UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

GUSTAVO OLIVEIRA LIMA JUNIOR

NÚMEROS INTEIROS, CONGRUÊNCIAS E SOMAS DE QUADRADOS

FORTALEZA

2013

GUSTAVO OLIVEIRA LIMA JUNIOR

NÚMEROS INTEIROS, CONGRUÊNCIAS E SOMAS DE QUADRADOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departemento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Robério Rogério

Coorientador: Prof. Dr. Marcelo Ferreira de Melo

FORTALEZA

2013

GUSTAVO OLIVEIRA LIMA JUNIOR

NÚMEROS INTEIROS, CONGRUÊNCIAS E SOMAS DE QUADRADOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 09 / 08 / 2013.

BANCA EXAMINADORA

Prof. Dr. José Robério Rogério (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará (UFC)

Prof. Dr. João Montenegro de Miranda
Universidade Estadual do Ceará (UECE)

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

S58a Lima Júnior, Gustavo Oliveira
Números inteiros, congruências e somas de quadrados / Gustavo Oliveira Lima Júnior. – 2013.
61 f. : il., enc. ; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2013.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Dr. José Robério Rogério.
Coorientação : Prof. Dr. Marcelo Ferreira de Melo.

1. Números inteiros. 2. Matemática – Ensino médio. 3. Axiomas. I. Título.

CDD 510

Dedico este Trabalho de Conclusão de Curso a todos os "amigos", encarnados ou espirituais que me suportam a convivência e ainda me inspiram na busca amorosa do conhecimento.

AGRADECIMENTOS

A Deus, O Incognoscível, Aquele que é só amor, por me permitir existir em condições de completar mais essa tarefa.

À espiritualidade superior que gerencia nossos passos com justiça.

Aos amigos “Reginaldo”, “Nico”, “Luís Carlos”, “Sr. Gustavo”, “D. Rita”, “Nicolas”, “Gabriel”, “Carla”, “Bárbara”, “Helena”, “Ana”, “Beatriz”, “Toinha”, “Jurema”, “Kelly” e “Joana D’arc” que transformam meus desânimos em esperanças.

A todos os professores exemplares do núcleo PROFMAT-UFC que, por suas solicitudes, promoveram nosso melhor aprendizado.

Ao professor José Robério Rogério que pacientemente me conduziu desde o início com suas excelentes sugestões, entremeadas com momentos de conversas e orientações sobre a postura ética que devemos tomar frente às adversidades na vida.

Aos professores José Othon Dantas Lopes e João Montenegro de Miranda pela atenção dispensada a todos nós, bem como análises e recomendações apropriadas nesse trabalho.

Aos professores Elon Lages Lima, Eduardo Wagner, Paulo Cezar Pinto Carvalho, Augusto César Morgado (in memorian) entre outros visionários que gestaram o projeto do curso PROFMAT baseados em suas experiências no PAPMEM desde o ano 2001.

Aos amigos Maria Batista de Lima e João José de Lima por toda a ajuda e atenção dispensadas a mim durante esse tempo.

Ao grupo gestor da escola estadual Danísio Dalton da Rocha Corrêa na cidade de Barreira que durante os anos $2011 - 2012$ me destinou algum tempo livre para estudos.

À CAPES cujo aporte financeiro foi fundamental para os gastos necessários.

À minha família que tolerou pacientemente meu afastamento por tantos dias durante a execução desse trabalho.

Ao Mestre Jesus por sua dedicação a todos “aqueles”que um dia foram anjos.

RESUMO

O presente trabalho propõe uma forma de apresentação aos alunos do ensino básico alguns conceitos associados ao conjunto dos números inteiros tais como, divisibilidade, MDC, MMC, congruências e somas de quadrados de uma maneira mais pragmática e menos abstrata. Apresentando-os através de formas visuais ou de problemas contextualizados com nossa realidade física mais imediata, favorecendo o melhor entendimento dos axiomas, operações e propriedades por aqueles alunos como também novos métodos de conduta para os professores a fim de que suas tarefas nos processos ensino-aprendizagem se tornem mais fáceis.

Palavras-chave: Números inteiros. Matemática - Ensino médio. Axiomas.

ABSTRACT

This paper proposes a way of presenting to primary pupils some concepts associated with the set of integers such as divisibility, GCD, LCM, congruences and sums of squares in a more pragmatic and less abstract way. Presenting them through visual forms or contextualized problems with our physical reality more immediate, favoring a better understanding of the axioms, operations and properties for those students as well as new methods of conduct for teachers so that their work processes teaching become easier.

Keywords: Integer numbers. Mathematics - High school. Axioms.

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Conjunto dos números inteiros
$>$	Sinal de desigualdade: maior do que
$\geqslant$	Sinal de desigualdade: maior do que ou igual a
$<$	Sinal de desigualdade: menor do que
$\leqslant$	Sinal de desigualdade: menor do que ou igual a
$\|a\|$	Módulo de um número real a
$\mid$	Sinal de divisibilidade exata
$\nmid$	Sinal da não divisibilidade exata
$\neq$	Sinal da não igualdade entre dois números
$\in$	Símbolo de pertinência entre elemento e conjunto
$\notin$	Símbolo de não pertinência entre elemento e conjunto
$\mathbf{A} - \mathbf{B}$	Diferença entre dois conjuntos
$\frac{a}{b}$	Quociente da divisão entre os números a e b
(a, b)	Máximo divisor comum dos inteiros a e b
$[a, b]$	Mínimo múltiplo comum dos inteiros a e b
$\equiv$	Relação de congruência
$\not\equiv$	Relação de não congruência
$f : A \to B$	Função entre os conjuntos A e B
$f \circ g$	Composição das funções f e g
$\overline{x}$	Inverso multiplicativo da classe de equivalência x

