mostrar que $246^{2015} \equiv 1 \pmod{7}$.*

Solução: *Note que* $246 = 6 \cdot 41$. *Como* $6 \equiv -1 \pmod 7$, *podemos elevar esta congruência a* 2015, *donde*

$$6^{2015} \equiv (-1)^{2015} \equiv -1 \pmod 7.$$

Analogamente, $41 \equiv -1 \pmod 7$. *Então, elevando esta congruência a* 2015, *obtemos* $41^{2015} \equiv (-1)^{2015} \equiv -1 \pmod 7$. *Multiplicando as duas congruências obtidas membro a membro, ficamos com*

$$6^{2015} \cdot 41^{2015} \equiv (-1) \cdot (-1) \pmod 7.$$

Como $6^{2015} \cdot 41^{2015} = (6 \cdot 41)^{2015} = 246^{2015}$, *segue que* $246^{2015} \equiv 1 \pmod 7$.

Observação: Apesar do item 3 da Proposição 3.5.2 nos garantir que podemos multiplicar uma congruência em ambos os lados por um número inteiro, o mesmo não vale para a divisão. Isto é, a implicação.

$$ac \equiv bc \pmod n \implies a \equiv b \pmod n$$

não é válida sempre. Por exemplo, $6 \equiv 2 \pmod 4$, isto é, $2 \cdot 3 \equiv 2 \cdot 1 \pmod 4$, porém não é verdade que $3 \equiv 1 \pmod 4$. Para tratar disto, temos o seguinte resultado.

Proposição 3.5.3 (Cancelamento do termo comum)**.** *Se* $ac \equiv bc \pmod n$, *então* $a \equiv b \pmod{n/d}$, *onde* $d = mdc(c, n)$.

Exemplo 3.5.4. *Mostrar que, para* $a, b, c \in \mathbb{Z}$ *e* $n \in \mathbb{N}$, *se* $ac \equiv bc \pmod n$ *e se* c *e* n *são primos entre si, então*

$$a \equiv b \pmod n.$$

Solução: *Como* n *e* c *são primos entre si, deve ser* $mdc(c, n) = 1$ *e o resultado é imediato.*

Definição 3.5.2 (Resíduo)**.** *Sejam* $a \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Um inteiro* b *tal que* $a \equiv b \pmod n$ *é dito resíduo de* a *módulo* n.

Definição 3.5.3 (Sistema Completo de Resíduos - SCR)**.** *Dizemos que o conjunto* $S = \{r_1, r_2, r_3, \ldots, r_n\}$ *é um Sistema Completo de Resíduos (SCR) módulo* n *se são satisfeitas as condições:*

1. $r_i \not\equiv r_j \pmod n$ *sempre que* $i \neq j$, *com* $i, j \in I_n = \{1, 2, \ldots, n\}$;
2. *para todo inteiro* a, *existe* $i \in I_n$ *tal que* $a \equiv r_i \pmod n$.

Exemplo 3.5.5. *Mostrar que o conjunto* $S = \{0, 1, 2\}$ *é um Sistema Completo de Restos módulo* 3.

Solução: *É claro que quaisquer dois elementos de S são incongruentes módulo 3. Devemos, portanto, mostrar que todo e qualquer número é congruente módulo 3 a um destes elementos. De fato, pelo Algoritmo da Divisão, segue-se que, para algum $k \in \mathbb{Z}$, n é de uma das seguintes formas:*

i) $n = 3k$;

ii) $n = 3k + 1$;

iii) $n = 3k + 2$.

Em cada um dos casos, n será congruente a $0, 1$ ou 2, respectivamente, como queríamos mostrar.

Lema 3.5.4 (SCR trivial)**.** *Seja $n \in \mathbb{N}$. O conjunto $S = \{0, 1, 2, 3, \ldots, n-1\}$ é um Sistema Completo de Restos módulo n.*

Definição 3.5.4 (Congruência Linear)**.** *Sejam $a, b, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. Chamamos de congruência linear toda congruência da forma*

$$ax \equiv b \pmod{n}, \quad a \neq 0.$$

O conjunto dos x para os quais esta congruência é verdadeira é chamado de conjunto solução da congruência linear.

Teorema 3.5.5 (Existência de soluções)**.** *A congruência $ax \equiv b \pmod{n}$ possui solução se, e somente se, $d = mdc(a, n)$ divide b.*

Demonstraçao: Ora, se existe $x \in \mathbb{Z}$ tal que $ax \equiv b \pmod{n}$, então existe $y \in \mathbb{Z}$ tal que

$$ax - b = ny.$$

Se $d = mdc(a, n)$ tem-se que $d \mid a$ e $d \mid n$, consequentemente d divide toda combinação linear entre a e n. Portanto, $d \mid (ax - ny) = b$.

Reciprocamente, suponha que $d = mdc(a, b) \mid b$. Assim, existe $q \in \mathbb{Z}$ tal que $b = qd$ e pelo Teorema de Bachet-Bézout (Teorema 3.4.3), existem r e s inteiros tais que $ar + ns = d$. Multiplicando essa equação por q, otemos:

$$a \cdot (rq) + n \cdot (sq) = dq = b \Leftrightarrow n \mid [a \cdot (rq) - b].$$

De onde segue que, $x_0 = rq$ é solução da equação $ax \equiv b \pmod{n}$.■

Exemplo 3.5.6. $6x \equiv 2 \pmod{3}$ *é um exemplo de congruência linear. O conjunto solução desta congruência é vazio, pois $mdc(6, 3) = 3$ e $3 \nmid 2$, isto é, $6x \equiv 2 \pmod{3}$ não tem solução.*

Exemplo 3.5.7. *A congruência linear* $8x \equiv 4 \pmod 6$ *tem solução, pois* $mdc(8,6) = 2$ *e* $2 \mid 4$. *Uma das soluções é* 2, *visto que* $6 \mid (8 \cdot 2 - 4)$. *Além desta,* $8, 14, -4$, *ou qualquer número da forma* $2 + 6k, k \in \mathbb{Z}$ *também é solução da congruência, pois:*

$$8 \cdot 2 \equiv 4 \pmod 6 \tag{3.1}$$

$$8 \cdot 6k \equiv 0 \pmod 6. \tag{3.2}$$

Somando (1) com (2), obtemos:

$$8 \cdot 2 + 8 \cdot 6k \equiv 4 + 0 \pmod 6$$
$$8 \cdot (2 + 6k) \equiv 4 \pmod 6.$$

Note, por fim, que 5 *também é solução da congruência* $8x \equiv 4 \pmod 6$, *porém,* 5 *não é da forma* $2 + 6k$, *que só gera números pares. Portanto, o conjunto*

$$S' = \{2 + 6k : k \in \mathbb{Z}\}$$

não contém todas as soluções desta congruência.

Definição 3.5.5 (Soluções distintas)**.** *Duas soluções* x_1 *e* x_2 *da congruência linear*

$$ax \equiv b \pmod n$$

são ditas distintas módulo n *se*

$$x_1 \not\equiv x_2 \pmod n.$$

Exemplo 3.5.8. *Assim, na congruência* $8x \equiv 4 \pmod 6$, 2 *e* 5 *são duas soluções incongruentes módulo* 6, *pois* $2 \not\equiv 5 \pmod 6$, *e, portanto, são soluções distintas módulo* 6. *Porém, as soluções do conjunto* S' *são todas congruentes módulo* 6, *pois*

$$2 + 6k_1 \equiv 2 + 6k_2 \pmod 6, \quad \forall k_1, k_2 \in \mathbb{Z}.$$

Teorema 3.5.6 (Quantidade de Soluções Incongruentes)**.** *Sejam* $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ *e* $d = mdc(a, n)$. *Se* $d \mid b$, *então a congruência linear*

$$ax \equiv b \pmod n$$

possui exatamente d *soluções incongruentes módulo* n.

Demonstração. Por definição de congruência modular, a equação $ax \equiv b \pmod n$ é equivalente à existência de um inteiro $y \in \mathbb{Z}$ tal que:

$$ax - ny = b.$$

Como $d = \text{mdc}(a, n)$ e por hipótese $d \mid b$, podemos dividir toda a equação por d:

$$\frac{a}{d}x - \frac{n}{d}y = \frac{b}{d}.$$

Definindo $a' = \frac{a}{d}$, $n' = \frac{n}{d}$ e $b' = \frac{b}{d}$, reescrevemos a equação como a congruência:

$$a'x \equiv b' \pmod{n'}.$$

Dado que $\text{mdc}(a', n') = 1$, essa congruência admite uma única solução módulo n', a qual chamaremos de x_0. As soluções gerais para x são dadas por:

$$x_k = x_0 + kn' = x_0 + k\frac{n}{d}, \quad \text{para todo } k \in \mathbb{Z}.$$

Analisando a congruência dessas soluções módulo n, temos que $x_k \equiv x_j \pmod{n}$ se, e somente se:

$$x_0 + k\frac{n}{d} \equiv x_0 + j\frac{n}{d} \pmod{n} \iff k\frac{n}{d} \equiv j\frac{n}{d} \pmod{n}.$$

Dividindo os dois lados por $\frac{n}{d}$ e o módulo n por $\text{mdc}\left(\frac{n}{d}, n\right) = \frac{n}{d}$, obtemos:

$$k \equiv j \pmod{d}.$$

Isso mostra que as soluções x_k e x_j são congruentes módulo n se, e somente se, os seus índices k e j forem congruentes módulo d. Tomando $k \in \{0, 1, 2, \ldots, d-1\}$, obtemos exatamente d soluções incongruentes módulo n:

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2\frac{n}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{n}{d}.$$

□

Corolário 3.5.7 (Caso $d = 1$)**.** *Se $mdc(a, n) = 1$, a congruência linear $ax \equiv b \pmod{n}$ tem uma única solução módulo n.*

Exemplo 3.5.9. *Resolver a congruência linear $12x \equiv 6 \pmod{9}$ e encontrar as soluções distintas módulo 9.*

Solução: *Como $mdc(12, 9) = 3$ e $3 \mid 6$, a congruência tem exatamente 3 soluções distintas módulo 9. Uma destas soluções é $x_0 = 2$, pois $12 \cdot 2 - 6 = 18 = 2 \cdot 9$. Como*

$$\frac{n}{mdc(a, n)} = \frac{9}{3} = 3,$$

obtemos o conjunto de soluções gerais:

$$S = \{2 + 3k : k \in \mathbb{Z}\}.$$

Três soluções distintas módulo 9 são obtidas fazendo $k = 0, 1, 2$, resultando em $\{2, 5, 8\}$.

Exemplo 3.5.10. *Resolver a congruência linear* $3x \equiv 15 \pmod 2$.
Solução: *Primeiramente, note que resolver esta congruência é equivalente a resolver a congruência*

$$3x \equiv 1 \pmod 2,$$

pois $15 \equiv 1 \pmod 2$. *Como* 3 *e* 2 *são primos entre si (*$mdc(3,2) = 1$*), a congruência tem solução única módulo* 2. *Uma solução particular é* $x_0 = 1$, *visto que* $3(1) = 3 \equiv 1 \pmod 2$. *Assim, o conjunto solução desta congruência é:*

$$S = \{1 + 2k : k \in \mathbb{Z}\}.$$

Lema 3.5.8. *Seja* $r_i \in \mathbb{Z}$, *para cada* $i \in I_n$. *Se* $S = \{r_1, r_2, r_3, \ldots, r_n\}$ *é um SCR módulo* n, *então* $S_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, \ldots, a \cdot r_n\}$ *também é, desde que* $mdc(a, n) = 1$.

Demonstração. Como S_a tem n elementos, precisamos apenas mostrar que estes são incongruentes dois a dois. Então, para cada $i, j \in I_n$, consideremos a congruência:

$$ar_i \equiv ar_j \pmod n.$$

Como $\text{mdc}(a, n) = 1$, podemos cancelar o termo a e obter:

$$r_i \equiv r_j \pmod n.$$

Mas isso só acontece se $i = j$, pois $r_i, r_j \in S$, que é um SCR módulo n. Ou seja, os elementos de S_a são dois a dois incongruentes módulo n. Portanto, S_a é um SCR módulo n. ∎

Teorema 3.5.9 (Pequeno Teorema de Fermat)**.** *Se* p *é primo,* $a \in \mathbb{Z}$ *e* $p \nmid a$, *então* $a^{p-1} \equiv 1 \pmod p$.

Demonstração. Como $p \in P$ e $p \nmid a$, segue-se que $\text{mdc}(a, p) = 1$. Se considerarmos o SCR módulo n trivial

$$S = \{0, 1, 2, 3, \ldots, p - 1\},$$

o Lema 3.5.8 nos garante que $S_a = \{0, a, 2a, 3a, \ldots, (p-1)a\}$ também é um SCR módulo n. Daí, cada elemento de S é congruente a um único elemento de S_a (estão numa correspondência biunívoca). É óbvio que $0 \equiv 0 \pmod p$. Portanto, ainda temos uma correspondência biunívoca do conjunto $S \setminus \{0\}$ com o conjunto $S_a \setminus \{0\}$. Apesar de não sabermos quais são os pares de números congruentes gerados por esta correspondência, podemos multiplicar as congruências membro a membro. Fazendo isso, e reorganizando se necessário os termos ou fatores, obtemos:

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod p,$$

ou seja,

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}.$$

Como p não divide nenhum número da lista $1, 2, 3, \ldots, p-1$, deve ser primo com todos eles. Cancelando estes termos, ficamos com:

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

■

Exemplo 3.5.11. *Calcule o resto da divisão de* $97^{88} + 89^{96}$ *por* 8633.
Solução: *Observe que* $8633 = 97 \cdot 89$. *Pelo Pequeno Teorema de Fermat, temos:*

$$89^{96} \equiv 1 \pmod{97} \tag{3}$$

$$97^{88} \equiv 1 \pmod{89} \tag{4}$$

Ora, $97 \equiv 0 \pmod{97}$. *Logo,* $97^{88} \equiv 0 \pmod{97}$. *Somando isto a (3), obtemos:*

$$89^{96} + 97^{88} \equiv 1 + 0 \equiv 1 \pmod{97}.$$

Analogamente, como $89 \equiv 0 \pmod{89}$, *temos* $89^{96} \equiv 0 \pmod{89}$. *Somando a (4), obtemos:*

$$89^{96} + 97^{88} \equiv 0 + 1 \equiv 1 \pmod{89}.$$

Ou seja,

$$89 \mid (89^{96} + 97^{88} - 1) \quad e \quad 97 \mid (89^{96} + 97^{88} - 1).$$

Como $mdc(89, 97) = 1$, *segue-se que:*

$$89 \cdot 97 \mid (89^{96} + 97^{88} - 1),$$

isto é,

$$97^{88} + 89^{96} \equiv 1 \pmod{8633}.$$

Portanto, $97^{88} + 89^{96}$ *deixa resto* 1 *na divisão por* 8633.

Definição 3.5.6 (SRR)**.** *Dizemos que um conjunto* $R = \{r_1, r_2, r_3, \ldots, r_k\}$, *onde* $r_i \in \mathbb{Z}$, $\forall i \in I_k$, *é um Sistema Reduzido de Resíduos (SRR) módulo* n *se as seguintes condições são satisfeitas:*

1. $mdc(r_i, n) = 1, \forall i \in I_k$;
2. $r_i \not\equiv r_j \pmod{n}$, *se* $i, j \in I_k$ *e* $i \neq j$; *e*
3. *para cada* $m \in \mathbb{N}$ *com* $mdc(m, n) = 1, \exists i \in I_k$ *tal que* $m \equiv r_i \pmod{n}$.

Exemplo 3.5.12. *Como bem sabemos, o conjunto* $S = \{0, 1, 2, 3, 4, 5\}$ *é um SCR módulo* 6*. Dentre os elementos de* S*, os únicos não primos com* 6 *são os números:* 0*, pois* $mdc(0, 6) = 6$*;* 2*, pois* $mdc(2, 6) = 2$*;* 3*, pois* $mdc(3, 6) = 3$*; e* 4*, pois* $mdc(4, 6) = 2$*. "Retirando" estes elementos de* S*, ficamos com o conjunto* $R = \{1, 5\}$*, que é um sistema reduzido de resíduos módulo* 6*.*

Lema 3.5.10. *Se* $R = \{r_1, r_2, r_3, \ldots, r_{\phi(n)}\}$ *é um SRR módulo* n*, então*

$$R_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, \ldots, a \cdot r_{\phi(n)}\}$$

também é um SRR módulo n*, desde que se tenha* $mdc(a, n) = 1$*.*

Demonstração. Para provar que R_a é um Sistema Reduzido de Resíduos (SRR) módulo n, devemos demonstrar três propriedades fundamentais:

1. **Quantidade de elementos:** O conjunto R possui exatamente $\phi(n)$ elementos por ser um SRR. Como R_a é formado multiplicando cada elemento de R por a, R_a possui a mesma cardinalidade, ou seja, $\phi(n)$ elementos.