LISTA DE SIGLAS

CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
IMPA	Instituto Nacional de Matemática Pura e Aplicada
MDC	Máximo Divisor Comum
MMC	Mínimo Múltiplo Comum
OBM	Olimpíada Brasileira de Matemática
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
PAPMEM	Programa de Aperfeiçoamento de Professores do Ensino Médio
PROFMAT	Mestrado Profissional em Matemática
RPM	Revista do Professor de Matemática
SBM	Sociedade Brasileira de Matemática

SUMÁRIO

1 INTRODUÇÃO

É fato indiscutível que perpassa os limites das análises gerais sociológicas que a educação brasileira vem apresentando resultados inadequados de proficiência em quase todas as avaliações sérias de verificação dos níveis de aprendizagem em Matemática no ensino básico e que um menor rendimento acontece exatamente naquelas regiões provincianas mais afastadas dos centros culturais que não recebem o investimento e atenção adequados. Essa percepção vem se tornando cada vez mais presente nos dias atuais em virtude da rapidez com que as informações circulam hoje em nossa sociedade. Sobre essa má formação, especificamente dos alunos que chegam ao ensino médio, somam-se problemas que envolvem outras esferas do comportamento humano, passando não raras vezes pelas responsabilidades civis e criminais, por exemplo, o consumo de drogas ilícitas, o aumento da violência no âmbito escolar e as graves consequências subjacentes. O enfrentamento de tantas questões de naturezas tão variadas requer bem mais que adequação dos resultados estatísticos, e também passa por tomadas de decisões fortes na condução e re-elaboração das regras que regem os processos ensino-aprendizagem, com um maior amparo e proteção ao aluno, subsidiando meios de aperfeiçoamento do corpo docente com aprofundamento em seu conhecimento técnico e valorização salarial de sua carreira. O não enfrentamento dessas questões contribui, em última análise, para a eterna tipificação do conhecimento produzido em nossos ambientes escolares como inócuos, ineficientes e desvinculados do bom senso e da realidade.

Entre tantas ações a serem postas em prática para a reversão da realidade descrita acima, situam-se novos modos de apresentação dos conhecimentos, como tentativa de readaptação dos nossos esforços em tornar mais atrativo para uma ampla classe de jovens, dos assuntos que naturalmente devem fazer parte em suas formações básicas nos ensinos fundamental e médio.

Com a escolha de trabalhar o tema dos números inteiros este trabalho propõe algumas sugestões mínimas de posturas a serem adotadas em nosso posicionamento frente à nossa

plateia de interesse, desde uma forma mais concreta de apresentação das propriedades numéricas, passando por certa forma mais lógica e rigorosa no encadeamento das ideias, até o desenvolvimento, quando possível, de trabalhos próprios para alunos mais talentosos em Matemática. Especificamente, a introdução das congruências serve ao propósito de tentar incentivar esses alunos que possuam gosto pelo aprendizado para uma gama maior e mais adequada de assuntos do que somente aqueles normalmente tratados nos livro-textos. Nesses, ainda temos que certas escolhas de alguns temas e o modo como se faz isso não parece ser algumas vezes o mais adequado. Como exemplo mais evidente, temos o processo de determinação do máximo divisor comum entre dois inteiros positivos. Costuma-se quase sempre incentivar os alunos a utilizar o processo de fatoração conjunta daqueles números, apesar da beleza e simplicidade do método das divisões sucessivas de Euclides que, de tão eficiente, ainda é utilizado séculos após sua descoberta, como bem indica [6]. Ao incentivo daquele gosto pela Matemática devem ser acrescentados processos lógicos, precisos e eficientes que, por si só, evidenciam a beleza do aprendizado nessa matéria fascinante.

O modo específico de construção desse trabalho, que baseia-se por introduzir alguns dos assuntos com problemas que aguçam a curiosidade e nos desafiam a apresentar respostas simples através da procura lógica metódica ou até métodos heurísticos, tenta traduzir parte de uma generalidade de atuação que qualquer professor, pode adotar em suas mais variadas gradações de exigências e níveis de dificuldades em sua prática. Aqui se inserem desde tentativas simples de conexão das regras axiomáticas com o dia a dia da maioria dos alunos, valorização de suas iniciativas pessoais com estímulos em suas atividades de aprendizagem até o incentivo daqueles outros, cuja jovialidade e curiosidade já assumem o papel principal na condução de suas vidas escolares, com aprofundamentos substanciais em vários tópicos mais específicos de Matemática.

2 CONJUNTO DOS NÚMEROS INTEIROS

2.1 Introdução aos Inteiros e Contagem

- Tales brinca de arrumar bolinhas em um arranjo retangular de maneira que fique em cada fila a mesma quantidade e o mesmo aconteça com as colunas, sem sobrar bolinha alguma. Mileto também faz o mesmo separadamente. Eles podem construir livremente suas figuras e dispõem de 660 e 630 bolinhas respectivamente. Dentre os retângulos que ambas as crianças podem obter com a mesma quantidade de colunas, qual é a quantidade máxima de colunas observada ?

O exemplo acima, embora trabalhe com grandezas discretas positivas, serve como estímulo para a introdução da Matemática com números inteiros especialmente nos primeiros meses de trabalho no ensino médio pois fornece visualizações quase concretas das operações básicas envolvendo esses números como também mostra, de maneira muito simples, os fundamentos que existem por trás das propriedades operacionais.

Contas, pedras, traços num osso, parecem ser os primeiros elementos nas manifestações da Matemática como modelagem da realidade em nossa evolução cultural. Até podemos ousar dizer que a Matemática das contagens discretas é a base de nosso desenvolvimento tecnológico, pois é o primeiro passo na sistematização, armazenamento e transferências de informações entre as gerações que se sucedem em nossa sociedade.

Sem querer extrapolar nossa intenção básica, nos concentraremos de volta aos nossos dois personagens gregos e suas bolinhas em arranjos retangulares para mostrar que as operações básicas da adição, multiplicação e suas propriedades operacionais podem ser intuitivamente melhor compreendidas com a utilização de simples artifícios.

As propriedades da operação de adição entre dois inteiros positivos tornam-se óbvias quando imaginamos a reunião de duas coleções distintas dessas bolinhas. Sendo que a

soma é maior do que suas partes exceto se alguma das partes não contiver bola alguma. As propriedades comutativa e associativa são claras quando se percebe que a mudança na ordem de união das partes não altera o resultado final. Se adicionarmos a um conjunto de bolas outro sem elementos, isso não altera a quantidade daquele primeiro, e que para torná-lo sem elemento algum basta quitar uma dívida (associação razoável para números negativos) com a mesma quantidade de elementos.

A multiplicação de dois inteiros é definida como a repetição da adição de uma mesma quantidade, por exemplo, $5 \cdot 4 = 5 + 5 + 5 + 5$ ou também $4 + 4 + 4 + 4 + 4$. Usando a disposição retangular descrita no exemplo inicial podemos imaginar o enfileiramento de quatro colunas com cinco bolas cada ou o contrário. De imediato percebemos a validade da propriedade comutativa da multiplicação olhando para esse arranjo retangular sob essas duas perspectivas. Para a propriedade associativa é necessário requerer uma terceira direção de distribuição das bolas, arranjando-as na forma de um bloco retangular com vários níveis em que as três perspectivas básicas de visualização para a base do bloco não alteram a quantidade de bolas que formam o conjunto. Multiplicar por "um" significa um retângulo de uma só linha, que possui uma quantidade de bolas igual à quantidade de colunas, enquanto que qualquer retângulo sem linhas não pode conter bola alguma, sugerindo o resultado da multiplicação por zero. A propriedade distributiva é bem percebida quando dividimos o arranjo retangular em duas regiões através de uma linha divisória paralela a um de seus lados, mostrando que a quantidade total de bolas é igual às duas quantidades em que o conjunto foi separado. Por fim, é óbvio que se uma disposição retangular possui zero bolas, ela possuirá zero linhas ou zero colunas.

Essa apresentação meio divertida auxilia na assimilação das propriedades básicas operacionais dos inteiros, vistas a seguir como axiomas. Tentações à parte, é bom ter prudência nas exemplificações para não exagerá-las ou correr o risco e aceitar a premissa falsa de achar que qualquer assunto envolvendo Matemática pode ser contextualizado. Mas é saudável utilizar sempre que possível um ponto de vista da aplicabilidade real ou pelo menos sensata nas apresentações dos assuntos. Para uma visão mais detalhada sobre tais problemas veja [7].

Ao avançar sobre os conceitos de divisores de um número inteiro positivo N podemos associar uma pergunta equivalente:

De quantos modos podemos dispor, sem sobras, N bolas em arranjos retangulares?

As respostas distintas mostram as quantidades de linhas e colunas possíveis, que são os

divisores procurados. Na prática de sala de aula, ao atingir esse ponto, algum aluno mais curioso ousa propor uma reformulação do problema inicial: “vamos tentar achar um inteiro que seja o maior divisor simultâneo de 660 e 630.”
Ao procurarmos meios de fazer isso seremos apresentados aos primórdios de desenvolvimento e sistematização lógico do nosso conhecimento matemático através de uma viagem desde 2300 anos atrás, cuja importância não é menor que seu legado visto que parte daquela matemática grega ainda é utilizada, com as devidas adaptações, até hoje em dia.

Essa pequena introdução de tentar adaptar as regras operacionais dos inteiros positivos para um contexto mais visual e prático de apresentação é usualmente uma chamada aos alunos mais reticentes para melhor apreciar a beleza e os padrões na Matemática e talvez começarem a desenvolver aquele sentimento meio raro hoje em dia de contentamento e prazer em suas descobertas individuais.

2.2 Definição Axiomática

Não são poucos os alunos que ficam curiosos sobre como resolver problemas dos tipos seguintes:

Exemplo 2.2.1. *Podemos cobrir um tabuleiro tipo xadrez de* 5 *linhas e* 5 *colunas com peças de dominós que cobrem exatamente duas casas do tabuleiro cada uma?*

Exemplo 2.2.2. *Todas as peças de um conjunto de dominós são postas em fila tal que os valores descritos nas extremidades de peças adjacentes combinam. Em uma das extremidades da fila aparece o número* 6*, qual número aparecerá na outra?*

Exemplo 2.2.3. *Podemos cobrir um tabuleiro de xadrez de* 8 *linhas e* 8 *colunas com peças de dominós que cobrem exatamente* 2 *casas do tabuleiro cada uma de forma que as casas inferior direita e superior esquerda do tabuleiro fiquem descobertas?*

Exemplo 2.2.4. *João comprou uma agenda com* 96 *folhas numeradas de* 1 *a* 192*. Pedro, seu irmão, destacou* 25 *páginas escolhidas de maneira aleatória dessa agenda e adicionou os* 50 *números obtidos. É possível que Pedro obtenha* 2014 *como resultado dessa adição?*

Esses e muitos outros exemplos interessantes podem ser encontrados em [3]. Apesar de muito instigantes, para respondê-los não necessitamos de aprofundamento significativo em teorias matemáticas. Bastam conceitos bem simples, presentes já nos primórdios dos sistemas de contagem. Começaremos agora pelo mais básico.

O conjunto dos números inteiros, representado por

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

consta dos números naturais, dos seus opostos mais o zero. Utilizaremos algumas propriedades desses elementos para construir a teoria necessária ao nosso estudo.

Tentaremos minimizar nossa apresentação no sentido de torná-la menos prolixa mas não tão concisa a ponto de haver lacunas de entendimento, por isso adotaremos o ponto de vista axiomático, em que elegemos algumas sentenças não demonstradas como verdadeiras e, a partir daí, construiremos o encadeamento das ideias subsequentes.