2. **Coprimalidade dos elementos com** n**:** Para todo $r_i \in R$, temos $\text{mdc}(r_i, n) = 1$. Como por hipótese $\text{mdc}(a, n) = 1$, a propriedade do máximo divisor comum garante que o produto de dois inteiros relativamente primos com n também é relativamente primo com n:

$$\text{mdc}(a \cdot r_i, n) = 1 \quad \text{para todo } i \in \{1, 2, \ldots, \phi(n)\}.$$

3. **Incongruência par a par módulo** n**:** Suponha que existam elementos $a \cdot r_i, a \cdot r_j \in R_a$ tais que:

$$a \cdot r_i \equiv a \cdot r_j \pmod{n}.$$

   Como $\text{mdc}(a, n) = 1$, podemos cancelar o fator a de ambos os lados da congruência, obtendo:

$$r_i \equiv r_j \pmod{n}.$$

   Contudo, sendo R um SRR, seus elementos são todos incongruentes módulo n entre si. Logo, $r_i \equiv r_j \pmod{n}$ só é possível se $i = j$. Portanto, todos os elementos de R_a são distintos módulo n.

Como R_a é composto por $\phi(n)$ elementos mutuamente incongruentes módulo n e todos primos entre si com n, conclui-se que R_a é um SRR módulo n. □

3.6 Resíduos Quadráticos

As seções anteriores serviram para fixar a teoria necessária para podermos definir e estudar as propriedades de resíduos quadráticos e estudar algumas congruências não lineares. Isto é o que faremos a partir de agora.

Definição 3.6.1 (Resíduo Quadrático)**.** *Sejam $a, n \in \mathbb{Z}$ e primos entre si. Se $x^2 \equiv a \pmod{n}$ tiver solução, dizemos que a é um resíduo quadrático módulo n. Em caso contrário, isto é, $x^2 \not\equiv a \pmod{n}$ para todo inteiro x, dizemos que a não é um resíduo quadrático módulo n, ou ainda, a é um resíduo não-quadrático.*

Exemplo 3.6.1. *Na congruência $x^2 \equiv 2 \pmod{7}$, tem-se que 2 é resíduo quadrático módulo 7, pois $mdc(2, 7) = 1$ e $7 \mid (3^2 - 2)$, isto é, $x = 3$ é solução da congruência.*

Teorema 3.6.1. *Sejam $a \in \mathbb{Z}, p \in P^*$ e mdc(p, a) = 1. Se a congruência $x^2 \equiv a \pmod{p}$, tiver uma solução $x_0 \in \{1, 2, \ldots p-1\}$, então $mdc(x_0, p) = 1$ e $p - x_0$ também é solução não congruente a x_0. Além disso, essas são exatamente as duas únicas soluções incongruentes módulo p.*

Demonstração: Com efeito, se existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$, então

$$mdc(x_0, p) = mdc(x_0^2, p) = mdc(a, p) = 1.$$

Por outro lado,

$$(p - x_0)^2 \equiv x_0^2 \equiv a \pmod{p}.$$

Assim, x_0 e $p - x_0$ são ambas soluções da equação $x^2 \equiv a \pmod{p}$ e são incongruentes entre si. Com efeito, se fosse $x_0 \equiv (p - x_0) \pmod{p}$, então $2x_0 \equiv p \equiv 0 \pmod{p}$, ou seja, $p \mid 2x_0$. Mas, como p é um primo maior do que 2, pelo Lema de Euclides, isto obrigaria a termos $p \mid x_0$, o que seria absurdo haja vista que $mdc(x_0, p) = 1$.

Provemos, finalmente, que estas são as únicas soluções possíveis. De fato, se $x_1 \in \{1, 2, \ldots, p-1\}$ é outra solução, então

$$x_1^2 \equiv a \equiv x_0^2 \pmod{p} \implies p \mid (x_1^2 - x_0^2) \implies p \mid (x_1 - x_0) \quad \text{ou} \quad p \mid (x_1 + x_0).$$

No primeiro caso, temos $x_1 \equiv x_0 \pmod{p}$, já no segundo caso, $x_1 \equiv (p - x_0) \pmod{p}$. ■

Exemplo 3.6.2. *A congruência $3x^2 \equiv 12 \pmod{13}$ possui ou não solução?*
Solução: *Notemos que a congruência tem solução pois, para $x = 2$, tem-se que $3 \cdot 2^2 = 12 \equiv 12 \pmod{13}$.*

Teorema 3.6.2 (Teorema de Lagrange)**.** *Se $mdc(c_n, p) = 1$, com $p \in P$, então a congruência*

$$c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0 \equiv 0 \pmod{p}$$

tem, no máximo, n soluções incongruentes módulo p, onde $c_i \in \mathbb{Z}$, $i \in I_n$.

Demonstração. Utilizemos o Princípio de Indução Finita sobre o grau do polinômio. Notemos que para $n = 1$ o resultado é válido, pois temos a congruência $c_1 x + c_0 \equiv 0 \pmod{p}$, ou ainda,

$$c_1 x \equiv -c_0 \pmod{p}$$

que possui uma única solução incongruente módulo p, pelo Corolário 3.5.7 do Teorema 3.5.7. Suponhamos válido para $n = k-1$, isto é, se $g(x)$ é um polinômio de grau $k-1$, então a congruência $g(x) \equiv 0 \pmod{p}$ tem, no máximo, $k-1$ soluções incongruentes módulo p.

Mostremos que o resultado é válido para $n = k$. Para tanto, suponhamos que não valha, isto é, que existe um polinômio f de grau k tal que a congruência

$$f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_2 x^2 + c_1 x + c_0 \equiv 0 \pmod{p}$$

tenha (pelo menos) $k+1$ soluções incongruentes módulo p, sendo $\text{mdc}(c_n, p) = 1$. Digamos que estas soluções sejam: $x_0, x_1, x_2, \ldots, x_k$. Fixando x_0, temos que $f(x) - f(x_0) \equiv 0 \pmod{p}$, pois $f(x_0) \equiv 0 \pmod{p}$. Mas,

$$\begin{aligned} f(x) - f(x_0) &= c_k x^k + \cdots + c_1 x + c_0 - (c_k x_0^k + \cdots + c_1 x_0 + c_0) \\ &= c_k(x^k - x_0^k) + c_{k-1}(x^{k-1} - x_0^{k-1}) + \cdots + c_1(x - x_0). \end{aligned}$$

Percebamos que $(x - x_0)$ é um fator comum de cada parcela $c_i(x^i - x_0^i)$, com $i \in I_k$. Assim, para todo $i \in I_k$, tem-se $c_i(x^i - x_0^i) = (x - x_0) \cdot p_{i-1}(x)$, onde $p_{i-1}(x)$ é um polinômio de grau $i-1$. Seja

$$h(x) = \sum_{i=0}^{k-1} p_i(x).$$

Então $h(x)$ é um polinômio de grau $k-1$, com c_k sendo o coeficiente de x^{k-1}. Daí,

$$f(x) - f(x_0) = (x - x_0) \cdot h(x) \equiv 0 \pmod{p},$$

e isto significa que $p \mid (x - x_0) \cdot h(x)$. Como as raízes $x_{i's}$ são incongruentes duas a duas, tem-se $p \nmid (x_i - x_0)$, para cada $i \in \{1, \ldots, k\}$, logo deve-se ter $p \mid h(x_i)$ para cada $i \in I_k$. Ou seja, a congruência $h(x) \equiv 0 \pmod{p}$ possui k soluções incongruentes módulo p, contrariando a hipótese de indução. Logo, o resultado é válido para $n = k$ e, pelo PIF, vale para todo polinômio satisfazendo as condições do teorema. ∎

Lema 3.6.3. *Seja $p \in P^*$. Se $x, y \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, com $x \neq y$, então*

$$x^2 \not\equiv y^2 \pmod{p}.$$

Demonstração: Suponha, por absurdo, que $x^2 \equiv y^2 \pmod{p}$, onde $x, y \in \{1, 2, \ldots, \frac{p-1}{2}\}$ e $x \neq y$. Então,

$$(x-y)(x+y) = x^2 - y^2 \equiv 0 \pmod{p},$$

Como p é primo, pelo Lema de Euclides segue que

$$p \mid (x-y) \quad \text{ou} \quad p \mid (x+y).$$

Se $p \mid (x-y)$, então $x \equiv y \pmod{p}$. Entretanto,

$$-\frac{p-3}{2} \leq x - y \leq \frac{p-3}{2},$$

de modo que $|x-y| < p$. Assim, o único múltiplo de p possível é

$$x - y = 0,$$

ou seja, $x = y$, o que contradiz a hipótese. Por outro lado, se $p \mid (x+y)$, como

$$2 \leq x + y \leq p - 1,$$

então,

$$0 < x + y < p,$$

o que impossibilita que $x+y$ seja múltiplo de p. Novamente obtemos uma contradição. Como ambos os casos conduzem a contradições, concluímos que a hipótese

$$x^2 \equiv y^2 \pmod{p}$$

é falsa. Portanto,

$$x^2 \not\equiv y^2 \pmod{p}.$$

O Lema 3.6.3 é um resultado fundamental em Teoria dos Números, pois é justamente ele que garante que os números

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

são todos distintos módulo p. Como existem exatamente $\frac{p-1}{2}$ resíduos quadráticos não nulos módulo p, conclui-se que esse conjunto representa todos os resíduos quadráticos não nulos módulo p. Esse fato é a base para a demonstração da Lei da Reciprocidade Quadrática apresentado posteriormente.

Definição 3.6.2 (Função Maior Inteiro)**.** *A função*

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\} \end{aligned}$$

é denominada função maior inteiro.

Teorema 3.6.4. *Seja $p \in P^*$. Dentre os números $1, 2, 3, \ldots, p-1$, temos exatamente $\left\lfloor \frac{p}{2} \right\rfloor$ resíduos quadráticos módulo p.*

Aqui está o código corrigido com a estrutura segura para evitar o sumiço dos parágrafos e corrigir os erros de compilação:

Code snippet **Demonstração:** Sendo $p \in P^*$ um número primo ímpar, temos que $\left\lfloor \frac{p}{2} \right\rfloor = \frac{p-1}{2}$. Por definição, um elemento $a \in \{1, 2, 3, \ldots, p-1\}$ é um resíduo quadrático módulo p se existir algum $x \in \{1, 2, 3, \ldots, p-1\}$ tal que:

$$x^2 \equiv a \pmod{p}.$$

Considere o conjunto de todos os quadrados dos elementos de $\{1, 2, 3, \ldots, p-1\}$ módulo p:

$$S = \left\{1^2, 2^2, 3^2, \ldots, (p-1)^2\right\} \pmod{p}.$$

Observe que, para qualquer $x \in \{1, 2, \ldots, p-1\}$, vale a identidade:

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}.$$

Isso mostra que os elementos da lista S emparelham-se dois a dois, gerando os mesmos resíduos:

$$1^2 \equiv (p-1)^2 \pmod{p}, \quad 2^2 \equiv (p-2)^2 \pmod{p}, \quad \ldots, \quad k^2 \equiv (p-k)^2 \pmod{p},$$

onde $k = \frac{p-1}{2}$. Logo, o conjunto de todos os resíduos quadráticos reduz-se aos quadrados dos primeiros $\frac{p-1}{2}$ inteiros:

$$R_Q = \left\{1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\} \pmod{p}.$$

Para concluir a demonstração, devemos provar que todos os $\frac{p-1}{2}$ elementos de R_Q são distintos (incongruentes) módulo p.

Suponha, por absurdo, que existam inteiros i, j tais que $1 \leq i < j \leq \frac{p-1}{2}$ e:

$$i^2 \equiv j^2 \pmod{p} \implies j^2 - i^2 \equiv 0 \pmod{p} \implies (j-i)(j+i) \equiv 0 \pmod{p}.$$

Pelo Lema de Euclides, como p é um número primo, p deve dividir $(j-i)$ ou $(j+i)$:

1. Como $1 \leq i < j \leq \frac{p-1}{2}$, temos $0 < j - i < \frac{p-1}{2} < p$. Logo, $p \nmid (j-i)$.

2. Da mesma forma, $2 \leq j+i \leq \frac{p-1}{2} + \left(\frac{p-1}{2} - 1\right) = p-1 < p$. Logo, $p \nmid (j+i)$.

Como p não divide nenhum dos dois fatores, chegamos a uma contradição.

Portanto, os elementos $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ são dois a dois incongruentes módulo p, totalizando exatamente $\frac{p-1}{2} = \left\lfloor \frac{p}{2} \right\rfloor$ resíduos quadráticos. ■

Exemplo 3.6.3. *Do Teorema 3.6.4 decorre que* 6 *é a quantidade de resíduos quadráticos que o primo ímpar* 13 *possui, pois* $\left\lfloor \frac{13}{2} \right\rfloor = 6$. *Assim como* 15 *é a quantidade de resíduos quadráticos módulo* 31 *e* 18 *é a quantidade de resíduos quadráticos módulo* 37.

Definição 3.6.3 (Símbolo de Legendre)**.** *Sejam $a \in \mathbb{Z}$ e $p \in P^*$. O Símbolo de Legendre de a módulo p, denotado por $\left(\frac{a}{p}\right)$ (lê-se: a legendre p), é definido como:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } p \nmid a \text{ e } a \text{ é resíduo quadrático módulo } p; \\ 0, & \text{se } p \mid a; \\ -1, & \text{se } p \nmid a \text{ e } a \text{ não é resíduo quadrático módulo } p. \end{cases}$$

Exemplo 3.6.4. *Determine os valores de:*

1. $\left(\frac{1}{7}\right)$;
2. $\left(\frac{2}{3}\right)$;
3. $\left(\frac{110}{11}\right)$.

Solução: *Note que resolver os problemas acima consiste em analisar se $p \mid a$ ou se $p \nmid a$ e, neste caso, se a congruência $x^2 \equiv a \pmod{p}$ tem solução. Deste modo:*

1. *Para $x^2 \equiv 1 \pmod{7}$, temos $7 \nmid 1$ e $x = 1$ é solução ($1^2 = 1$). Então, $\left(\frac{1}{7}\right) = 1$.*
2. *Para $x^2 \equiv 2 \pmod{3}$, temos $3 \nmid 2$. Testando os resíduos de 3 ($\{1, 2\}$): $1^2 \equiv 1$ e $2^2 \equiv 4 \equiv 1$. Como nenhum quadrado é 2, a congruência não tem solução. Então, $\left(\frac{2}{3}\right) = -1$.*
3. *Para $x^2 \equiv 110 \pmod{11}$, notamos que $110 = 11 \times 10$, logo $11 \mid 110$. Portanto, $\left(\frac{110}{11}\right) = 0$.*

Teorema 3.6.5 (Critério de Euler)**.** *Se $p \in P^*$ e $mdc(p, a) = 1$, então*

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

Demonstração. Vamos considerar os casos em que a é ou não resíduo quadrático módulo p.

1º caso: a é resíduo quadrático módulo p. Então a congruência $x^2 \equiv a \pmod{p}$ tem solução. Seja x_0 uma solução. Então $p \nmid x_0$, pois $p \mid (a - x_0^2)$ e, se $p \mid x_0$, teríamos $p \mid x_0^2$, o que implicaria $p \mid a$, contrariando a hipótese.

Assim, por Fermat:

$$x_0^{p-1} \equiv 1 \pmod{p} \implies (x_0^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \tag{5}$$

Por outro lado, como $a \equiv x_0^2 \pmod{p}$, segue que:

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \pmod{p} \tag{6}$$

Por transitividade em (5) e (6), temos que:

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

2º caso: a não é resíduo quadrático módulo p. Como $p \in P^*$ e $\text{mdc}(p, a) = 1$, por Fermat, temos:

$$(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$$

isto é, $p \mid [(a^{\frac{p-1}{2}})^2 - 1] = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Como p é primo, segue que $p \mid (a^{\frac{p-1}{2}} - 1)$ ou $p \mid (a^{\frac{p-1}{2}} + 1)$, o que significa:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{ou} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{7}$$

Seja $X = \{i^2 : 1 \leq i \leq \frac{p-1}{2}\}$. Notemos que $a \notin X$, pois todo elemento de X é resíduo quadrático. Mostremos que todo elemento de X satisfaz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. De fato, considere i tal que $i \in I_{\frac{p-1}{2}}$. Como, $1 \leq i \leq \frac{p-1}{2}$, tem-se $p \nmid i$, donde, por Fermat:

$$i^{p-1} \equiv 1 \pmod{p} \implies (i^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad \forall k \in X.$$

Pelo Teorema de Lagrange, o polinômio $f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ tem, no máximo, $\frac{p-1}{2}$ raízes. Mas X tem exatamente $\frac{p-1}{2}$ elementos que satisfazem $f(x) \equiv 0 \pmod{p}$. Portanto, vale a implicação:

$$k \text{ satisfaz } x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \implies k \in X \tag{8}$$

Como $a \notin X$, por (8), segue que a não satisfaz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Assim, por (7), resta que:

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

■

Exemplo 3.6.5. *Como* $2^4 = 16 \equiv -1 \pmod{17}$*, segue que* $(2^4)^2 \equiv (-1)^2 \pmod{17}$*, ou seja,* $2^8 \equiv 1 \pmod{17}$*. Assim, pelo Critério de Euler:*

$$\left(\frac{2}{17}\right) \equiv 2^{\frac{17-1}{2}} \equiv 2^8 \equiv 1 \pmod{17}.$$

E isso só é verdadeiro se $\left(\frac{2}{17}\right) = 1$*.*

Da definição do símbolo de Legendre também chegamos a esse resultado, pois $x = 6$ *é solução da congruência* $x^2 \equiv 2 \pmod{17}$*, visto que* $6^2 = 36 = 2 \cdot 17 + 2 \equiv 2 \pmod{17}$*.*

Teorema 3.6.6. *O Símbolo de Legendre é uma função completamente multiplicativa, isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demonstração: Se p é um primo ímpar e $a, b \in \mathbb{Z}$, inicialmente, note que se $p \mid a$ ou $p \mid b$, então $p \mid ab$, e pela definição do símbolo de Legendre,

$$\left(\frac{ab}{p}\right) = 0.$$

Além disso,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0,$$

de modo que a igualdade é verdadeira. Suponhamos, portanto, que $p \nmid a$ e $p \nmid b$. Pelo Critério de Euler,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

e

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}.$$

Multiplicando essas congruências, obtemos

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \pmod{p}.$$

Aplicando novamente o Critério de Euler,

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p},$$

e, consequentemente,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Por outro lado, cada um dos números

$$\left(\frac{a}{p}\right), \quad \left(\frac{b}{p}\right), \quad \left(\frac{ab}{p}\right)$$

pertence ao conjunto $\{-1, 1\}$. Como $p \geq 3$, a congruência módulo p entre dois elementos de $\{-1, 1\}$ implica sua igualdade. Logo,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

■

Exemplo 3.6.6. *Como o símbolo de Legendre é completamente multiplicativo, temos que:*

$$\left(\frac{8}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{4}{7}\right) = 1 \cdot 1 = 1.$$

De fato, pois $x = 3$ é solução da congruência $x^2 \equiv 2 \pmod 7$ (já que $3^2 = 9 \equiv 2 \pmod 7$) e $x = 2$ é solução da congruência $x^2 \equiv 4 \pmod 7$.

Teorema 3.6.7 (Lema de Gauss)**.** *Sejam $a \in \mathbb{Z}$, $mdc(p, a) = 1$ e $p \in P^*$. Consideremos os restos na divisão por p dos números*

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a.$$

Então,

$$\left(\frac{a}{p}\right) = (-1)^r,$$

onde r é o número de restos que são maiores do que $\frac{p}{2}$.

Demonstração. Digamos que $a_1, a_2, \ldots, a_s$ sejam os restos menores que $\frac{p}{2}$ e $b_1, b_2, \ldots, b_r$ sejam os maiores que $\frac{p}{2}$.

Tendo que, cada elemento da lista $1a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ é congruente a seu resto, isto é, a um a_i ou um b_j, com $i \in I_s$ e $j \in I_r$. Podemos multiplicar todas as congruências membro a membro, obtendo:

$$1a \cdot 2a \cdot 3a \cdot \cdots \cdot \left(\frac{p-1}{2}\right)a \equiv a_1 a_2 \ldots a_s b_1 b_2 \ldots b_r \pmod p.$$

Ou ainda,

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv a_1 a_2 \ldots a_s b_1 b_2 \ldots b_r \pmod p. \tag{9}$$

Nossa demonstração consistirá agora em concluir que

$$a_1, a_2, \ldots, a_s, p - b_1, p - b_2, \ldots, p - b_r \tag{10}$$

são, a menos da ordem, os números $1, 2, \ldots, \frac{p-1}{2}$. Uma vez que $\frac{p}{2} < b_j < p$, multiplicando por -1 e somando p a todos os membros da desigualdade, decorre que $0 < p - b_j < \frac{p}{2}$, isto é, $1 \leq p - b_j \leq \frac{p-1}{2}$.

Basta mostrarmos que os números da lista (10) são todos incongruentes módulo p. Se $a_i \equiv p - b_j \pmod{p}$, teríamos $a_i + b_j \equiv 0 \pmod{p}$. Mas como $a_i \equiv k \cdot a$ e $b_j \equiv t \cdot a$ para alguns $k, t \in \{1, \ldots, \frac{p-1}{2}\}$, isso implicaria $(k+t)a \equiv 0 \pmod{p}$. Como $\text{mdc}(a, p) = 1$, teríamos $k + t \equiv 0 \pmod{p}$, o que é impossível pois $2 \leq k + t \leq p - 1$. Portanto, os números da lista (10) são exatamente os elementos da lista $1, 2, \ldots, \frac{p-1}{2}$. Logo, por reflexividade:

$$a_1 a_2 \ldots a_s (p - b_1)(p - b_2) \ldots (p - b_r) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) \pmod{p},$$

e como, $p - b_i \equiv -b_i \pmod{p}$, isto equivale a:

$$(-1)^r a_1 a_2 \ldots a_s b_1 b_2 \ldots b_r \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Por transitividade com a congruência (9):

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^r \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Como $\text{mdc}\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$, podemos cancelar o fatorial, obtendo:

$$a^{\frac{p-1}{2}} \equiv (-1)^r \pmod{p}.$$

Pelo Critério de Euler, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Assim, $\left(\frac{a}{p}\right) \equiv (-1)^r \pmod{p}$, o que implica:

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

■

Exemplo 3.6.7. *Tomemos $a = 3$ e $p = 11$ no Lema de Gauss. Calculando os restos módulo 11 dos múltiplos de 3 na lista $\{1, 2, 3, 4, 5\}$ (pois $\frac{11-1}{2} = 5$):*

$$1 \cdot 3 \equiv 3 \pmod{11}$$
$$2 \cdot 3 \equiv 6 \pmod{11}$$
$$3 \cdot 3 \equiv 9 \pmod{11}$$
$$4 \cdot 3 = 12 \equiv 1 \pmod{11}$$
$$5 \cdot 3 = 15 \equiv 4 \pmod{11}$$

Os restos obtidos são $\{3, 6, 9, 1, 4\}$. Dentre estes restos, apenas 6 e 9 são maiores do que $\frac{11}{2} = 5,5$. Portanto, temos $r = 2$ restos na região superior. Assim, pelo Lema de Gauss:

$$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

3.6.1 Suplementos à Lei de Reciprocidade Quadrática

Enquanto a Lei de Reciprocidade Quadrática relaciona os símbolos de Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$ para primos ímpares distintos p e q, os *Suplementos* abordam os casos em que o valor do numerador não é um primo ímpar. Em particular, o Primeiro Suplemento dedica-se a caracterizar os primos ímpares p para os quais -1 é um resíduo quadrático, isto é, estabelece a condição necessária e suficiente para que a congruência

$$x^2 \equiv -1 \pmod{p}$$

admita solução em $\mathbb{Z}$.

Teorema 3.6.8 (1º Teorema Suplementar)**.** *Se $p \in P^*$, então*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 4 \\ -1, & \text{se } p \equiv -1 \pmod 4. \end{cases}$$

Demonstração. Pelo Algoritmo da Divisão, na divisão por 4, todos os inteiros são da forma $4k, 4k+1, 4k+2$ ou $4k+3$. Como p é um primo ímpar, as possibilidades se reduzem a $4k+1$ ou $4k+3$. É fácil ver que $p = 4k+1$ equivale a $p \equiv 1 \pmod 4$ e que $p = 4k+3$ equivale a $p \equiv 3 \equiv -1 \pmod 4$. Vamos analisar o valor de $(-1)^{\frac{p-1}{2}}$ em cada um destes casos:

1º caso: $p = 4k+1$.
Então $p-1 = 4k$, isto é, $\frac{p-1}{2} = 2k$ é par. Daí, $(-1)^{\frac{p-1}{2}} = 1$. Pelo Critério de Euler:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

ou seja, $\left(\frac{-1}{p}\right) = 1$, se $p \equiv 1 \pmod 4$.

2º caso: $p = 4k+3$.
Então $p-1 = 4k+2 = 2(2k+1)$, isto é, $\frac{p-1}{2} = 2k+1$ é ímpar. Daí, $(-1)^{\frac{p-1}{2}} = -1$. Pelo Critério de Euler:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

ou seja, $\left(\frac{-1}{p}\right) = -1$, se $p \equiv -1 \pmod 4$.

■

Exemplo 3.6.8. *O Teorema 3.6.8 nos fornece $\left(\frac{-1}{13}\right) = 1$, pois $13 \equiv 1 \pmod 4$. De fato, -1 é um resíduo quadrático módulo 13, pois $x = 5$ é solução da congruência $x^2 \equiv -1 \pmod{13}$ (visto que $5^2 = 25 \equiv 12 \equiv -1 \pmod{13}$).*

Pelo mesmo teorema, $\left(\frac{-1}{7}\right) = -1$*, já que* $7 \equiv 3 \equiv -1 \pmod 4$*. Com efeito, a congruência* $x^2 \equiv -1 \pmod 7$ *não tem solução. Pelo Algoritmo da Divisão, qualquer* x *é da forma* $7k + r$*, com* $r \in \{0, 1, 2, 3, 4, 5, 6\}$*. Testando os quadrados dos restos:*

- $0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4$ *e* $3^2 \equiv 9 \equiv 2$;
- $4^2 \equiv 16 \equiv 2 \quad 5^2 \equiv 25 \equiv 4$ *e* $6^2 \equiv 36 \equiv 1$.

Os resíduos quadráticos módulo 7 *são* $\{0, 1, 2, 4\}$*. Como* $-1 \equiv 6 \pmod 7$ *não pertence a este conjunto, 7 nunca divide* (x^2+1)*. Por isso, pela definição do Símbolo de Legendre,* $\left(\frac{-1}{7}\right) = -1$.

Proposição 3.6.9. *Seja* n *um natural ímpar maior do que* 2*. Então, vale a igualdade:*

$$1 + 2 + 3 + \cdots + \frac{n-1}{2} = \frac{n^2 - 1}{8}.$$

Demonstração rápida: Trata-se da soma de uma Progressão Aritmética (PA) com $k = \frac{n-1}{2}$ termos. A fórmula da soma é $S_k = \frac{(a_1+a_k)k}{2}$.

$$S_k = \frac{\left(1 + \frac{n-1}{2}\right)\left(\frac{n-1}{2}\right)}{2} = \frac{\left(\frac{n+1}{2}\right)\left(\frac{n-1}{2}\right)}{2} = \frac{\frac{n^2-1}{4}}{2} = \frac{n^2 - 1}{8}.$$

■

Teorema 3.6.10 (2º Teorema Suplementar)**.** *Se* $p \in P^*$*, então*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8 \\ -1, & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Demonstração. Pelo Critério de Euler, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p$. Mostraremos que a validade da congruência

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p \tag{11}$$

será suficiente para, por transitividade, concluirmos o teorema. Para isto, consideraremos todos os possíveis restos de p na divisão por 8. Mas antes, vamos demonstrar que a congruência (11) é verdadeira. Seja $i \in \{1, 2, 3, \ldots, \frac{p-1}{2}\}$. Então, se i é par, segue que:

$$i \equiv i \cdot (-1)^i \pmod p. \tag{12}$$

Se, porém, i é ímpar, segue que:

$$p - i \equiv (-1)^i \cdot i \pmod p. \tag{13}$$

Percebamos que, em ambos os tipos, (12) ou (13), os números dos membros esquerdos das congruências são sempre números pares. Mais ainda, estes números são

$2, 4, 6, \ldots, p-1$. Assim, multiplicando todas essas $\frac{p-1}{2}$ congruências membro a membro, obtemos:

$$2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{(1+2+\cdots+\frac{p-1}{2})} \pmod{p}.$$

Como $2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-1) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$ e, pela Proposição 3.6.9, $1+2+\cdots+\frac{p-1}{2} = \frac{p^2-1}{8}$, temos:

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Cancelando o fator $(\frac{p-1}{2})!$, obtemos o resultado da congruência (11). Agora, analisaremos os restos de p módulo 8 usando a igualdade:

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8}. \tag{14}$$

1º caso: $p = 8k+1$.
Então $\frac{8k(8k+2)}{8} = 2k(4k+1)$, que é **par**. Logo, $(-1)^{\frac{p^2-1}{8}} = 1$.

2º caso: $p = 8k+3$.
Então $\frac{(8k+2)(8k+4)}{8} = (4k+1)(2k+1)$, que é **ímpar**. Logo, $(-1)^{\frac{p^2-1}{8}} = -1$.

3º caso: $p = 8k+5$.
Então $\frac{(8k+4)(8k+6)}{8} = (2k+1)(4k+3)$, que é **ímpar**. Logo, $(-1)^{\frac{p^2-1}{8}} = -1$.

4º caso: $p = 8k+7$.
Então $\frac{(8k+6)(8k+8)}{8} = 2(4k+3)(k+1)$, que é **par**. Logo, $(-1)^{\frac{p^2-1}{8}} = 1$.

Isso conclui que $\left(\frac{2}{p}\right) = 1$ se $p \equiv \pm 1 \pmod 8$ e $\left(\frac{2}{p}\right) = -1$ se $p \equiv \pm 3 \pmod 8$. □

Exemplo 3.6.9. *Do Teorema 3.8, segue que* $\left(\frac{2}{5}\right) = -1$ *e* $\left(\frac{2}{7}\right) = 1$, *pois* $5 \equiv -3 \pmod 8$ *e* $7 \equiv -1 \pmod 8$. *Esse é o mesmo resultado obtido através da definição do símbolo. Com efeito, a congruência* $x^2 \equiv 2 \pmod 5$ *não tem solução, pois o Algoritmo da Divisão garante que* x *é da forma* $5t, 5t+1, 5t+2, 5t+3$ *ou* $5t+4$. *Calculando* $x^2 - 2 \pmod 5$ *para cada resto:*

- *Se* $x \equiv 0$, *então* $x^2 - 2 \equiv -2 \equiv 3 \pmod 5$
- *Se* $x \equiv 1$, *então* $x^2 - 2 \equiv 1 - 2 \equiv 4 \pmod 5$
- *Se* $x \equiv 2$, *então* $x^2 - 2 \equiv 4 - 2 \equiv 2 \pmod 5$
- *Se* $x \equiv 3$, *então* $x^2 - 2 \equiv 9 - 2 \equiv 7 \equiv 2 \pmod 5$
- *Se* $x \equiv 4$, *então* $x^2 - 2 \equiv 16 - 2 \equiv 14 \equiv 4 \pmod 5$

Como nenhum desses resultados é múltiplo de 5 *(ou seja,* $\equiv 0 \pmod 5$*), concluímos que* $\left(\frac{2}{5}\right) = -1$. *Por outro lado,* $x = 3$ *é solução da congruência* $x^2 \equiv 2 \pmod 7$ *(visto que* $3^2 = 9 \equiv 2 \pmod 7$*) e, por isso,* $\left(\frac{2}{7}\right) = 1$.

3.7 A Lei de Reciprocidade Quadrática

Nesta seção apresentaremos um importante teorema que nos ajudará a relacionar o valor para o Símbolo de Legendre entre dois primos distintos. Conhecendo o valor para $\left(\frac{p}{q}\right)$, será que temos condições de determinarmos $\left(\frac{q}{p}\right)$? A Lei mostrará em qual caso isso é possível.

O próximo resultado é fundamental para a demonstração da Lei. Para demonstrá-lo, utilizaremos alguns resultados, tais como o Algoritmo da Divisão e o Lema de Gauss. Pedimos aos leitores que, caso não recordem, revejam estes teoremas antes de prosseguir.

Teorema 3.7.1 (Eisenstein)**.** *Seja a um inteiro ímpar e $p \in P^*$, tal que $mdc(p, a) = 1$. Definindo*

$$M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \left\lfloor \frac{3a}{p} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{p-1}{2}\right) \cdot a}{p} \right\rfloor,$$

temos

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

Demonstração. Nossa demonstração consiste, inicialmente, em determinar os restos módulo p do conjunto $Y_a = \{a, 2a, \ldots, \frac{p-1}{2}a\}$. Para isso, aplicamos o Algoritmo da Divisão para cada elemento de Y_a:

$$\begin{aligned} a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1, \quad 0 \leq r_1 < p \\ 2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2, \quad 0 \leq r_2 < p \\ &\vdots \\ \left(\frac{p-1}{2}\right)a &= p\left\lfloor \frac{\left(\frac{p-1}{2}\right) \cdot a}{p} \right\rfloor + r_{\frac{p-1}{2}}, \quad 0 \leq r_{\frac{p-1}{2}} < p. \end{aligned}$$

Perceba que cada r_k corresponde aos a_i (menores que $p/2$) ou b_j (maiores que $p/2$) definidos na demonstração do Lema de Gauss. Somando as igualdades membro a membro e utilizando a Proposição 3.1:

$$a\left(\frac{p^2-1}{8}\right) = p\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum r_k = pM + \sum a_i + \sum b_j. \tag{3.3.11}$$

Seja $I = \sum a_i$ e $S = \sum b_j$. Como vimos no Lema de Gauss, os números $\{a_1, \ldots, a_s, p - b_1, \ldots, p - b_r\}$ são, a menos da ordem, $\{1, 2, \ldots, \frac{p-1}{2}\}$. Logo:

$$\frac{p^2-1}{8} = \sum a_i + \sum(p - b_j) = I + rp - S. \tag{3.3.12}$$

Subtraindo (3.3.12) de (3.3.11), obtemos:

$$\frac{p^2-1}{8}(a-1) = p(M-r) + 2S.$$

Como a é ímpar por hipótese, $(a-1)$ é par, o que torna o lado esquerdo da igualdade par. Para que o lado direito seja par, como $2S$ já o é, $p(M-r)$ deve ser par. Sendo p um primo ímpar, conclui-se que $(M-r)$ é par.
Isso significa que M e r possuem a mesma paridade. Portanto:

$$(-1)^r = (-1)^M.$$

Pelo Lema de Gauss, $\left(\frac{a}{p}\right) = (-1)^r$, logo $\left(\frac{a}{p}\right) = (-1)^M$. ∎

Para ilustrar o Teorema 3.7.1 de Eisenstein na prática, vamos calcular o símbolo de Legendre em dois casos simples.