Axioma 2.2.1. *Vamos supor conhecidas as operações binárias em* $\mathbb{Z}$ *chamadas de* adição*, e* multiplicação *que associam a cada par de números* $(a, b) \in \mathbb{Z}^2$ *respectivamente sua soma*

$a + b$ e produto $a \cdot b$.
Essas operações satisfazem as propriedades abaixo:

1. *A adição é comutativa.*
   Para todos $a, b \in \mathbb{Z}$ tem-se $a + b = b + a$

2. *A adição é associativa.*
   Para todos $a, b, c \in \mathbb{Z}$ tem-se $a + (b + c) = (a + b) + c$

3. *Existência do elemento neutro da adição.*
   Existe o elemento zero*, designado por* 0 *tal que para todo $a \in \mathbb{Z}$ tem-se $a + 0 = 0 + a = a$*

4. *Existência do elemento simétrico aditivo.*
   Para todo $a \in \mathbb{Z}$, existe seu simétrico aditivo designado por $-a$ tal que $a + (-a) = (-a) + a = 0$

5. *A multiplicação é comutativa.*
   Para todos $a, b \in \mathbb{Z}$ tem-se $a \cdot b = b \cdot a$

6. *A multiplicação é associativa.*
   Para todos $a, b, c \in \mathbb{Z}$ tem-se $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

7. *Existência do elemento neutro da multiplicação.*
   Existe o elemento um *designado por* 1 *, diferente de* zero *tal que para todo $a \in \mathbb{Z}$ tem-se que $a \cdot 1 = 1 \cdot a = a$*

8. *Distributividade da multiplicação em relação à adição.*
   Para todos $a, b, c \in \mathbb{Z}$ tem-se $a(b + c) = a \cdot b + a \cdot c$ e $(a + b)c = a \cdot c + b \cdot c$

9. *Não existência de divisores do zero.*
   Para todos $a, b \in \mathbb{Z}$, tais que $a \cdot b = 0$ tem-se $a = 0$ ou $b = 0$.

O conjunto $\mathbb{Z}$ com as operações de adição e multiplicação satisfazendo os axiomas listados acima recebe o nome de *Domínio de Integridade*. É sobre essa estrutura que desenvolveremos nosso estudo, enfatizando, por comodidade, a utilização dos inteiros positivos devido a sua melhor associação com os processos de quantificação e contagem na vida cotidiana de nossos alunos do ensino básico, o que não impede, pela estrutura simétrica de $\mathbb{Z}$, que tal ênfase também possa ser feita nos números negativos.

Utilizaremos sistematicamente algumas definições como também propriedades de $\mathbb{Z}$ amplamente conhecidas que podem ser provadas a partir dos axiomas anteriores, tais como as leis de corte, as regras de sinais da multiplicação, o anulamento no produto por zero, as monotonicidades das relações de ordem, etc. As demonstrações em $\mathbb{N}$ de algumas dessas propriedades podem ser vistas em [6]. Também adotaremos como axiomas o *Princípio de Indução Finita*, e o *Algoritmo da Divisão de Euclides*.

Axioma 2.2.2 (Indução - 1ª forma)**.** *Suponhamos que seja dada uma afirmação $P(n)$ dependendo de $n \in \mathbb{N}$ tal que*

- *$P(a)$ é verdadeira*
- *para $k \in \mathbb{N}$, $P(k+1)$ é verdadeira sempre que $P(k)$ for verdadeira*

Então, $P(n)$ é verdadeira para todo natural $n \geqslant a$.

Proposição 2.2.1 (Princípio da Boa Ordenação)**.** *Todo conjunto não vazio* **S** *de inteiros positivos possui um menor elemento.*

Demonstração. Definamos o conjunto $I_n = \{p \in \mathbb{N}; 1 \leqslant p \leqslant n\}$, consideremos o conjunto X de inteiros positivos, formado pelos números n tais que $I_n \subset \mathbb{N} - \mathbf{S}$, isto é, se algum inteiro $n \in X$ então nenhum dos inteiros de 1 até n está em **S**. Se for o caso de $1 \in \mathbf{S}$, o teorema estará demonstrado pois 1 será o menor elemento de **S**. Se entretanto tivermos $1 \notin \mathbf{S}$ então $1 \in X$. É claro que X não pode conter todos os inteiros positivos pois o conjunto **S** contém algum elemento. Assim, se $P(n)$ for a afirmação que $n \in X$, temos que a primeira hipótese de indução $P(1)$ é verdadeira, mas a segunda parte não deve se cumprir, isto é, deve existir algum $n \in X$ tal que $n+1 \notin X$. Assim, todos os inteiros de 1 até n não pertencem a **S** mas $n+1 \in \mathbf{S}$. Desse modo, $n+1$ é o menor elemento do conjunto **S**. □

Corolário 2.2.1 (Indução - 2ª forma)**.** *Suponhamos que seja dada uma afirmação $P(n)$ dependendo de $n \in \mathbb{N}$ tal que*

- *$P(a)$ é verdadeira*
- *para cada inteiro $m > a$, $P(m)$ é verdadeira sempre que $P(k)$ for verdadeira para $a \leqslant k < m$*

Então, $P(n)$ é verdadeira para todo natural $n \geqslant a$.

Demonstração. Definamos os conjuntos $X = \{n \in \mathbb{N}; n \geqslant a \text{ e } P(n) \text{ é verdadeira}\}$. Para mostrar que a afirmação $P(n)$ é verdadeira para todo $n \geqslant a$ basta mostrar que $X' = \{n \in \mathbb{N}; n \geqslant a \text{ e } P(n) \text{ é falsa}\}$ não possui elementos. Suponha por absurdo que X' não é vazio, então existe um elemento mínimo $p \in X'$. Note que $p \neq a$. Nessas condições, para todo natural $a \leqslant m < p$, teremos $m \in X$. Pela hipótese feita sobre X temos $p \in X$, uma contradição. □

Axioma 2.2.3 (Divisão Euclidiana)**.** *Dados dois inteiros a e b com $b > 0$, existem únicos inteiros q e r chamados respectivamente de quociente e resto da divisão, tais que $a = b \cdot q + r$ com $0 \leqslant r < b$.*

Embora no enunciado desse axioma exista a restrição para que o número b seja positivo, também poderíamos considerar $b \neq 0$ para que a divisão fosse enunciada de maneira seguinte:
"Dados dois inteiros a e b com $b \neq 0$, existem únicos inteiros q e r chamados de quociente e resto da divisão respectivamente, tais que $a = b \cdot q + r$ com $0 \leqslant r < \mid b \mid$."