Exemplo 3.7.1. *: Calcular* $\left(\frac{3}{7}\right)$.
Aqui, $p = 7$ *(primo ímpar) e* $a = 3$ *(ímpar, com* $\text{mdc}(3,7) = 1$*). O limite do somatório é* $\frac{p-1}{2} = \frac{7-1}{2} = 3$*. Calculamos* S*:*

$$\begin{aligned} S &= \sum_{x=1}^{3} \left\lfloor \frac{3x}{7} \right\rfloor \\ &= \left\lfloor \frac{3(1)}{7} \right\rfloor + \left\lfloor \frac{3(2)}{7} \right\rfloor + \left\lfloor \frac{3(3)}{7} \right\rfloor \\ &= \left\lfloor \frac{3}{7} \right\rfloor + \left\lfloor \frac{6}{7} \right\rfloor + \left\lfloor \frac{9}{7} \right\rfloor \\ &= 0 + 0 + 1 = 1 \end{aligned}$$

Como $S = 1$ *é ímpar, temos* $\left(\frac{3}{7}\right) = (-1)^1 = -1$*. Isso significa que* 3 *não é um resíduo quadrático módulo* 7 *(não existe nenhum* x *tal que* $x^2 \equiv 3 \pmod 7$*).*

Exemplo 3.7.2.

: Calcular $\left(\frac{7}{5}\right)$
Aqui, $p = 5$ (primo ímpar) e $a = 7$ (ímpar, com $\text{mdc}(7,5) = 1$). O limite do somatório é $\frac{p-1}{2} = \frac{5-1}{2} = 2$. Calculamos S:

$$\begin{aligned} S &= \sum_{x=1}^{2} \left\lfloor \frac{7x}{5} \right\rfloor \\ &= \left\lfloor \frac{7(1)}{5} \right\rfloor + \left\lfloor \frac{7(2)}{5} \right\rfloor \\ &= \left\lfloor \frac{7}{5} \right\rfloor + \left\lfloor \frac{14}{5} \right\rfloor \\ &= 1 + 2 = 3 \end{aligned}$$

Como $S = 3$ é ímpar, temos $\left(\frac{7}{5}\right) = (-1)^3 = -1$. Isso está correto, pois $7 \equiv 2 \pmod 5$, e sabemos que 2 não é um resíduo quadrático módulo 5.

Em vistas de estabelecer a Lei de Reciprocidade Quadrática, vamos revisar o símbolo de Legendre, denotado por $\left(\frac{a}{p}\right)$.

Para um número primo ímpar p e um inteiro a, define-se:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é um resíduo quadrático módulo } p \text{ e } p \nmid a, \\ -1 & \text{se } a \text{ é um não-resíduo quadrático módulo } p, \\ 0 & \text{se } p \mid a. \end{cases}$$

A importância deste símbolo na aritmética reside na sua capacidade de transformar a busca por soluções de congruências do tipo $x^2 \equiv a \pmod p$ em um cálculo algébrico sistemático. Ele é fundamental para a formulação da Lei da Reciprocidade Quadrática e possui propriedades multiplicativas cruciais, como $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ como demonstrado no Teorema 3.6.6 da Seção 3.6. Na teoria dos números moderna, é a base para testes de primalidade e sistemas de criptografia assimétrica (Hardy; Wright, 2008). Vejamos alguns exemplos:

- **Exemplo 1:** $\left(\frac{2}{7}\right) = 1$. O número 2 é um resíduo quadrático módulo 7 pois $3^2 = 9 \equiv 2 \pmod 7$.
- **Exemplo 2:** $\left(\frac{5}{7}\right) = -1$. O número 5 não é um resíduo quadrático módulo 7, pois ao testarmos os quadrados $1^2, 2^2, 3^2 \pmod 7$ obtemos os restos $\{1, 4, 2\}$, nenhum dos quais é 5.

O próximo resultado, conhecido como Lei de Reciprocidade Quadrática - LRQ, estabelece que se ao menos um dos primos p ou q for congruente a $1 \pmod 4$, então p será um resíduo quadrático módulo q se, e somente se, q for um resíduo quadrático módulo p. Caso ambos sejam congruentes a $3 \pmod 4$, ocorre a reciprocidade inversa (um será resíduo e o outro não-resíduo).

Teorema 3.7.2 (Lei de Reciprocidade Quadrática - LRQ)**.** *Sejam $p, q \in P^*$ números primos ímpares distintos, então:*

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

Demonstração: Existem mais de 240 demonstrações publicadas para este teorema. A demonstração a seguir, devida a (Eisenstein, 1844), destaca-se por sua elegância geométrica e apoia-se num corolário do Lema de Gauss. Conforme estruturado em textos clássicos como Santos (Santos, 2015), a prova baseia-se na contagem de pontos

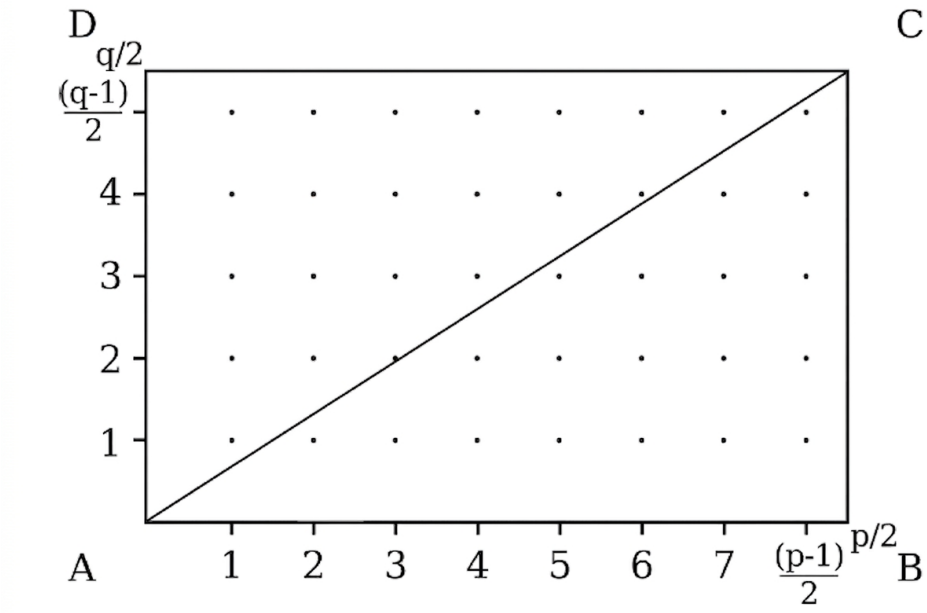


Figura 1 – Demonstração da LRQ

de coordenadas inteiras (pontos de rede) no interior de uma região no plano cartesiano.

Sejam p e q primos ímpares distintos. Consideremos o retângulo no plano Euclidiano com vértices nos pontos $(0,0)$, $(p/2,0)$, $(p/2,q/2)$ e $(0,q/2)$. O interior desse retângulo contém um número de pontos de coordenadas inteiras dado pelo produto dos números inteiros positivos menores que $p/2$ e $q/2$. Seja S o conjunto desses pontos:

$$S = \left\{ (x,y) \in \mathbb{Z}^2 \;\middle|\; 1 \leq x \leq \frac{p-1}{2},\ 1 \leq y \leq \frac{q-1}{2} \right\}$$

O número total de pontos em S é claramente:

$$|S| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

Agora, traçamos a diagonal principal do retângulo, conectando a origem $(0,0)$ ao vértice $(p/2,q/2)$. A equação da reta que contém essa diagonal é $y = \frac{q}{p}x$.

Como p e q são primos distintos e $x < p/2$, não existe nenhum ponto do conjunto S exatamente sobre a diagonal (pois $qy = px$ implicaria que p divide x, o que é impossível já que $0 < x < p/2$). Portanto, a diagonal divide o conjunto de pontos S em duas regiões disjuntas: os pontos abaixo da diagonal e os pontos acima da diagonal.

1. **Pontos abaixo da diagonal:** Para um dado valor inteiro de x (com $1 \leq x \leq \frac{p-1}{2}$), os pontos (x,y) abaixo da reta $y = \frac{q}{p}x$ devem satisfazer $1 \leq y < \frac{q}{p}x$. O número de tais inteiros y é exatamente a parte inteira de $\frac{qx}{p}$, denotada por $\lfloor \frac{qx}{p} \rfloor$.

Somando sobre todos os x possíveis, o número total de pontos abaixo da diagonal, que chamaremos de μ, é:

$$\mu = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$$

2. **Pontos acima da diagonal:** Por uma simetria análoga, permutando os eixos, o número de pontos do conjunto S que estão acima da diagonal, que chamaremos de ν, é dado por:

$$\nu = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$$

Como o total de pontos no retângulo é a soma dos pontos abaixo e acima da diagonal, temos:

$$\mu + \nu = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

Pelo Lema de Gauss (que estabelece que $\left(\frac{a}{p}\right) = (-1)^m$, onde m é o número de múltiplos de a no intervalo $[1, \frac{p-1}{2}]$ cujos restos módulo p são maiores que $p/2$), tem-se:

$$\left(\frac{q}{p}\right) = (-1)^{\mu} \quad \text{e} \quad \left(\frac{p}{q}\right) = (-1)^{\nu}$$

Multiplicando ambos os símbolos de Legendre e utilizando a soma total dos pontos $\mu + \nu$ deduzida pela geometria do retângulo, obtemos:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu} \cdot (-1)^{\nu} = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Isso conclui a demonstração geométrica da Lei da Reciprocidade Quadrática. ■

Exemplo 3.7.3. *Verifique se* 6481 *é resíduo quadrático módulo* 6661.

Solução: *Notemos que isto equivale a calcular* $\left(\frac{6481}{6661}\right)$. *Como tanto* 6481 *quanto* 6661 *são primos ímpares e ambos são congruentes a 1 módulo 4, pela Lei de Reciprocidade Quadrática:*

$$\left(\frac{6481}{6661}\right)\left(\frac{6661}{6481}\right) = (-1)^{\frac{6661-1}{2}\cdot\frac{6481-1}{2}} = 1.$$

Dessa forma, $\left(\frac{6481}{6661}\right) = \left(\frac{6661}{6481}\right)$. *Primeiramente, note que:*

$$6661 \equiv 180 \pmod{6481}, \quad \textit{ou seja,} \quad \left(\frac{6661}{6481}\right) = \left(\frac{180}{6481}\right).$$

Fatorando $180 = 2^2 \cdot 3^2 \cdot 5$, *e usando a propriedade multiplicativa do símbolo:*

$$\left(\frac{180}{6481}\right) = \left(\frac{2^2 \cdot 3^2 \cdot 5}{6481}\right) = \left(\frac{2^2}{6481}\right)\left(\frac{3^2}{6481}\right)\left(\frac{5}{6481}\right).$$

Como 2^2 *e* 3^2 *são quadrados perfeitos, seus símbolos de Legendre são iguais a* 1*. Assim:*

$$\left(\frac{180}{6481}\right) = 1 \cdot 1 \cdot \left(\frac{5}{6481}\right) = \left(\frac{5}{6481}\right).$$

Como $5 \equiv 1 \pmod 4$*, aplicamos a Lei de Reciprocidade Quadrática novamente para inverter o símbolo:*

$$\left(\frac{5}{6481}\right) = \left(\frac{6481}{5}\right).$$

Finalmente, observando que $6481 \equiv 1 \pmod 5$*, temos:*

$$\left(\frac{6481}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Portanto, como o símbolo final é 1*, concluímos que* 6481 *é resíduo quadrático módulo* 6661*.*

Em seu trabalho acadêmico (Teixeira, 2021), demonstrou a irracionalidade de $\sqrt{2}$, vamos demonstrar, a mesma, abaixo e em seguida vamos mostrar a irracionalidade para qualquer p primo.

Exemplo 3.7.4. $\sqrt{2}$ *é irracional.*

Demonstração: *Suponha por absurdo que* $\sqrt{2} \in \mathbb{Q}$*. Assim, existem a e b inteiros primos entre si tais que*

$$\sqrt{2} = \frac{a}{b}.$$

Consequentemente,

$$2b^2 = a^2.$$

Tomemos um p primo ímpar tal que $p \equiv \pm 3 \pmod 8$*. Por outro lado, é notório que as congruências abaixo têm soluções:*

$$x^2 \equiv a^2 \pmod p \quad e \quad x^2 \equiv b^2 \pmod p.$$

Pelo símbolo de Legendre, $\left(\frac{a^2}{p}\right) = 1$ *e* $\left(\frac{b^2}{p}\right) = 1$*, mas, como* $a^2 \equiv 2b^2 \pmod p$*, segue que*

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

Temos que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$*.*

Se $p \equiv 3 \pmod 8$*, existe um inteiro k tal que* $p = 8k + 3$*, assim:*

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k+2)(8k+4)}{8} = (2k+1)(4k+1)$$

logo, $\frac{p^2-1}{8}$ *é ímpar e, portanto,* $\left(\frac{2}{p}\right) = -1$*.*

Se $p \equiv -3 \pmod 8$*, existe k inteiro tal que* $p = 8k - 3$*, então*

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k-4)(8k-2)}{8} = (2k-1)(4k-1)$$

o que implica que $\frac{p^2-1}{8}$ *é ímpar, portanto* $\left(\frac{2}{p}\right) = -1$. *Temos uma contradição! Portanto,* $\sqrt{2}$ *é irracional.* ■

Seguindo o mesmo método feito por (Teixeira, 2021) podemos demonstrar a irracionalidade de $\sqrt{3}$.

Exemplo 3.7.5. $\sqrt{3}$ *é irracional.*

Demonstração: *Suponha por absurdo que* $\sqrt{3} \in \mathbb{Q}$. *Assim, existem a e b inteiros primos entre si tais que*

$$\sqrt{3} = \frac{a}{b}.$$

Consequentemente,

$$3b^2 = a^2.$$

Tomemos um p primo ímpar tal que $p \equiv \pm 5 \pmod{12}$. *Por outro lado, é notório que as congruências abaixo têm soluções:*

$$x^2 \equiv a^2 \pmod{p} \quad e \quad x^2 \equiv b^2 \pmod{p}.$$

Pelo símbolo de Legendre, $\left(\frac{a^2}{p}\right) = 1$ *e* $\left(\frac{b^2}{p}\right) = 1$, *mas, como* $a^2 \equiv 3b^2 \pmod{p}$, *segue que*

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{3b^2}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{3}{p}\right).$$

Pela Lei de Reciprocidade Quadrática, sabemos que:

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Se $p \equiv 5 \pmod{12}$, *existe um inteiro k tal que* $p = 12k + 5$, *assim* $\frac{p-1}{2} = 6k + 2$ *(que é par) e* $p \equiv 2 \pmod{3}$, *do que resulta* $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. *Portanto:*

$$\left(\frac{3}{p}\right) = (-1)^{6k+2} \cdot (-1) = 1 \cdot (-1) = -1.$$

Se $p \equiv -5 \equiv 7 \pmod{12}$, *existe um inteiro k tal que* $p = 12k+7$, *assim* $\frac{p-1}{2} = 6k+3$ *(que é ímpar) e* $p \equiv 1 \pmod{3}$, *do que resulta* $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. *Portanto:*

$$\left(\frac{3}{p}\right) = (-1)^{6k+3} \cdot 1 = (-1) \cdot 1 = -1.$$

Temos uma contradição! Portanto, $\sqrt{3}$ *é irracional.* ■

Tendo em vista os resultados anteriores é natural indagarmos se conseguimos demonstrar a irracionalidade de $\sqrt{p}$, com p primo. A resposta é sim. Inclusive, Renan (Isneri; Vieira; Silva, 2024) demonstra a irracionalidade de $\sqrt[2n]{p}$, com p primo para

todo n natural. Todavia, apresentaremos a irracionalidade de $\sqrt{p}$, de uma forma que entendemos ser mais simples, apesar de utilizarmos essencialmente as mesmas ideias.

Observação: Para o próximo resultado, vale relembrar a seguinte propriedade: Pela Lei de Reciprocidade Quadrática (LRQ):

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

segue que, se $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, temos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \implies \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Por outro lado, se $p \equiv 3 \pmod 4$ e $q \equiv 3 \pmod 4$, então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \implies \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Teorema 3.7.3. *Se p é primo, então $\sqrt{p} \notin \mathbb{Q}$.*

Demonstração: Para $p = 2$ ou $p = 3$ o resultado já foi verificado. Vamos provar para p primo maior do que 3. Para isto, faremos uso dos seguintes fatos:

Fato 1: Segue da Lei dos Resíduos Quadráticos que dado p primo ímpar, existem exatamente $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não quadráticos. Assim, se $p \geq 5$, existem resíduos a e a' tais que:

$$\left(\frac{a}{p}\right) = 1 \quad \text{e} \quad \left(\frac{a'}{p}\right) = -1.$$

Fato 2: Para todo a e p inteiros tais que $m.d.c\{a, p\} = 1$, o Teorema de Dirichlet assegura que existem infinitos primos da forma $a + pk$, com $k \in \mathbb{Z}$.

Passemos agora a demonstração do Teorema. Suponha por absurdo que $\sqrt{p} = \frac{m}{n}$ com m, n inteiros tais que $(m, n) = 1$ e $n \neq 0$. Isto equivale a dizer que $n^2p = m^2$. Assim, para todo primo q, tem-se:

$$1 = \left(\frac{m^2}{q}\right) = \left(\frac{n^2p}{q}\right) = \left(\frac{n^2}{q}\right)\left(\frac{p}{q}\right) = 1 \cdot \left(\frac{p}{q}\right) = \left(\frac{p}{q}\right).$$

Vamos dividir a prova em dois casos:

Caso 1: $p \equiv 1 \pmod 4$.

Pela observação anterior, segue da LRQ que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Entretanto, escolhendo um primo q da forma $q = a' + pk$ (Fato 2) com $\left(\frac{a'}{p}\right) = -1$ (Fato 1),

$$\left(\frac{q}{p}\right) = \left(\frac{a + pK}{p}\right) = \left(\frac{a}{p}\right) = -1,$$

teremos uma contradição.

Caso 2: $p \equiv 3 \pmod 4$

Considere $a \in \mathbb{Z}$ com $\left(\frac{a}{p}\right) = 1$ (Fato 1). Como p é primo maior ou igual a 5, tem-se $m.d.c\{4, p\} = 1$. Logo, pelo Teorema Chinês dos Restos, o sistema de congruências abaixo tem solução inteira.

$$\begin{cases} x & \equiv & 3 & \pmod 4 \\ x & \equiv & a & \pmod p. \end{cases}$$

Seja q_0 uma solução desse sistema. Em particular, $q_0 \equiv a \pmod p$. Desde que a é um resíduo quadrático, $p \nmid a$, consequentemente, $p \nmid q_0$, uma vez que a e q_0 têm os mesmos restos quando divididos por p. Isto implica que $m.d.c\{q_0, p\} = 1$. Da primeira equação conclui-se que $m.d.c\{q_0, 4\} = 1$. Portanto, $m.d.c\{q_0, 4p\} = 1$. Pelo Teorema de Dirichlet (FATO 2) podemos escolher um primo q tal que $q = q_0 + 4pK$. Portanto,

$$\begin{cases} q & \equiv & q_0 & \equiv & 3 & \pmod 4 \\ q & \equiv & q_0 & \equiv & a & \pmod p. \end{cases}$$

Seque da primeira equação e da LRQ que $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Portanto,

$$\left(\frac{p}{q}\right) = 1 \implies \left(\frac{q}{p}\right) = -1.$$

Por outro lado, segue da segunda equação:

$$\left(\frac{q}{p}\right) = \left(\frac{q_0}{p}\right) = \left(\frac{a}{p}\right) = 1, \quad \text{um absurdo.}$$

O absurdo seguiu da hipótese de $\sqrt{p}$ ser racional. ■

Uma outra aplicação bem interessante é apresentada abaixo. Ela diz essencialmente que nenhum primo da forma $6k + 5$ fatora o termo $x^2 + 3$, qualquer que seja $x \in \mathbb{Z}$.

Exemplo 3.7.6. *Todos os divisores primos ímpares de* $x^2 + 3$ *pertencem à classe* $1 \pmod 3$.

Demonstração: É suficiente provar que, se p é primo da forma $5+6k$, então $\left(\frac{-3}{p}\right) = -1$. Ora, note que, claramente $p \neq 3$. Ademais,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right).$$

Por outro lado, da Lei de Reciprocidade Quadrática,

$$\left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Assim,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right).$$

De onde seque que,

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Por outro lado, desde que $p = 6k + 5$, temos $p \equiv 2 \pmod 3$, assim,

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1 \implies \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1. \quad \blacksquare$$

4 Equações diofantinas

A formulação das equações diofantinas constitui um dos pilares centrais da Teoria elementar dos números. Em termos matemáticos estritos, o conceito de equação diofantina faz referência a qualquer equação, envolvendo uma ou múltiplas variáveis, na qual as soluções admissíveis estão rigorosamente restritas a um conjunto numérico específico (Zawaira A.; Hitchcock, 2009). O escopo desse conjunto de soluções pode abranger os números racionais, os inteiros ou até mesmo apenas os números não negativos, dependendo da especificidade do problema matemático em análise.

Do ponto de vista analítico, contudo, o interesse acadêmico frequentemente recai de forma mais específica sobre a determinação de soluções inteiras para equações cujos coeficientes também pertencem, eles próprios, ao conjunto dos números inteiros (Koshy, 2007). Tais expressões são denominadas equações diofantinas em deferência a Diofanto de Alexandria, um matemático da antiguidade que registrou extensas contribuições literárias sobre o tema e a sua resolução matemática (Koshy, 2007; Zawaira A.; Hitchcock, 2009).

É importante destacar que a caracterização matemática fundamental de uma equação diofantina não é determinada pela sua estrutura algébrica ou pelo grau do polinómio em questão, mas sim pela restrição prévia do domínio das suas soluções. Por exemplo, mediante a imposição fundamental de que as soluções sejam inteiras, uma equação puramente linear da forma

$$2x + 3y = 4 \tag{4.1}$$

é classificada formalmente como uma equação diofantina (Zawaira A.; Hitchcock, 2009).

De maneira análoga, formulações não lineares clássicas, tais como as equações quadráticas representadas por

$$x^2 + y^2 = 1 \tag{4.2}$$

e a célebre equação que descreve os comprimentos dos lados dos triângulos pitagóricos,

$$x^2 + y^2 = z^2 \tag{4.3}$$

inserem-se estritamente nesta mesma categoria matemática, desde que submetidas à mesma restrição de domínio para as suas variáveis (Koshy, 2007).

4.1 Equações diofantinas lineares

Uma subcategoria de particular importância e amplamente estudada na Teoria elementar dos números é a das equações diofantinas lineares. De forma rigorosa, uma

equação diofantina linear de duas variáveis é uma expressão algébrica do primeiro grau que pode ser escrita na forma geral:

$$ax + by = c \tag{4.4}$$

onde a, b e c são constantes inteiras dadas, com a e b não simultaneamente nulos, e para a qual se procuram soluções (x, y) que pertençam estritamente ao conjunto dos números inteiros ($\mathbb{Z}$) (Koshy, 2007; Zawaira A.; Hitchcock, 2009).

Do ponto de vista geométrico, resolver uma equação diofantina linear de duas variáveis equivale a determinar os pontos que residem sobre a reta descrita pela equação no plano cartesiano cujas coordenadas sejam estritamente inteiras. Na literatura matemática, estes pontos bidimensionais formados exclusivamente por coordenadas inteiras são frequentemente denominados pontos de rede (*lattice points*) (Zawaira A.; Hitchcock, 2009).

Um teorema fundamental associado a estas equações estabelece o seu critério de solubilidade: a equação linear $ax + by = c$ admite pelo menos uma solução inteira se, e somente se, o máximo divisor comum (MDC) dos coeficientes a e b, denotado por $d = \text{mdc}(a, b)$, for um divisor exato do termo independente c (Koshy, 2007). Caso esta condição seja satisfeita, a equação possuirá um número infinito de soluções inteiras, que podem ser sistematicamente determinadas com o auxílio do Algoritmo de Euclides.

Para ilustrar este conceito analítico, consideremos o seguinte exemplo prático:

$$2x + 3y = 4. \tag{4.5}$$

Neste caso, os coeficientes são $a = 2$ e $b = 3$. O máximo divisor comum entre 2 e 3 é 1 ($\text{mdc}(2, 3) = 1$). Uma vez que 1 é, por definição, um divisor de 4 (o termo independente c), o teorema garante matematicamente que esta equação possui soluções no conjunto dos inteiros (Zawaira A.; Hitchcock, 2009).

Em contrapartida, analisemos um segundo exemplo:

$$21x + 7y = 11. \tag{4.6}$$

Aqui, os coeficientes fornecidos são $a = 21$ e $b = 7$. Calculando o seu máximo divisor comum, obtemos $\text{mdc}(21, 7) = 7$. No entanto, o número 7 não divide exatamente o termo independente 11. Consequentemente, com base no critério de solubilidade previamente estabelecido, é possível afirmar com absoluto rigor que não existe qualquer par de números inteiros (x, y) capaz de satisfazer esta igualdade (Koshy, 2007).

4.2 Equações diofantinas não lineares

Em contraste com o caso linear, as equações diofantinas não lineares caracterizam-se pela presença de variáveis elevadas a potências estritamente superiores a um, ou pelo

produto entre diferentes variáveis. Devido à sua complexidade algébrica, não existe um algoritmo universal capaz de determinar a solubilidade de todas as equações diofantinas não lineares, o que torna o seu estudo um dos campos mais profundos e desafiantes da Teoria dos números (Koshy, 2007).

Na literatura matemática, as formas mais clássicas e historicamente investigadas de equações diofantinas não lineares assumem as expressões $x^2 + y^2 = z^2$, $x^n + y^n = z^n$ e $x^2 - Ny^2 = \pm 1$ (Koshy, 2007; Zawaira A.; Hitchcock, 2009).

O exemplo mais célebre de uma equação diofantina não linear é o que define os chamados ternos pitagóricos:

$$x^2 + y^2 = z^2. \tag{4.7}$$

As soluções inteiras e positivas desta equação correspondem, geometricamente, aos comprimentos dos lados de um triângulo retângulo (Zawaira A.; Hitchcock, 2009).

O conhecimento sobre estas soluções precede largamente o próprio Teorema de Pitágoras. Evidências arqueológicas, como uma famosa tábua de argila babilónica preservada na Universidade de Columbia, demonstram que civilizações antigas já dominavam as soluções desta equação há mais de 3500 anos. De igual modo, os antigos egípcios empregavam o terno pitagórico primitivo $(3, 4, 5)$ na topografia e na medição de terras, usando cordas com nós para garantir a formação de ângulos retos perfeitos após as inundações do rio Nilo (Zawaira A.; Hitchcock, 2009).

Outra classe fundamental de equações não lineares surge da generalização do problema pitagórico para potências superiores. O eminente matemático Pierre de Fermat dedicou especial atenção à equação:

$$x^4 - y^4 = z^2. \tag{4.8}$$

Fermat provou, através do seu método da descida infinita, que esta equação não admite soluções inteiras não triviais. A partir deste resultado, formulou um corolário de grande impacto: a área de um triângulo retângulo com lados de comprimento inteiro (um triângulo pitagórico) nunca pode ser igual a um quadrado perfeito inteiro (Zawaira A.; Hitchcock, 2009).

A generalização mais famosa, no entanto, é dada pela equação:

$$x^n + y^n = z^n \tag{4.9}$$

Conhecida no contexto do Último Teorema de Fermat, esta conjectura afirmava que, para qualquer número inteiro $n \geq 3$, não existem soluções inteiras positivas (x, y, z) que satisfaçam a igualdade (Koshy, 2007). Esta equação ditou o rumo da Teoria algébrica dos números moderna até ser integralmente demonstrada por Andrew Wiles no final do século XX.

Além das potências puras, outras formas não lineares continuam a motivar investigação matemática rigorosa. Um exemplo notável é a equação associada à Conjectura de Catalan:

$$x^m - y^n = 1. \tag{4.10}$$

onde se procuram soluções inteiras para variáveis e expoentes. Esta equação investiga a existência de potências perfeitas consecutivas, tendo sido provado que a única solução inteira não trivial ocorre para $3^2 - 2^3 = 1$ (Koshy, 2007).
As equações diofantinas representam um dos pilares mais antigos e fascinantes da Teoria dos Números. Diferentemente das equações lineares, cujas soluções podem ser completamente caracterizadas pelo Algoritmo de Euclides Estendido e pelo Teorema de Bachet-Bézout, as equações diofantinas não lineares impõem desafios analíticos e computacionais significativamente superiores.

Definição 4.2.1. *Uma equação diofantina não linear é uma equação da forma*

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{4.11}$$

onde f é um polinômio de grau $d > 1$ com coeficientes inteiros, para o qual buscam-se soluções inteiras ou racionais para as variáveis x_i.

O estudo dessas equações não se restringe apenas à busca por soluções, mas à determinação da existência, da finitude ou da infinitude do conjunto de soluções. O Décimo Problema de Hilbert, proposto em 1900, questionava a existência de um algoritmo geral para decidir se uma equação diofantina arbitrária possuia solução. Em 1970, o Teorema de Matiyasevich demonstrou que tal algoritmo é impossível, o que justifica a necessidade de métodos específicos para diferentes classes de equações não lineares.

4.3 Equações Diofantinas Quadráticas

As equações diofantinas de segundo grau, ou quadráticas, constituem a transição natural após o estudo das formas lineares. Elas envolvem termos de grau 2, como x^2, y^2 ou o produto xy. A análise dessas equações está intrinsecamente ligada à teoria das formas quadráticas e ao estudo das seções cônicas sobre corpos de números.

Uma das formas mais gerais para duas variáveis é dada por:

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{4.12}$$

onde os coeficientes pertencem a $\mathbb{Z}$. A classificação dessas equações depende crucialmente do discriminante $\Delta = B^2 - 4AC$. Se $\Delta < 0$, a equação representa uma elipse e possui um número finito de soluções. Se $\Delta > 0$ e não é um quadrado perfeito, a equação pode ter infinitas soluções, como ocorre na célebre Equação de Pell.

O estudo das formas quadráticas binárias e a representação de inteiros por essas formas (por exemplo, quais números podem ser escritos como soma de dois quadrados) são temas centrais nesta subseção.

Exemplo 4.3.1 (Ternos Pitagóricos)**.** *A equação $x^2 + y^2 = z^2$ é a mais clássica das equações quadráticas. Suas soluções inteiras positivas, conhecidas como ternos pitagóricos, podem ser parametrizadas pelas fórmulas de Euclides:*

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

onde $m > n > 0$ são inteiros coprimos de paridades distintas.

Exemplo 4.3.2 (Equação de Pell)**.** *A equação $x^2 - Dy^2 = 1$, onde D é um inteiro positivo não quadrado perfeito, possui infinitas soluções em $\mathbb{Z}$. A solução fundamental (x_1, y_1) pode ser encontrada através da expansão em frações contínuas de $\sqrt{D}$, e as demais soluções (x_n, y_n) derivam da relação:*

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n.$$

4.4 O Método da Descida Infinita

O **Método da Descida Infinita** é uma variante da prova por contradição, baseada no Princípio da Boa Ordenação dos números naturais. Desenvolvido formalmente por Pierre de Fermat, o método é utilizado para demonstrar que uma determinada propriedade não pode ser satisfeita por nenhum número inteiro positivo. A estrutura lógica do método consiste em:

1. Supor que existe uma solução no conjunto dos números inteiros positivos.
2. Mostrar que, a partir dessa solução, é possível construir uma nova solução que seja estritamente menor que a anterior.
3. Argumentar que a repetição desse processo criaria uma sequência infinita estritamente decrescente de inteiros positivos ($n_1 > n_2 > n_3 > \dots$).
4. Concluir que isso é um absurdo, pois qualquer subconjunto não vazio de números naturais deve possuir um elemento mínimo.

De acordo com Hardy e Wright (Hardy; Wright, 2008), este método é fundamental na Teoria dos números, sendo o precursor do princípio da indução matemática.

No que segue apresentamos duas aplicações clásicas do Método de Descida Infinita.

Exemplo 4.4.1. *Irracionalidade de $\sqrt{p}$, com p primo.*

Demonstração: (pode ser encontrada em (Hefez, A., 2006)) Seja p um primo qualquer. Suponha que $\sqrt{p}$ seja racional. Então, existem inteiros positivos a e b tais que $\sqrt{p} = a/b$.

$$a^2 = pb^2 \tag{4.13}$$

Isso implica que a^2 é múltiplo de p. Como p é um número primo, o Lema de Euclides garante que p também divide a. Seja $a = pa_1$. Substituindo:

$$(pa_1)^2 = pb^2 \implies p^2a_1^2 = pb^2 \implies b^2 = pa_1^2 \tag{4.14}$$

Dessa forma, b^2 também é múltiplo de p, logo p divide b ($b = pb_1$). Obtemos uma nova solução de inteiros positivos (a_1, b_1) tal que $a_1 < a$ (pois $a_1 = a/p$). Repetindo o processo, teríamos uma descida infinita de inteiros positivos, o que é impossível uma vez que o Príncipio da Boa Ordenação garante que entre zero e a só existe uma quantidade finita de inteiros. Portanto, $\sqrt{p}$ é irracional.

Exemplo 4.4.2. *A Equação* $x^3 + 3y^3 + 9z^3 = 0$
Considere a busca por soluções inteiras para $x^3 + 3y^3 + 9z^3 = 0$. *Claramente,* $(0, 0, 0)$ *é uma solução. Suponha que exista uma solução* (x, y, z) *com valores positivos:*

1. x^3 *deve ser múltiplo de* 3, *logo* $x = 3x_1$.
2. *Substituindo:* $27x_1^3 + 3y^3 + 9z^3 = 0 \implies 9x_1^3 + y^3 + 3z^3 = 0$.
3. *Agora,* y^3 *deve ser múltiplo de* 3, *logo* $y = 3y_1$.
4. *Substituindo:* $9x_1^3 + 27y_1^3 + 3z^3 = 0 \implies 3x_1^3 + 9y_1^3 + z^3 = 0$.
5. *Finalmente,* z^3 *deve ser múltiplo de* 3, *logo* $z = 3z_1$.

Isso resulta na equação original $x_1^3 + 3y_1^3 + 9z_1^3 = 0$, *onde* $0 < x_1 < x, 0 < y_1 < y, 0 < z_1 < z$. *Repetindo o processo, teríamos uma descida infinita de inteiros positivos, o que novamente é impossível. A descida infinita prova que a única solução possível é a trivial* $(0, 0, 0)$.