Exemplo 2.2.5. *Na divisão de 21 por 4 temos $q = 5$ e $r = 1$ pois $21 = 4 \cdot 5 + 1$ enquanto que ao dividir -27 por 6 temos $q = -5$ e $r = 3$ pois $-27 = 6(-5) + 3$.*

Definição 2.2.1. *A divisão Euclidiana é denominada* exata *quando tem $r = 0$. Nesse caso usamos a notação $b|a$ para indicar $a = b \cdot q$ e dizemos que* b divide a. *Caso contrário, escrevemos $b \nmid a$.*

Exemplo 2.2.6. *São exatas as divisões:*
12 por 3 pois $12 = 3 \cdot 4$ como também -24 por 6 pois $-24 = 6(-4)$ e escrevemos $3|12$ e $6|(-24)$ enquanto que a divisão de 14 por 5 não é exata pois $14 = 5 \cdot 2 + 4$ e, assim $5 \nmid 14$.

Surgem naturalmente algumas propriedades da divisão exata que utilizaremos neste texto. Para uma abordagem mais detalhada veja [8].

Proposição 2.2.2. *Em relação à divisão exata valem as seguintes propriedades:*

1. $1|a$ *para todo* $a \in \mathbb{Z}$
2. $a|a$ *para todo* $a \in \mathbb{Z}$ *e* $a \neq 0$
3. $a|0$ *para todo* $a \in \mathbb{Z}$ *e* $a \neq 0$.

Demonstração. As igualdades seguintes justificam cada item
$a = 1 \cdot a$; $a = a \cdot 1$ e $0 = a \cdot 0$. □

Proposição 2.2.3. *Para todos $a, b, c \in \mathbb{Z}$ com $a \neq 0$ e $b \neq 0$, se $a|b$ e $b|c$ então $a|c$.*

Demonstração. Se $a|b$ e $b|c$ implica que existem inteiros d e e tais que $b = a \cdot d$ e $c = b \cdot e$. Substituindo $b = a \cdot d$ na outra equação temos $c = b \cdot e = (a \cdot d)e = a(d \cdot e) = a \cdot f$ onde f é um certo número inteiro. Assim, temos que $a|c$. □

Proposição 2.2.4. *Sejam $a, b, c, d \in \mathbb{Z}$ com $a \neq 0$ e $c \neq 0$. Se $a|b$ e $c|d$ então $a \cdot c|b \cdot d$. Em particular temos que $a \cdot c|b \cdot c$.*

Demonstração. Se $a|b$ e $c|d$ então existem inteiros e e f tais que $b = a \cdot e$ e $d = c \cdot f$. Portanto, $b \cdot d = (a \cdot e)(c \cdot f) = (a \cdot c)(e \cdot f) = (a \cdot c)g$ onde $g \in \mathbb{Z}$, e $a \cdot c|b \cdot d$. □

Proposição 2.2.5. *Se $a, b, c, x, y \in \mathbb{Z}$ com $a \neq 0$ são tais que $a|b$ e $a|c$ então $a|(b \cdot x + c \cdot y)$. Isto é, se um número inteiro divide dois outros, também dividirá qualquer combinação linear inteira entre esses dois números.*

Demonstração. Se $a|b$ e $a|c$ então existem inteiros d e e tais que $b = a \cdot d$ e $c = a \cdot e$. Assim,

$$b \cdot x + c \cdot y = (a \cdot d)x + (a \cdot e)y = a(d \cdot x) + a(e \cdot y) = a[d \cdot x + e \cdot y] = a \cdot f$$

onde $f = d \cdot x + e \cdot y$ é um inteiro, o que mostra $a|(b \cdot x + c \cdot y)$. □

Proposição 2.2.6. *Dados $a, b \in \mathbb{Z}$ com $a > 0$ e $b > 0$. Se $a|b$ então $a \leqslant b$.*

Demonstração. Se $a|b$, existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$ e $c > 0$. Como $1 \leqslant c$, temos que $a \leqslant a \cdot c = b$. □

A proposição acima às vezes é utilizada para provar a igualdade entre dois inteiros positivos a e b mostrando que $a|b$ e $b|a$, daí seguem $a \leqslant b$ e $b \leqslant a$, donde $a = b$.

A divisão de um inteiro positivo N por 2 pode ser escrita de duas formas apenas: $N = 2q$ ou $N = 2q + 1$. No primeiro caso chamaremos N de *par*, no outro, *ímpar*.

A paridade de um número, apesar de ser um conceito bem simples, pode servir de ferramenta poderosa para inúmeras aplicações. Neste espaço comentaremos as respostas dos exercícios propostos no início dessa seção. Mas observemos inicialmente os seguintes resultados.

Proposição 2.2.7. *A soma de dois inteiros é par se, e somente se, ambos os números possuem a mesma paridade.*

Demonstração. Basta ver que se $a = 2q$ e $b = 2q'$, então $a + b = 2q + 2q' = 2(q + q')$. Se ambos os números são ímpares, digamos $a = 2q + 1$ e $b = 2q' + 1$, então $a + b = (2q + 1) + (2q' + 1) = 2(q + q' + 1)$ é um inteiro par.
Agora, usando a implicação contrapositiva, se eles possuem diferentes paridades, por exemplo, $a = 2q$ e $b = 2q' + 1$, temos que $a + b = 2q + (2q' + 1) = 2(q + q') + 1$ é um inteiro ímpar. □

Proposição 2.2.8. *O produto de dois inteiros é par se, e somente se, ao menos um deles é par.*

Demonstração. Se $a = 2q$ então $a \cdot b = (2q)b = 2(q \cdot b)$ é par. Usando a implicação contrapositiva, suponha agora que ambos sejam ímpares, $a = 2q + 1$ e $b = 2q' + 1$, então $a \cdot b = (2q + 1)(2q' + 1) = 4qq' + 2q + 2q' + 1 = 2(2qq' + q + q') + 1$ é um inteiro ímpar. □

Sobre os problemas iniciais podemos argumentar que é impossível cobrir as $5 \cdot 5 = 25$ casas do tabuleiro no exercício 1, pois essa é uma quantidade ímpar e não pode ser coberta completamente aos pares por cada pedra do dominó.
Sobre o exercício 2 percebamos que no interior da fila os números são postos em duplas justapostas, como existem oito números 6 e um deles está numa extremidade da fila, deve haver outro desse número na outra extremidade.
É impossível cobrir o tabuleiro do exercício 3 da forma descrita pois as duas casas deixadas fora possuem as mesma cor e cada pedra do dominó cobre exatamente duas cores opostas.
Para terminar, temos que no exercício 4, a soma dos números em cada folha (frente e verso) é ímpar, assim a adição de 25 números ímpares pode ser vista como a adição de 12 duplas de números ímpares (que gera um resultado par) mais um outro ímpar, cujo resultado geral é um número ímpar e, portanto, nunca será 2014.

2.3 Números Primos

Definição 2.3.1. *Um número inteiro e positivo p é chamado* primo *quando possui somente dois divisores positivos.*

São primos os inteiros $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ De acordo com a definição acima, o número 1 não é primo pois só possui um divisor positivo.

De acordo com a sugestão de visualizar os divisores como a quantidade de linhas ou colunas de uma disposição retangular, podemos dizer que os únicos modos de arranjo no caso da quantidade de bolinhas ser um número primo são aqueles de uma única linha ou coluna.

Uma dúvida que surge naturalmente refere-se à quantidade dos primos. A resposta já foi dada por Euclides em seu Livro IX dos Elementos. Essa prova é considerada um primor de beleza, simplicidade e engenhosidade. Ela utiliza pela primeira vez a redução ao absurdo como forma de demonstração. Mas antes precisaremos do seguinte teorema.

Teorema 2.3.1 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de primos positivos.*

Demonstração. Seja um inteiro positivo n maior do que 1. Pode acontecer dele ser primo e, neste caso não temos mais nada a provar. Suponhamos agora que n seja composto, então tomemos $p_1 > 1$ o menor dentre os divisores positivos de n. A minimalidade dessa escolha obriga que p_1 seja primo, pois, caso contrário, poderíamos escrever $p_1 = q \cdot r$ com $q < p_1$ e teríamos $q|p$, uma contradição, pois p_1 é o menor elemento com essa propriedade. Logo escrevemos $n = p_1 \cdot n_1$. Se n_1 for primo o teorema estará demonstrado. Caso contrário, tomamos p_2 como o menor fator (primo, pelo mesmo argumento acima) de n_1 e temos $n = p_1 \cdot p_2 \cdot n_2$. Vamos continuar esse processo e obter uma sequência decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$ que deve ser finita pois todos são positivos e, o último deles deve ser primo, pois caso contrário o processo continuaria. Os primos obtidos nessa construção, $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma

$$n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_k^{a_k}$$

Para mostrarmos a unicidade usamos a segunda forma do *Princípio de Indução Finita*. Para $n = 2$ a afirmação é verdadeira. Suponhamos que ela seja válida para todos os inteiros maiores que 1 e menores do que n. Vamos mostrar que ela também é válida para

n. Nestas condições, se n for primo, o Teorema estará demonstrado. Suponhamos então que n é composto e que tenha duas fatorações

$$n = p_1 \cdot p_2 \ldots p_s = q_1 \cdot q_2 \ldots q_r$$

Vamos provar que $r = s$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 \cdot q_2 \ldots q_r$ ele divide pelo menos um dos fatores q_j (Proposição 2.4.2 adiante). Sem perda de generalidade podemos supor que $p_1|q_1$.Como são ambos primos, isso significa que $p_1 = q_1$. Logo, após cancelar p_1 em ambos os membros, ficamos com $p_2 \ldots p_s = q_2 \ldots q_r < n$. A hipótese de indução nos diz que essas duas fatorações são idênticas pois representam um valor menor do que n, e com mais propriedade, temos que as primeiras fatorações também são idênticas, assim $r = s$. □

Agora vamos mostrar a argumentação simples que prova a infinidade dos primos.

Teorema 2.3.2. *Os números primos existem em quantidade infinita.*

Demonstração. Suponha que exista apenas um número finito de primos denominados $p_1, p_2, \ldots, p_n$. Mostraremos que essa condição acarreta uma contradição lógica. Portanto, a tese de que existem infinitos números primos é que deve ser verdadeira.
Tomemos o número inteiro $N = p_1 \cdot p_2 \ldots p_n + 1$. Pelo *Teorema Fundamental da Aritmética* N possui um fator primo p_i que deve ser um dos primos $p_1, \ldots, p_n$. Temos assim que p_i divide N e também divide o produto $p_1 \cdot p_2 \ldots p_n$, logo divide $N - p_1 \cdot p_2 \ldots p_n$ pois esse é uma combinação linear inteira. Assim, p_i divide 1 o que é absurdo pois $p_i \neq 1$. □

Após responder o questionamento sobre a quantidade de primos, parece bastante natural continuar essa investigação sobre suas distribuições relativas e como determinar se um dado número inteiro é ou não primo. Essas perguntas, entretanto, não têm respostas elegantemente simples como a demonstração do teorema anterior e é objeto de estudo de muitas mentes brilhantes hoje em dia. Basta lembrar que a segurança de quase todas as operações financeiras pela internet se baseia na criptografia, isto é, no embaralhamento e substituição dos Bytes que compõem a informação original por outra sequência, aparentemente indecifrável mas que pode ser restaurada pelo recebedor. A base matemática que fundamenta esse processo é a impossibilidade de determinar facilmente a forma fatorada de um inteiro gigantesco.