5 Aplicação: Questões olímpicas

5.1 Apoio a docentes

A inserção de estudantes em competições científicas, particularmente em olimpíadas de Matemática como a OBMEP e a OBM, demanda uma transição pedagógica do modelo tradicional para um foco intensivo em resolução de problemas. Sob a ótica de Pólya (1945), essa prática exige o desenvolvimento de um raciocínio heurístico. Para o docente, o acesso a um material de apoio didático robusto e estruturado não é apenas um facilitador, mas um pilar essencial para o sucesso dessa mediação. Tais recursos permitem que o professor explore tópicos de combinatória, teoria dos números e geometria plana com uma profundidade que o currículo básico muitas vezes negligencia por limitações de carga horária.

Mais do que apenas apresentar enunciados complexos, o material didático especializado oferece diferentes perspectivas de resolução, incentivando o pensamento lateral e a autonomia do aluno frente ao desconhecido. Ao fundamentar essa prática nas premissas de Pólya, o professor assume a função de instigar o estudante por meio de questionamentos, auxiliando-o nas etapas de compreender o problema e conceber um plano, em vez de simplesmente fornecer a resposta. Segundo (Nogueira; Gomes, 2014), a eficácia do treinamento olímpico está intrinsecamente ligada à capacidade do professor de atuar como um mentor, papel este que é fortalecido quando há subsídios teóricos e práticos claros à sua disposição. O material serve, portanto, como uma ponte entre a intuição heurística do estudante e o rigor formal necessário para os diversos níveis de competição.

Dessa forma, investir na produção e no acesso a esses conteúdos é fundamental para motivar tanto alunos iniciantes quanto medalhistas veteranos. Um bom guia didático permite que o professor organize o conhecimento de forma espiralada, garantindo que o desafio olímpico seja uma experiência de crescimento intelectual contínuo e uma ferramenta de democratização do saber matemático avançado.

5.2 Desafios e Potencialidades da Teoria dos Números Avançada no Treinamento Olímpico

A inserção de tópicos do ensino superior, como a Lei da Reciprocidade Quadrática e o estudo de equações diofantinas não lineares (quadráticas e cúbicas), representa um dos maiores desafios pedagógicos na preparação para olimpíadas de alto nível. O

principal obstáculo reside na transposição didática: é preciso converter o rigor formal e a abstração algébrica desses teoremas em ferramentas heurísticas de resolução de problemas, ampliando o arsenal estratégico do aluno, conforme defendido pela visão de Pólya (1945).

No caso das equações diofantinas de grau superior, como as equações de Pell ou curvas cúbicas simples, o conhecimento avançado atua em duas frentes. Primeiramente, como método direto de resolução através de algoritmos de descida infinita ou frações contínuas. Em segundo lugar, e de forma altamente estratégica na fase de *estabelecimento de um plano* (o segundo passo de Pólya), a Lei da Reciprocidade Quadrática funciona como um poderoso filtro de restrição de possibilidades. Ao analisar resíduos quadráticos, o competidor consegue eliminar vastas classes de candidatos a solução, transformando um problema aparentemente intratável em uma análise de poucos casos particulares. Assim, o domínio dessas técnicas não apenas fornece respostas, mas refina a capacidade analítica de restringir o domínio do problema, instrumentalizando o aluno a enfrentar questões rebuscadas de forma mais independente e criativa.

5.3 Exemplos Clássicos

A fim de consolidar a compreensão das ferramentas teóricas discutidas, esta seção elenca problemas basilares que ilustram a aplicação prática da Teoria dos Números em cenários desafiadores. Os exemplos a seguir foram selecionados por servirem como verdadeiros paradigmas metodológicos: eles não apenas demonstram o poder computacional da Lei da Reciprocidade Quadrática e das técnicas de resolução de equações diofantinas não lineares, mas também funcionam como modelos (ou *templates* heurísticos) para a abordagem de questões mais intrincadas frequentemente encontradas em competições de alto nível.

5.3.1 Aplicações da Lei da Reciprocidade Quadrática

O cálculo de resíduos quadráticos e a determinação de solubilidade de congruências são consideravelmente simplificados por meio da Lei da Reciprocidade Quadrática, cujos corolários clássicos permitem caracterizar divisores primos de formas quadráticas.

Exemplo 5.3.1. *O caráter quadrático do número 3.*
Um problema clássico consiste em determinar para quais primos ímpares p a congruência $x^2 \equiv 3 \pmod{p}$ possui solução. Pela Lei da Reciprocidade Quadrática, relaciona-se o símbolo de Legendre $\left(\frac{3}{p}\right)$ com $\left(\frac{p}{3}\right)$. Analisando os casos em que $p \equiv 1 \pmod{4}$ e $p \equiv 3 \pmod{4}$, conclui-se elegantemente que 3 é resíduo quadrático módulo p se, e somente

se, $p \equiv \pm 1 \pmod{12}$*. Esse tipo de raciocínio é a base para a classificação de resíduos para qualquer primo* q*.*

Exemplo 5.3.2. *Solubilidade de congruências específicas.*
Determinar se a equação $x^2 \equiv 17 \pmod{29}$ *possui solução inteira. Como 17 e 29 são primos ímpares e* $29 \equiv 1 \pmod{4}$*, a lei garante que* $\left(\frac{17}{29}\right) = \left(\frac{29}{17}\right)$*. Como* $29 \equiv 12 \pmod{17}$*, o problema se reduz a avaliar* $\left(\frac{12}{17}\right)$*, que por meio das propriedades multiplicativas do símbolo de Legendre e do Primeiro Suplemento, revela rapidamente se a equação original tem raízes, dispensando testes exaustivos.*

Exemplo 5.3.3. *Fatores primos de formas quadráticas.*
Demonstrar que todo divisor primo ímpar p *da forma* $x^2 - 2$ *satisfaz* $p \equiv \pm 1 \pmod{8}$*. Se* $p \mid (x^2 - 2)$*, então* $x^2 \equiv 2 \pmod{p}$*, o que significa que 2 é um resíduo quadrático módulo* p*. Pelo Segundo Suplemento da Lei da Reciprocidade Quadrática, sabe-se que* $\left(\frac{2}{p}\right) = 1$ *se, e somente se,* $p \equiv \pm 1 \pmod{8}$*. Esta aplicação é amplamente utilizada em provas de existência de infinitos primos de certas progressões aritméticas.*

5.3.2 Equações Diofantinas Não Lineares

Diferentemente das equações lineares, resolvidas pelo Algoritmo de Euclides, as equações diofantinas não lineares exigem ferramentas algébricas variadas, como uso de módulos convenientes e o método da descida infinita.

Exemplo 5.3.4. *Ternos Pitagóricos.*
A equação $x^2 + y^2 = z^2$ *é o exemplo primordial de equação diofantina não linear. Sua solução clássica envolve demonstrar que, para soluções primitivas (onde* $mdc(x, y, z) = 1$*), os valores podem ser representados por* $x = m^2 - n^2$*,* $y = 2mn$ *e* $z = m^2 + n^2$*, com* m *e* n *inteiros de paridades distintas e primos entre si. Esse problema ilustra a técnica fundamental de fatoração algébrica associada a argumentos de paridade.*

Exemplo 5.3.5. *A Equação de Pell.*
Dada pela forma $x^2 - dy^2 = 1$*, onde* d *é um inteiro positivo não quadrado perfeito. A importância deste exemplo reside no fato de que, uma vez encontrada a solução fundamental* (x_1, y_1) *(frequentemente via frações contínuas), existem infinitas soluções geradas pela relação recursiva associada a* $(x_1 + y_1\sqrt{d})^n$*. É uma equação recorrente em problemas que exigem a demonstração de infinitude de soluções para arranjos combinatórios ou geométricos.*

Exemplo 5.3.6. *O Método da Descida Infinita de Fermat.*
Provar que a equação $x^2 + y^2 = 3z^2$ não possui soluções inteiras não triviais. O argumento clássico analisa a equação módulo 3. Como os resíduos quadráticos módulo 3 são apenas 0 e 1, a soma $x^2 + y^2$ só pode ser múltipla de 3 se ambos x e y forem múltiplos de 3. Isso implica que z também deve ser múltiplo de 3, permitindo dividir a equação por 9. Esse processo iterativo cria uma sequência estritamente decrescente de inteiros positivos, o que é impossível, provando assim que a única solução é a trivial $(0, 0, 0)$.

5.4 Questões Olímpicas

A evolução das olimpíadas de matemática no mundo remonta ao final do século XIX, tendo como marco inicial a Competição Eötvös na Hungria, em 1894. Como destacam (Barbeau; Taylor, 2009), o objetivo primordial dessas iniciativas era identificar jovens talentos e estimular o raciocínio lógico em oposição à mera memorização de fórmulas. Contudo, o movimento ganhou escala global com a criação da Olimpíada Internacional de Matemática (IMO) em 1959, na Romênia, contando inicialmente com apenas sete países do bloco soviético. Ao longo das décadas, a competição expandiu-se para mais de cem nações, tornando-se o padrão ouro de excelência acadêmica pré-universitária e fomentando a criação de competições regionais e continentais que hoje compõem uma vasta rede de intercâmbio científico.

No Brasil, o desenvolvimento das olimpíadas matemáticas teve início institucional em 1979, com a criação da Olimpíada Brasileira de Matemática (OBM) pela Sociedade Brasileira de Matemática (SBM). Inicialmente voltada para um público restrito, a cultura olímpica no país sofreu uma transformação radical em 2005 com a criação da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Esse projeto de massificação tornou-se uma das maiores competições do gênero no mundo, atingindo milhões de estudantes anualmente e revelando talentos em regiões remotas do país. Graças a essa base sólida, o Brasil consolidou-se como uma potência olímpica, exemplo disto é o fato que sediou eventos de prestígio, como a IMO 2017 e o Congresso Internacional de Matemáticos em 2018.

A participação em olimpíadas de matemática transcende a mera disputa acadêmica, atuando como um poderoso catalisador para o desenvolvimento cognitivo e social dos estudantes. De acordo com Kenderov (Kenderov, 2006), esses certames são fundamentais para o ecossistema educacional, pois estimulam o pensamento não algorítmico, o raciocínio heurístico, a criatividade e a resiliência na resolução de problemas complexos habilidades altamente transferíveis para diversas áreas do conhecimento e pesquisa. No contexto nacional, Biondi, Machado e Menezes-Filho (Biondi; Machado; Menezes-

Filho, 2012) demonstram empiricamente o impacto positivo da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) no desempenho escolar geral dos alunos. O estudo evidencia que a simples presença e o engajamento de estudantes com essas provas e com os materiais de estudo oferecidos têm o potencial de elevar a proficiência acadêmica e incentivar a escolha futura por carreiras científicas e tecnológicas.

5.4.1 Questões sobre resíduos quadráticos e Lei da reciprocidade quadrática

I.) **Referência:** IMO Shortlist 1998, Problema N5.

Enunciado: Determine todos os inteiros positivos n para os quais existe um inteiro m tal que $2^n - 1$ divide $m^2 + 9$.

Resolução:
Para $n = 1$, temos $2^1 - 1 = 1$, que divide $m^2 + 9$ para qualquer inteiro m. Logo, $n = 1$ é solução.

Para $n > 1$, suponha por absurdo que n possua um divisor ímpar $k > 1$. Como $k \mid n$, segue da fatoração de polinômios que $2^k - 1 \mid 2^n - 1$. Por transitividade, $2^k - 1 \mid m^2 + 9$.

Analisando o comportamento de $2^k - 1$ módulo 3 e módulo 4 (para $k \geq 3$ ímpar):

- **Módulo 3:** $2^k \equiv (-1)^k \equiv -1 \pmod 3 \implies 2^k - 1 \equiv 1 \pmod 3$. Logo, $3 \nmid 2^k - 1$.
- **Módulo 4:** Como $k \geq 3$, $2^k \equiv 0 \pmod 4 \implies 2^k - 1 \equiv 3 \pmod 4$.

Como $2^k - 1 \equiv 3 \pmod 4$, este número deve possuir obrigatoriamente pelo menos um fator primo p tal que $p \equiv 3 \pmod 4$.

Sendo $p \mid 2^k - 1$, temos $p \mid m^2 + 9$, o que implica na congruência:

$$m^2 \equiv -9 \pmod p$$

Como já mostramos que $p \neq 3$ (e $p > 3$), o máximo divisor comum entre 9 e p é 1, permitindo-nos avaliar o símbolo de Legendre:

$$\left(\frac{-9}{p}\right) = \left(\frac{-1 \cdot 3^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)^2 = \left(\frac{-1}{p}\right)$$

Para que a congruência tenha solução, exige-se que $\left(\frac{-1}{p}\right) = 1$. No entanto, pela Primeira Lei Complementar da Reciprocidade Quadrática, para $p \equiv 3 \pmod 4$, temos:

$$\left(\frac{-1}{p}\right) = -1$$

Chegamos a uma contradição. Portanto, n não pode ter divisores ímpares maiores que 1, o que implica que n deve ser uma potência de 2, ou seja, $n = 2^s$, para algum $s \geq 0$.

Nota sobre a recíproca: Para $n = 2^s$, todo fator primo $p > 3$ de $2^{2^s} - 1$ satisfaz $p \equiv 1 \pmod 4$, garantindo que -9 seja resíduo quadrático módulo p. A existência do inteiro m é então formalmente garantida pela aplicação do Lema de Hensel seguido do Teorema Chinês dos Restos.

II.) **Referência:** Olimpíada Balcânica de Matemática (BMO) 1998, Problema 4.

Enunciado: Prove que a equação diofantina $y^2 = x^5 - 4$ não possui soluções conjunto dos números inteiros.

Resolução e Explicação: Para demonstrar que não há soluções, analisaremos a equação sob o módulo 11, explorando os resíduos quadráticos.

Primeiro, determinamos os resíduos quadráticos possíveis para $y^2 \pmod{11}$. Calculando os quadrados perfeitos modulo 11: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 5$, $5^2 \equiv 3 \pmod{11}$. Assim, $y^2 \pmod{11} \in \{0, 1, 3, 4, 5, 9\}$.

Agora, analisamos as possíveis congruências para $x^5 \pmod{11}$. Se $11 \mid x$, então $x^5 \equiv 0 \pmod{11}$. Se $11 \nmid x$, pelo Pequeno Teorema de Fermat, $x^{10} \equiv 1 \pmod{11}$. Isso implica que $(x^5)^2 \equiv 1 \pmod{11}$, logo $x^5 \equiv \pm 1 \pmod{11}$ (ou seja, 1 ou 10). Portanto, os valores possíveis para $x^5 \pmod{11}$ são $\{0, 1, 10\}$.

Subtraindo 4, obtemos as possibilidades para $x^5 - 4 \pmod{11}$:

- Se $x^5 \equiv 0 \implies x^5 - 4 \equiv -4 \equiv 7 \pmod{11}$
- Se $x^5 \equiv 1 \implies x^5 - 4 \equiv -3 \equiv 8 \pmod{11}$
- Se $x^5 \equiv 10 \implies x^5 - 4 \equiv 6 \pmod{11}$

Os únicos valores possíveis para a expressão do lado direito $x^5 - 4 \pmod{11}$ formam o conjunto $\{6, 7, 8\}$.

Comparando com os resíduos quadráticos válidos para o lado esquerdo y^2 ($\{0, 1, 3, 4, 5, 9\}$), notamos que a interseção é vazia. Logo, a igualdade nunca ocorrerá módulo 11, o que prova de forma elegante que a equação original não tem solução nos números inteiros.

III.) **Referência:** Olimpíada Internacional de Matemática (IMO) 1996, Problema 4.

Enunciado: Os inteiros positivos a e b são tais que os números $15a + 16b$ e $16a - 15b$ são ambos quadrados perfeitos. Encontre o menor valor possível que pode ser assumido pelo menor desses dois quadrados.

Resolução : Sejam $15a + 16b = x^2$ e $16a - 15b = y^2$, com $x, y > 0$. Queremos encontrar o menor valor para $\min(x^2, y^2)$.

Multiplicando a primeira equação por 15 e a segunda por 16, e depois somando as duas:

$$15(15a + 16b) + 16(16a - 15b) = 15x^2 + 16y^2$$

$$225a + 240b + 256a - 240b = 15x^2 + 16y^2 \implies 481a = 15x^2 + 16y^2$$

Fatorando 481, obtemos $481 = 13 \times 37$. Logo, a expressão $15x^2 + 16y^2$ deve ser múltipla de 13 e de 37.

Analisando módulo 13:

$$\begin{aligned} 15x^2 + 16y^2 \equiv 0 \pmod{13} &\implies 2x^2 + 3y^2 \equiv 0 \pmod{13} \\ &\implies 2x^2 \equiv -3y^2 \pmod{13}. \end{aligned}$$

Multiplicando ambos os lados por 7 (o inverso de 2 (mod 13)):

$$x^2 \equiv -21y^2 \equiv 5y^2 \pmod{13}$$

Avaliamos o símbolo de Legendre $\left(\frac{5}{13}\right)$. Pela Reciprocidade Quadrática:

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$$

Como 5 não é um resíduo quadrático módulo 13, a única forma da congruência $x^2 \equiv 5y^2 \pmod{13}$ ser verdadeira é se $y \equiv 0 \pmod{13}$. Consequentemente, $13 \mid y$ e $13 \mid x$.

Analisando módulo 37:

$$15x^2 + 16y^2 \equiv 0 \pmod{37} \implies 15x^2 \equiv -16y^2 \pmod{37}$$

Multiplicando por 5:

$$75x^2 \equiv -80y^2 \pmod{37} \implies x^2 \equiv -6y^2 \pmod{37}$$

Avaliamos o símbolo de Legendre $\left(\frac{-6}{37}\right)$:

$$\left(\frac{-6}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)\left(\frac{3}{37}\right)$$

Sabe-se que $\left(\frac{-1}{37}\right) = 1$ (pois $37 \equiv 1 \pmod 4$), $\left(\frac{2}{37}\right) = -1$ (pois $37 \equiv 5 \pmod 8$), e $\left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$. Assim, $\left(\frac{-6}{37}\right) = 1 \times (-1) \times 1 = -1$. Como -6 também não é resíduo quadrático módulo 37, temos obrigatoriamente que $37 \mid y$ e $37 \mid x$.

Conclusão: Como 13 e 37 são coprimos, tanto x quanto y devem ser múltiplos de $13 \times 37 = 481$. Para minimizar os quadrados, tomamos o menor múltiplo positivo:

$x = y = 481$. Testando essa hipótese nas equações originais: $15a + 16b = 481^2$ e $16a - 15b = 481^2$. Igualando, temos $15a + 16b = 16a - 15b \implies a = 31b$. Substituindo na primeira: $15(31b) + 16b = 481b = 481^2 \implies b = 481$. Isso nos dá $a = 31 \times 481 = 14911$. Como encontramos valores inteiros e positivos para a e b, a hipótese é válida. O menor valor que pode ser assumido é $481^2 = 231361$.

5.4.2 Questões que envolvem equações diofantinas não lineares

Abaixo, apresentam-se seis exemplos de questões reais que utilizam o arcabouço das equações diofantinas não lineares:

I.) **IMO 1988 (Problema 6):** Sejam a e b inteiros positivos tais que $ab+1$ divide a^2+b^2. Mostre que $\frac{a^2+b^2}{ab+1}$ é o quadrado de um inteiro. (Utiliza a técnica de *Vieta Jumping* em uma equação quadrática).

Resolução : Suponha, por absurdo, que exista algum par de inteiros positivos (a, b) tal que:

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

onde k **não** é um quadrado perfeito. Mostraremos que essa hipótese nos joga em um processo de descida infinita, gerando uma contradição.

Podemos reescrever a relação acima como uma equação diofantina quadrática (não linear) nas variáveis a e b:

$$a^2 - kba + b^2 - k = 0 \tag{5.1}$$

Considere o conjunto S de todos os pares de inteiros positivos (x, y) que satisfazem a equação $x^2 - kxy + y^2 - k = 0$. Como assumimos que S não é vazio, pelo Princípio da Boa Ordenação, deve existir um par $(a, b) \in S$ que minimiza a soma $a + b$. Sem perda de generalidade, podemos assumir que $a \geq b > 0$.

Agora, fixamos o valor de b e olhamos para a equação (5.1) como uma equação polinomial de segundo grau na variável x:

$$x^2 - kbx + (b^2 - k) = 0$$

Sabemos que $x_1 = a$ é uma raiz inteira e positiva desta equação. Seja $x_2 = c$ a outra raiz. Pelas relações de Vieta para equações quadráticas, sabemos que:

$$a + c = kb \implies c = kb - a \tag{5.2}$$

$$a \cdot c = b^2 - k \implies c = \frac{b^2 - k}{a} \tag{5.3}$$

A partir da equação (5.2), dado que k, b e a são inteiros, conclui-se imediatamente que c também é um número inteiro. Vamos analisar a natureza de c:

a) **Caso 1:** $c = 0$
Se $c = 0$, ao substituirmos na equação (5.3), obtemos $0 = b^2 - k \implies k = b^2$. Isto implicaria que k é um quadrado perfeito, o que contradiz frontalmente nossa hipótese inicial. Portanto, $c \neq 0$.

b) **Caso 2:** $c < 0$
Se c for negativo, então $c \leq -1$. Como $b \geq 1$, temos que $bc \leq -1$, o que nos dá $bc + 1 \leq 0$.
Como c é uma raiz da nossa equação, ela satisfaz $c^2 - kbc + b^2 - k = 0$, que isolando os termos se torna:

$$c^2 + b^2 = k(bc + 1)$$

Como $c \neq 0$ e $b \neq 0$, o membro esquerdo $c^2 + b^2$ é estritamente positivo. No entanto, sabendo que $k > 0$ (já que $a^2 + b^2$ e $ab + 1$ são positivos) e que $bc + 1 \leq 0$, o membro direito $k(bc + 1)$ seria menor ou igual a zero. Uma contradição. Logo, c não pode ser negativo.

Dessa forma, a única alternativa restante é que c seja um inteiro estritamente positivo ($c > 0$). Logo, o par (c, b) também pertence ao conjunto S de soluções inteiras positivas.

Pela nossa escolha minimalista do par (a, b), a soma de seus elementos deve ser menor ou igual a de qualquer outra solução em S. Portanto:

$$a + b \leq c + b \implies a \leq c$$

No entanto, analisando a relação de Vieta (5.3) e lembrando que $a \geq b$, temos:

$$c = \frac{b^2 - k}{a} < \frac{b^2}{a} \leq \frac{a^2}{a} = a \implies c < a$$

Chegamos a uma contradição matemática inevitável: provamos simultaneamente que $a \leq c$ e que $c < a$.

Como a suposição de que k não é um quadrado perfeito quebra a consistência aritmética do problema, ela é necessariamente falsa.

Conclui-se, portanto, que $\frac{a^2+b^2}{ab+1} = k$ **deve ser o quadrado de um inteiro**. □

II.) **IMO 2006 (Problema 4):** Determine todos os pares de inteiros (x, y) que satisfazem a equação exponencial-quadrática $1 + 2^x + 2^{2x+1} = y^2$.

Resolução : Para resolver esta equação diofantina não linear, dividiremos a análise de acordo com a natureza do expoente inteiro x em três casos principais: $x < 0$, $x = 0$ e $x > 0$.

Caso 1: $x < 0$
Se $x \leq -1$, os termos 2^x e 2^{2x+1} tornam-se frações estritamente positivas.

- Se $x = -1$, temos: $1 + 2^{-1} + 2^{-1} = 1 + \frac{1}{2} + \frac{1}{2} = 2 = y^2$, o que não possui solução nos inteiros.
- Se $x \leq -2$, podemos limitar superiormente a expressão:

$$0 < 2^x + 2^{2x+1} \leq 2^{-2} + 2^{-3} = \frac{1}{4} + \frac{1}{8} = \frac{3}{8} < 1$$

  Portanto, o lado esquerdo da equação fica estritamente compreendido entre dois inteiros consecutivos:

$$1 < 1 + 2^x + 2^{2x+1} < 2$$

Como não existem quadrados perfeitos inteiros entre 1 e 2, concluímos que **não há soluções para** $x < 0$.

Caso 2: $x = 0$
Substituindo $x = 0$ diretamente na equação original, obtemos:

$$1 + 2^0 + 2^{2(0)+1} = y^2 \implies 1 + 1 + 2 = y^2 \implies y^2 = 4 \implies y = \pm 2$$

Isso nos fornece os dois primeiros pares de soluções: $(0, 2)$ **e** $(0, -2)$.

Caso 3: $x > 0$
Para $x \geq 1$, podemos isolar os termos potências de 2 e fatorar o lado direito da igualdade como uma diferença de quadrados:

$$2^x + 2^{2x+1} = y^2 - 1 \implies 2^x(1 + 2^{x+1}) = (y - 1)(y + 1)$$

Como o termo $2^x(1 + 2^{x+1})$ é par para qualquer $x \geq 1$, o produto $(y - 1)(y + 1)$ deve ser par, o que força y a ser um número ímpar.

Sendo y ímpar, os fatores $(y - 1)$ e $(y + 1)$ são inteiros pares consecutivos. O máximo divisor comum entre dois inteiros pares consecutivos é sempre 2:

$$\text{mdc}(y - 1, y + 1) = 2.$$

Como o produto desses fatores contém exatamente 2^x como sua potência máxima de 2, e a divisibilidade comum máxima entre eles é apenas um único fator 2, a potência 2^x deve ser distribuída de tal forma que um dos fatores absorva quase toda a potência de 2, restando ao outro fator apenas um único fator 2.

Sem perda de generalidade, assuma $y > 0$ (visto que se y é solução, $-y$ também será). Para $x \geq 2$, isso nos deixa com duas possibilidades de distribuição para os fatores:

Subcaso 3.1: $y - 1 = 2 \cdot A$ **e** $y + 1 = 2^{x-1} \cdot B$
onde A e B são inteiros ímpares positivos tais que $A \cdot B = 1 + 2^{x+1}$. Calculando a diferença entre as duas equações:

$$\begin{aligned}(y+1) - (y-1) = 2 \quad &\implies \quad 2^{x-1}B - 2A = 2 \implies 2^{x-2}B - A = 1 \\ &\implies \quad A = 2^{x-2}B - 1. \end{aligned} \tag{5.4}$$

Substituindo essa relação na identidade do produto $A \cdot B = 1 + 2^{x+1}$:

$$(2^{x-2}B - 1)B = 1 + 2^{x+1} \implies 2^{x-2}B^2 - B = 1 + 8 \cdot 2^{x-2}$$

Agrupando os termos em evidência com 2^{x-2}:

$$2^{x-2}(B^2 - 8) = B + 1. \tag{5.5}$$

Vamos testar os valores possíveis para o inteiro ímpar B:

- Se $B = 1$: $2^{x-2}(-7) = 2$, impossível pois o lado esquerdo seria negativo.
- Se $B = 3$: Substituindo na Equação (5.5), temos:

$$\begin{aligned}2^{x-2}(3^2 - 8) = 3 + 1 \quad &\implies \quad 2^{x-2}(1) = 4 \\ &\implies \quad 2^{x-2} = 2^2 \\ &\implies \quad x - 2 = 2 \\ &\implies \quad x = 4.\end{aligned}$$

  Se $x = 4$ e $B = 3$, encontramos $A = 2^2(3) - 1 = 11$. Assim, $y - 1 = 2 \cdot 11 = 22 \implies y = 23$.

- Se $B \geq 5$: Para $B \geq 5$, a inequação $B^2 - 8 > B + 1$ é sempre verdadeira. Como para $x \geq 2$ temos $2^{x-2} \geq 1$, o lado esquerdo de (5.5) crescerá muito mais rápido que o lado direito ($2^{x-2}(B^2 - 8) \geq B^2 - 8 > B + 1$), impossibilitando novas soluções inteiras.

Dessa forma, este subcaso nos dá a solução $x = 4$ e $y = \pm 23$.

Subcaso 3.2: $y - 1 = 2^{x-1} \cdot A$ **e** $y + 1 = 2 \cdot B$
De forma análoga, com $A \cdot B = 1 + 2^{x+1}$ sendo ímpares. Subtraindo as equações:

$$\begin{aligned}(y+1) - (y-1) = 2 \quad &\implies \quad 2B - 2^{x-1}A = 2 \\ &\implies \quad B - 2^{x-2}A = 1 \\ &\implies \quad B = 2^{x-2}A + 1.\end{aligned}$$

Substituindo em $A \cdot B = 1 + 2^{x+1}$:

$$A(2^{x-2}A + 1) = 1 + 8 \cdot 2^{x-2} \implies 2^{x-2}(A^2 - 8) = 1 - A$$

Como $A \geq 1$ é um inteiro positivo:

- Se $A = 1 \implies 2^{x-2}(-7) = 0$, impossível.
- Se $A = 3 \implies 2^{x-2}(1) = -2$, impossível.
- Se $A \geq 5 \implies A^2 - 8 > 0$, fazendo com que o lado esquerdo seja estritamente positivo, enquanto o lado direito $(1 - A)$ será estritamente negativo. Sem soluções aqui.

Por fim, resta checar manualmente se o valor limite $x = 1$ gera solução: $1 + 2^1 + 2^3 = 11 = y^2$ (não é quadrado perfeito).

Conclusão:
Todos os pares ordenados de inteiros (x, y) que satisfazem a equação dada são:

$$\boxed{(x, y) \in \{(0, 2), (0, -2), (4, 23), (4, -23)\}}$$

□

III.) **IMO 1981 (Problema 3):** Determine o valor máximo de $m^2 + n^2$, onde $1 \leq m, n \leq 1981$, satisfazendo a equação diofantina de quarto grau $(n^2 - mn - m^2)^2 = 1$.

Resolução :

A equação dada é de quarto grau, mas pode ser imediatamente simplificada extraindo-se a raiz quadrada de ambos os lados. Isso nos dá duas equações quadráticas não lineares:

$$n^2 - mn - m^2 = 1 \quad \text{ou} \quad n^2 - mn - m^2 = -1 \tag{5.6}$$

Podemos enxergar a relação (5.6) como uma equação do segundo grau na variável n:

$$n^2 - mn - (m^2 \pm 1) = 0$$

Aplicando a fórmula de Bhaskara para determinar n em função de m, obtemos:

$$n = \frac{m \pm \sqrt{m^2 - 4(1)(-(m^2 \pm 1))}}{2} = \frac{m \pm \sqrt{5m^2 \pm 4}}{2}$$

Para que n seja um número inteiro, é condição necessária e suficiente que o discriminante dentro da raiz seja um quadrado perfeito. Isto é, deve existir um inteiro k tal que:

$$5m^2 \pm 4 = k^2 \tag{5.7}$$

A equação (5.7) é uma forma clássica de equação do tipo Pell. Um teorema fundamental da teoria dos números (Teorema de Lucas) afirma que:

> *Um inteiro positivo m é um número de Fibonacci se, e somente se, $5m^2 + 4$ ou $5m^2 - 4$ for um quadrado perfeito.*

Portanto, m deve ser obrigatoriamente um termo da sequência de Fibonacci ($m = F_i$). Além disso, substituindo $m = F_i$ na expressão de n, as propriedades das identidades de Fibonacci (especificamente a Identidade de Cassini, $F_{i+1}F_{i-1} - F_i^2 = (-1)^i$) mostram que as únicas soluções inteiras positivas para o par (m, n) ocorrem quando m e n são números de Fibonacci consecutivos. Ou seja:

$$(m, n) = (F_i, F_{i+1}) \quad \text{ou} \quad (m, n) = (F_{i+1}, F_i)$$

Como o problema impõe a restrição de que $1 \leq m, n \leq 1981$, nosso objetivo se resume a encontrar o maior par de números de Fibonacci consecutivos que não ultrapassam o valor limite de 1981.

Vamos listar os termos da sequência de Fibonacci ($F_1 = 1, F_2 = 1, F_3 = 2, \dots$) até ultrapassar o limite estabelecido:

$$F_{10} = 55$$
$$F_{11} = 89$$
$$F_{12} = 144$$
$$F_{13} = 233$$
$$F_{14} = 377$$
$$F_{15} = 610$$
$$F_{16} = 987$$
$$F_{17} = 1597$$
$$F_{18} = 2584$$

Como $F_{18} = 2584 > 1981$, o maior número de Fibonacci permitido dentro do intervalo é $F_{17} = 1597$. O número de Fibonacci consecutivo a ele que respeita o intervalo inferior é $F_{16} = 987$.

Portanto, os pares que maximizam os valores das variáveis são $(m, n) = (987, 1597)$ ou $(m, n) = (1597, 987)$. Como a expressão que desejamos maximizar, $m^2 + n^2$, é simétrica, ambos os pares resultarão no mesmo valor máximo.

Calculando o valor máximo:

$$m^2 + n^2 = 987^2 + 1597^2$$

$$987^2 = 974.169$$

$$1597^2 = 2.550.409$$

$$m^2 + n^2 = 974.169 + 2.550.409 = 3.524.578$$

(Nota matemática: Pela identidade de Fibonacci, sabemos que $F_i^2 + F_{i+1}^2 = F_{2i+1}$. Logo, $F_{16}^2 + F_{17}^2 = F_{33} = 3.524.578$.)

Conclusão:
O valor máximo de $m^2 + n^2$ que satisfaz as condições do problema é:

$$\boxed{3.524.578}$$

□

IV.) **IMO 1998 (Problema 4):** Determine todos os pares de inteiros positivos (a, b) tais que ab^2+b+7 divide a^2b+a+b. (A análise recai sobre a equação $a^2b+a+b = k(ab^2 + b + 7)$).