2.4 Máximo Divisor Comum

Desde o ensino fundamental nossas crianças são apresentadas a problemas do tipo

Exemplo 2.4.1. *No piso de uma sala em forma retangular com* 3,36 *m de largura e* 4,00 *m de comprimento, um construtor deseja colocar peças de granito quadradas com medidas inteiras em centímetros e do mesmo tamanho. Determine a menor quantidade dessas peças que ele pode usar para cobrir completamente o piso, sem quebrar nenhuma.*

Como o piso deve ser completamente coberto, é claro que as peças quadradas devem ser encaixadas lado a lado com suas bordas paralelas aos lados do piso retangular de maneira a não deixar espaços vazios. Para determinar a menor quantidade dessas peças é necessário observar que essas devem possuir o maior tamanho possível. Seja N a medida máxima do lado dessas peças. O encaixe sem sobras nos diz que N deve ser um divisor simultâneo de 336 cm e 400 cm (transformadas as medidas racionais em inteiras). Caso ele exista, como achar tal divisor? Uma abordagem experimental é tentar encontrar explicitamente todos os divisores comuns positivos. Outro modo deve-se a *Euclides* por seu método das divisões sucessivas. Comecemos de maneira mais prosaica.
Após alguns testes de divisões chega-se aos conjuntos dos divisores positivos

$$\mathbf{D}(336) = \{\mathbf{1}, \mathbf{2}, 3, \mathbf{4}, 6, 7, \mathbf{8}, 12, 14, \mathbf{16}, 21, 24, 28, 42, 48, 56, 84, 112, 168, 336\}$$

$$\mathbf{D}(400) = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, 5, \mathbf{8}, 10, 15, \mathbf{16}, 20, 25, 40, 50, 80, 100, 200, 400\}$$

O maior valor dos divisores comuns é 16. Como $336 = 16 \cdot 21$ e $400 = 16 \cdot 25$ temos que cada quadrado cabe exatamente 21 vezes na largura e 25 no comprimento, totalizando $21 \cdot 25 = 525$ peças para ladrilhar completamente a sala.

Esse número $N = 16$ visto acima é o que chamamos de *máximo divisor comum* dos números 336 e 400. Mais geralmente temos a definição seguinte.

Definição 2.4.1. *O máximo divisor comum (abreviadamente MDC) de dois números a e b, não simultaneamente nulos, é o maior inteiro positivo que divide a e b. Denotamo-lo por (a, b).*

Exemplo 2.4.2. $(12, 8) = 4$, $(14, 7) = 7$, $(5, 3) = 1$.

A existência do máximo divisor comum é assegurada devido o fato de que o conjunto dos divisores positivos de qualquer inteiro não nulo é finito e possui ao menos o número 1. Daqui em diante, quando nos referirmos ao MDC de dois números, estaremos admitindo que ambos não sejam simultaneamente nulos.

Um fato interessante e muito útil é sempre sermos capazes de escrever o MDC de dois números inteiros como uma combinação inteira daqueles números. Vejamos no exemplo anterior que $16 = 336 \cdot 6 + 400(-5)$. Esse resultado geral é mostrado no próximo teorema.

Teorema 2.4.1. *O máximo divisor comum de dois inteiros pode sempre ser escrito como combinação inteira desses números. Em outras palavras, se $d = (a, b)$, então existem inteiros x e y tais que $d = a \cdot x + b \cdot y$.*

Demonstração. Vamos definir M como o conjunto de todas as combinações inteiras e positivas de a e b. Esse conjunto não é vazio visto que $a^2 + b^2 = a \cdot a + b \cdot b$ pertence a M. Em virtude do *Princípio da Boa Ordem* podemos tomar c, o menor elemento de M, que é escrito $c = a \cdot x_0 + b \cdot y_0$. Vamos mostrar que c é o maior divisor comum de a e b. Afirmamos que $c|a$. Pois na divisão euclidiana, $a = c \cdot q + r$ com $0 \leqslant r < c$

$$r = a - c \cdot q = a - (a \cdot x_0 + b \cdot y_0)q = (1 - x_0 \cdot q)a + (-y_0 \cdot q)b$$

Isso nos mostra que $r = 0$, pois caso contrário, r seria uma combinação inteira de a e b menor do que c. Isso é uma contradição em virtude da minimalidade de c. Da mesma maneira mostramos que $c|b$. Agora basta mostrar que c é igual ao maior divisor comum. Seja $d = (a, b)$. Assim, $a = d \cdot q_1$ e $b = d \cdot q_2$, portanto temos

$$c = x_0 \cdot a + y_0 \cdot b = x_0(d \cdot q_1) + y_0(d \cdot q_2) = d(x_0 \cdot q_1 + y_0 \cdot q_2)$$

o que nos mostra $d|c$. Como ambos os números d e c são positivos, temos $d \leqslant c$. Basta notar agora que a condição $d < c$ é impossível pois d é o maior dentre os divisores comuns. Resta então a opção $d = c$ como verdadeira. □

Utilizaremos o teorema acima para mostrar que o MDC de dois inteiros é divisível por qualquer outro divisor comum dos números dados. Esse resultado é muito útil para provar outras propriedades envolvendo o MDC.