Resolução :

Seja a relação de divisibilidade dada por:

$$ab^2 + b + 7 \mid a^2b + a + b$$

Para simplificar a expressão, multiplicamos o dividendo por b (o que preserva a divisibilidade, já que $b > 0$ e $ab^2 + b + 7 > b$):

$$ab^2 + b + 7 \mid b(a^2b + a + b) \implies ab^2 + b + 7 \mid a^2b^2 + ab + b^2$$

Subtraímos do dividendo o múltiplo $a(ab^2 + b + 7)$ do divisor para eliminar os termos em a^2:

$$(a^2b^2 + ab + b^2) - a(ab^2 + b + 7) = a^2b^2 + ab + b^2 - a^2b^2 - ab - 7a = b^2 - 7a$$

Assim, temos a condição fundamental:

$$ab^2 + b + 7 \mid b^2 - 7a$$

Analisamos agora os três casos possíveis para o valor de $b^2 - 7a$:

a) **Caso $b^2 - 7a = 0$:**
Temos $b^2 = 7a$. Como 7 é primo, b deve ser múltiplo de 7 ($b = 7k$ para $k \in \mathbb{Z}^+$). Substituindo: $(7k)^2 = 7a \implies 49k^2 = 7a \implies a = 7k^2$. Verificando na original, o quociente resulta em k, que é inteiro. Portanto, $(7k^2, 7k)$ é solução para todo $k \in \mathbb{Z}^+$.

b) **Caso $b^2 - 7a > 0$:**
Se o dividendo é positivo, ele deve ser maior ou igual ao divisor:

$$b^2 - 7a \geq ab^2 + b + 7$$

Rearranjando: $b^2 - b - 7 \geq a(b^2 + 7)$. Como $a \geq 1$, teríamos $b^2 - b - 7 \geq b^2 + 7 \implies -b - 7 \geq 7 \implies b \leq -14$, o que contradiz $b > 0$. Não há soluções aqui.

c) **Caso $b^2 - 7a < 0$:**
Seja $7a - b^2 > 0$. Pela propriedade da divisibilidade, o divisor deve ser menor ou igual ao valor absoluto do dividendo:

$$ab^2 + b + 7 \leq 7a - b^2 \implies b^2 + b + 7 \leq a(7 - b^2)$$

Para que o lado direito seja positivo, devemos ter $7 - b^2 > 0$, logo $b \in \{1, 2\}$.

- **Se $b = 1$:** $a + 8 \mid a^2 + a + 1$. Pela divisão polinomial: $a^2 + a + 1 = (a + 8)(a - 7) + 57$. Logo, $a + 8 \mid 57$. Como $a + 8 \geq 9$, as opções são $a + 8 = 19 \implies a = 11$ ou $a + 8 = 57 \implies a = 49$. De onde segue os pares de soluções: $(11, 1)$ e $(49, 1)$.
- **Se $b = 2$:** $4a+9 \mid 2a^2+a+2$. Multiplicando por 8: $4a+9 \mid 16a^2+8a+16$. Como $16a^2 + 8a + 16 = (4a + 9)(4a - 7) + 79$, temos $4a + 9 \mid 79$. Como 79 é primo e $4a + 9 \geq 13$, teríamos $4a + 9 = 79 \implies 4a = 70$ (sem solução inteira).

Conjunto Solução:

$$\{(11, 1), (49, 1)\} \cup \{(7k^2, 7k) : k \in \mathbb{Z}^+\}$$

A Utilidade das Equações Diofantinas:
A resolução deste problema demonstra como equações diofantinas (equações que buscam soluções inteiras) permitem converter problemas de divisibilidade em problemas de **limitantes geométricos e algébricos**. Ao usar a desigualdade entre divisor e dividendo, restringimos o espaço de busca infinito a um conjunto finito de casos testáveis, técnica essencial em criptografia, teoria dos números computacional e otimização de sistemas discretos.

V.) **USAMO 1986 (Problema 3):** Determine o menor inteiro $n > 1$ tal que a média quadrática dos primeiros n inteiros positivos seja um inteiro, resultando na equação de Pell: $\frac{(n+1)(2n+1)}{6} = k^2$.

Resolução:

A média quadrática (RMS) dos primeiros n inteiros é definida por:

$$\text{RMS} = \sqrt{\frac{1^2 + 2^2 + \cdots + n^2}{n}}$$

Utilizando a fórmula da soma dos quadrados dos primeiros n inteiros, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, a condição de que a RMS seja um inteiro k resulta na equação:

$$\frac{\frac{n(n+1)(2n+1)}{6}}{n} = k^2 \implies \frac{(n+1)(2n+1)}{6} = k^2$$

Expandindo a expressão e multiplicando por 6:

$$2n^2 + 3n + 1 = 6k^2$$

Para transformar esta equação em uma Equação de Pell padrão, multiplicamos ambos os lados por 8 para completar o quadrado no termo em n:

$$16n^2 + 24n + 8 = 48k^2$$

$$(4n+3)^2 - 9 + 8 = 48k^2 \implies (4n+3)^2 - 48k^2 = 1$$

Seja $x = 4n + 3$ e $y = k$. Temos a Equação de Pell:

$$x^2 - 48y^2 = 1$$

A solução fundamental para esta equação (com $y > 0$) pode ser encontrada por inspeção ou frações contínuas: Se $y = 1$, $x^2 - 48 = 1 \implies x^2 = 49 \implies x = 7$. Para $x = 7$: $4n + 3 = 7 \implies n = 1$. Contudo, o problema exige $n > 1$.

As soluções sucessivas (x_m, y_m) são geradas pela potência $(7 + \sqrt{48})^m$. A relação de recorrência para x é dada por $x_m = 14x_{m-1} - x_{m-2}$:

a) $x_1 = 7 \implies n = 1$

b) $x_2 = 14(7) - 1 = 97$. Verificamos se $x \equiv 3 \pmod 4$: $97 \div 4 = 24$ com resto 1. Não serve para n inteiro.

c) $x_3 = 14(97) - 7 = 1358 - 7 = 1351$. Verificamos se $x \equiv 3 \pmod 4$: $1351 = 4 \times 337 + 3$. O resto é 3.

Substituindo $x = 1351$ na definição de x:

$$4n + 3 = 1351 \implies 4n = 1348 \implies n = 337$$

Resultado: O menor inteiro é $n = 337$.

VI.) **Putnam 2001 (Problema A5):** Prove que existe um único par de inteiros positivos (a, n) que satisfaz a equação diofantina exponencial $a^{n+1} - (a + 1)^n = 2001$.

Resolução :

Primeiro, analisamos a equação para valores pequenos de n:

- Se $n = 1$: $a^2 - (a + 1) = 2001 \implies a^2 - a - 2002 = 0$. As raízes são $a = \frac{1 \pm \sqrt{1+8008}}{2} = \frac{1 \pm \sqrt{8009}}{2}$. Como 8009 não é um quadrado perfeito, não há solução inteira.
- Se $n = 2$: $a^3 - (a + 1)^2 = 2001 \implies a^3 - a^2 - 2a - 1 = 2001 \implies a^3 - a^2 - 2a - 2002 = 0$. Testando divisores de 2002, observamos que para $a = 13$: $13^3 - 13^2 - 2(13) = 2197 - 169 - 26 = 2002$. Logo, $(13, 2)$ é uma solução.

Para provar a unicidade, analisamos a equação via congruências: 1. Trabalhando módulo a: $-(1)^n \equiv 2001 \pmod{a} \implies -1 \equiv 2001 \pmod{a} \implies a \mid 2002$. 2. Trabalhando módulo $a + 1$: $a^{n+1} \equiv 2001 \pmod{a+1} \implies (-1)^{n+1} \equiv 2001 \pmod{a+1}$.

Caso 1: n é par.
Se n é par, $n+1$ é ímpar, então $-1 \equiv 2001 \pmod{a+1} \implies a+1 \mid 2002$. Como $\text{mdc}(a, a + 1) = 1$ e ambos dividem 2002, temos que $a(a + 1) \mid 2002$. Sabemos que $2002 = 2 \cdot 7 \cdot 11 \cdot 13$. O único produto de dois inteiros consecutivos que divide 2002 é $13 \times 14 = 182$ (pois $182 \times 11 = 2002$). Assim, $a = 13$ é o único candidato para n par. Como $a = 13, n = 2$ funciona, e a função $f(n) = 13^{n+1} - 14^n$ é estritamente crescente para $n \geq 2$, não há outro n par.

Caso 2: n é ímpar.
Se n é ímpar, $n+1$ é par, então $1 \equiv 2001 \pmod{a+1} \implies a+1 \mid 2000$. Também temos $a \mid 2002$. Se $n \geq 3$, e $a \geq 2$, o termo a^{n+1} cresce muito mais rápido que $(a+1)^n$. Para $a = 1$, teríamos $1 - 2^n = 2001$ (impossível). Para $a = 2$, $a+1 = 3$, mas $3 \nmid 2000$. Para $a = 3$, $a + 1 = 4$, e $4 \mid 2000$, mas $3^{n+1} - 4^n = 2001$ não possui soluções para n ímpar ≥ 3 (por exemplo, para $n = 3$, $81 - 64 = 17 \neq 2001$; para $n = 5$, $729 - 1024 < 0$). Uma análise de crescimento mostra que para $n \geq 3$, se

$a \leq 13$, a diferença é menor que 2001 ou negativa, e se $a \geq 14$, a diferença excede 2001 rapidamente.

Portanto, o único par é $(13, 2)$.

As resoluções precedentes, fundamentadas na aplicação da Lei da Reciprocidade Quadrática e no manejo de equações diofantinas não lineares, evidenciam a sofisticação exigida pela matemática de nível olímpico. Analisando esse percurso sob o prisma da heurística de George Pólya — cujas quatro etapas clássicas consistem em compreender o problema, conceber um plano, executá-lo e, por fim, realizar o retrospecto —, percebe-se que a atividade de resolução transcende a mera obtenção de uma resposta analítica.

Essa perspectiva de enriquecimento metodológico é corroborada pela própria essência da quarta etapa, momento em que o potencial formativo da questão finalmente se concretiza. Para o autor, a fase de revisão (ou retrospecto) é indispensável para o amadurecimento matemático:

> Mesmo os estudantes razoavelmente bons, quando resolvem o problema e escrevem cuidadosamente a solução, fecham o caderno e passam a procurar outra ocupação. Fazendo isso, perdem uma fase importante e instrutiva do trabalho. [...] reconsiderando e reexaminando o resultado e o caminho que conduziu a ele, poderiam consolidar o seu conhecimento e desenvolver a sua aptidão para resolver problemas. (Pólya, 1945)

É, fundamentalmente, na quarta etapa (a visão retrospectiva que ocorre a verdadeira expansão do arcabouço técnico. Ao revisar criticamente a eficácia dos argumentos aritméticos e das manipulações modulares recém-empregadas, o pesquisador ou estudante é capaz de abstrair as estruturas subjacentes a essas resoluções. Consequentemente, o uso de resíduos quadráticos e as substituições algébricas deixam de ser artifícios isolados e passam a integrar um repertório metodológico consolidado. Tal processo contínuo de internalização e reflexão incrementa substancialmente as ferramentas matemáticas disponíveis, aprimorando a intuição matemática e pavimentando o caminho para a elaboração de novos planos de ataque diante de futuros desafios.

6 Considerações Finais

A crescente difusão das olimpíadas de matemática em diversos níveis de ensino tem impulsionado não apenas o engajamento dos estudantes, mas também a sofisticação e a amplitude dos conteúdos programáticos exigidos nessas competições. Nesse cenário altamente dinâmico, a demanda por materiais didáticos e mídias de apoio de alta qualidade torna-se cada vez mais premente. Tais recursos consolidam-se como ferramentas de fundamental importância, servindo de subsídio tanto para os discentes, em sua jornada de preparação e aprofundamento, quanto para os docentes orientadores, que necessitam de bases sólidas para guiar seus alunos na construção de um raciocínio heurístico eficiente frente a problemas complexos.

Nesse contexto, o livreto pedagógico desenvolvido como produto deste trabalho propõe-se a preencher uma lacuna metodológica relevante. Ao estruturar uma abordagem que alia o rigor acadêmico à perspectiva de resolução de problemas de George Pólya, o material atua como uma ponte facilitadora para a transposição didática de temas avançados da Teoria dos Números — especificamente a *Lei da Reciprocidade Quadrática* e as *Equações Diofantinas Não Lineares* — para o ambiente de preparação olímpica. Para tanto, a obra articula a apresentação de exemplos clássicos, essenciais para a consolidação teórica, com a resolução detalhada de questões olímpicas de alto nível.

Mais do que apresentar caminhos mecânicos, a transição cuidadosa entre esses modelos fundamentais e os problemas de competição procurou evidenciar como a apropriação dessas ferramentas robustas enriquece a compreensão inicial do estudante, amplia suas possibilidades na concepção de um plano de ataque e simplifica a execução da solução. Além disso, fomenta-se o retrospecto crítico sobre as estratégias adotadas. Espera-se, portanto, que esta obra não apenas contribua para desmitificar esses conceitos matemáticos, mas também estimule a autonomia investigativa dos alunos e inspire a criação de novos materiais voltados ao ensino da matemática avançada.

Referências

ANDREESCU, Titu; ANDRICA, Dorin. **Number Theory: Structures, Examples, and Problems**. Boston, USA: Birkhäuser, 2009. Citado nas pp. 15, 16.

BARBEAU, Edward J.; TAYLOR, Peter J. **Challenging Mathematics in and Beyond the Classroom: The 16th ICMI Study**. New York: Springer, 2009. ISBN 978-0-387-09602-5. Citado na p. 69.

BIONDI, Aline L.; MACHADO, Danielle C.; MENEZES-FILHO, Naercio A. O impacto da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) no desempenho educacional. **Pesquisa e Planejamento Econômico**, IPEA, v. 42, n. 3, p. 411–443, 2012. Citado na p. 69.

BRASIL. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. **20ł OBMEP bate recorde histórico de escolas e municípios inscritos**. Abr. 2025. Disponível em: `https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2025/04/20a-obmep-bate-recorde-historico-de-escolas-e-municipios-inscritos`. Acesso em: 16 jul. 2026. Citado na p. 12.

COSTA JÚNIOR, Fernando Vieira. **Teoria dos Números e a Lei de Reciprocidade Quadrática**. [*S. l.: s. n.*], out 2014. Apresentação no III Colóquio de Matemática da Região Norte - Manaus. Universidade Federal de Alagoas – Campus de Arapiraca. Citado na p. 21.

DEHAENE, Stanislas. **The Number Sense: How the Mind Creates Mathematics**. Revised and Updated. Oxford, UK: Oxford University Press, 2011. Citado na p. 15.

EISENSTEIN, Ferdinand. Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste. **Journal für die reine und angewandte Mathematik**, v. 28, p. 246–248, 1844. Disponível em: `https://gdz.sub.uni-goettingen.de/id/PPN243919689_0028`. Citado na p. 52.

GAUSS, Carl Friedrich. **Disquisitiones Arithmeticae**. Leipzig: Gerh. Fleischer, 1801. Citado na p. 20.

HARDY, Godfrey Harold; WRIGHT, Edward Maitland. **An Introduction to the Theory of Numbers**. Oxford, UK: Oxford University Press, 2008. ISBN 978-0199219865. Citado nas pp. 52, 64.

HEFEZ, A. **Elementos de Aritmética**. Rio de Janeiro: Ed. SBM, 2006. Citado na p. 65.

HEFEZ, Abramo. **Aritmética**. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2016. (Coleção PROFMAT). ISBN 978-85-8337-181-6. Citado nas pp. 26, 27.

HEFEZ, Abramo. **Introdução à Teoria dos Números**. Rio de Janeiro, Brasil: Sociedade Brasileira de Matemática (SBM), 2002. v. 1. (Coleção PROFMAT). ISBN 978-85-85818-60-9. Citado nas pp. 22, 24.

ISNERI, Renan J.S.; VIEIRA, Vandenberg L.; SILVA, Maxwell A. Uma Prova da irracionalidade de $\sqrt[2n]{p}$. Em que p é primo, por meio da teoria dos resíduos quadráticos. **Revista Sergipana de Matemática e Educação Matemática**, ReviSeM, v. 9, n. 1, p. 22–37, 2024. Citado na p. 56.

KENDEROV, Petar S. Competitions and mathematics education. *In:* EUROPEAN MATHEMATICAL SOCIETY. PROCEEDINGS of the International Congress of Mathematicians. Madrid, Spain: [*s. n.*], 2006. v. 3, p. 1588–1598. Citado na p. 69.

KOSHY, Thomas. **Elementary Number Theory with Applications**. [*S. l.*]: 2ł edição. San Diego: Academic Press / Elsevier, 2007. Citado nas pp. 14, 15, 60–63.

NOGUEIRA, J. S.; GOMES, L. P. O impacto das Olimpíadas de Matemática na Formação Continuada de Professores e no Desenvolvimento de Talentos. **Revista de Educação Matemática e Científica**, São Paulo, v. 15, n. 3, p. 112–128, 2014. Citado na p. 66.

OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS. **A OBMEP em números**. 2026. Disponível em: `https://www.obmep.org.br/em-numeros.htm`. Acesso em: 17 jul. 2026. Citado na p. 13.

PÓLYA, George. **A arte de resolver problemas: um novo aspecto do método matemático**. Rio de Janeiro: Interciência, 1995. Citado na p. 19.

PÓLYA, George. **How to Solve It: A New Aspect of Mathematical Method**. Princeton, NJ: Princeton University Press, 1945. Citado nas pp. 6, 7, 14, 18, 83.

SANTOS, J. P. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2015. Citado nas pp. 21, 52.

SCHOENFELD, Alan H. **Mathematical Problem Solving**. Orlando, FL: Academic Press, 1985. Citado na p. 20.

TEIXEIRA, Daniela Mota. **Lei da Reciprocidade Quadrática e Problemas Olímpicos**. 2021. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) – Universidade Federal de Sergipe, Itabaiana, SE. Orientador: Samuel Brito Silva. Departamento de Matemática. Disponível em: `https://ri.ufs.br/bitstream/riufs/15777/2/DANIELA_MOTA_TEIXEIRA.pdf`. Citado nas pp. 55, 56.

ZAWAIRA A.; HITCHCOCK, G. **A Primer for Mathematics Competitions**. [*S. l.*]: Oxford: Oxford University Press, 2009. Citado nas pp. 14, 60–62.