Teorema 2.4.2. *O máximo divisor comum de dois inteiros é divisível por qualquer divisor comum dos inteiros dados.*

Demonstração. Seja d o maior divisor comum dos inteiros a e b. Podemos escrevê-lo como combinação inteira $d = a \cdot x + b \cdot y$ onde $x, y \in \mathbb{Z}$. Se c é qualquer divisor comum de a e b, isto é, $c|a$ e $c|b$ logo, pelo teorema acima, $c|(a \cdot x + b \cdot y)$, ou seja, $c|d$. □

Para ilustrar o teorema acima, no caso do exemplo particular no início dessa seção, relembremos que os múltiplos comuns de 336 e 400 são $1, 2, 4, 8$ e 16 e vemos que $16 = (336, 400)$ é divisível por todos os outros múltiplos comuns.

Proposição 2.4.1. *Para a, b e n inteiros com $n > 0$, temos $(n \cdot a, n \cdot b) = n(a, b)$.*

Demonstração. Basta ver que $(n \cdot a, n \cdot b)$ é o menor valor positivo das combinações inteiras $(n \cdot a)x + (n \cdot b)y$ que é igual a $n(a \cdot x + b \cdot y)$ onde $a \cdot x + b \cdot y$ é o menor valor positivo das combinações de a e b. □

Definição 2.4.2. *Chamamos de* primos entre si *aos inteiros a e b quando $(a, b) = 1$.*

Proposição 2.4.2. *Se um número primo p divide um produto de dois inteiros então ele divide um dos fatores.*

Demonstração. Seja p primo tal que $p|(a.b)$. Se p divide a, o teorema está demonstrado. Suponha então que $p \nmid a$, nessa condição, o único divisor positivo comum desses números é 1, assim, $(p, a) = 1$ e podemos escrever $p \cdot x + a \cdot y = 1$ com $x, y \in \mathbb{Z}$. Multiplicando ambos os lados dessa igualdade por b e reagrupando temos $p(x \cdot b) + (a \cdot b)y = b$. Como $p|p$ e, por hipótese, $p|(a \cdot b)$ vem que $p|[p(x \cdot b) + (a \cdot b)y]$, ou seja, $p|b$. □

Uma propriedade do MDC utilizada em demonstrações é dada pelo corolário seguinte. Ele nos diz que se extrairmos todos os fatores comuns entre dois números, as sobras são, necessariamente, números primos entre si.

Corolário 2.4.1. *Para inteiros a e b, se $d = (a, b)$ temos que $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Demonstração. Temos que $a = d \cdot q_1$ e $b = d \cdot q_2$. Valem as igualdades

$$d = (a, b) = (d \cdot q_1, d \cdot q_2) = d(q_1, q_2)$$

Daí vem que $d(q_1, q_2) = d$, ou seja, $(q_1, q_2) = 1$, assim, $(\frac{a}{d}, \frac{b}{d}) = 1$. □

Exemplo 2.4.3. *Como $(12, 15) = 3$, temos $(\frac{12}{3}, \frac{15}{3}) = 1$.*

Note que a recíproca desse corolário é sempre verdadeira, isto é, se acrescentarmos um fator comum a dois inteiros primos entre si, esse fator comum passa a ser seu MDC.

Este próximo resultado será usado para provar o método de determinação do MDC de dois inteiros por meio das divisões sucessivas. Apresentado por *Euclides* no seu *Livro VII*, ainda é um método computacional dos mais eficientes, ainda utilizado hoje em dia com poucas modificações.

Lema 2.4.1 (Lema de Euclides)**.** *Sejam a, b e m inteiros, tem-se* $(a, b) = (a, b + m \cdot a)$.

Demonstração. Podemos escrever (a, b) como combinação inteira de a e b. Assim,

$$(a, b) = a \cdot x_0 + b \cdot y_0 = a \cdot x_0 - m \cdot a \cdot y_0 + m \cdot a \cdot y_0 + b \cdot y_0 = a(x_0 - m \cdot y_0) + (b + m \cdot a)y_0$$

Como $(a, b + m \cdot a)|a$ e $(a, b + m \cdot a)|(b + m \cdot a)$ temos $(a, b + m \cdot a)|(a, b)$.
Agora mostraremos a divisão recíproca.
Como $(a, b)|a$ e $(a, b)|b$, temos $(a, b)|b + m \cdot a$ Assim, (a, b) é um divisor comum de a e $b + m \cdot a$, logo divide $(a, b + m \cdot a)$.
Como ambos, (a, b) e $(a, b + m \cdot a)$ são positivos, está provada sua igualdade. □

Vamos voltar novamente ao exemplo inicial em que $(336, 400) = 16$. Utilizaremos o *Algoritmo da Divisão de Euclides* para dividir 400 por 336. Em seguida, dividiremos sucessivamente o divisor pelo resto obtido até obtermos resto zero em alguma divisão.

$$400 = 336 \cdot 1 + 64$$
$$336 = 64 \cdot 5 + \mathbf{16}$$
$$64 = \mathbf{16} \cdot 4 + 0$$

O MDC dos dois inteiros é o último resto não nulo e o motivo é bem simples

$$(336, 400) = (336, 336 \cdot 1 + 64) = (336, 64) = (64 \cdot 5 + 16, 64) = (16, 64) = 16$$

A última igualdade vem do fato $16|64$. O custo desse procedimento comparado com o trabalho em determinar os divisores ou fatorar os números evidencia sua eficácia e rapidez. Infelizmente isso é pouco divulgado nos textos do ensino básico. Bem, talvez Euclides não seja conhecido por todos nossos autores de livros didáticos!

Tão importante como encontrar o MDC, esse algoritmo também fornece meios de escrevê-lo como combinação linear inteira dos números em questão. Com os dados do exemplo acima temos $400 = 336 \cdot 1 + 64$ e $336 = 64 \cdot 5 + 16$. Substituindo o resto 64 da primeira equação na segunda ficamos com $16 = 336 - (400 - 336 \cdot 1)5 = 336 \cdot 6 + 400(-5)$. Para maiores detalhes, recomendamos [6].

2.5 Mínimo Múltiplo Comum

Comparado ao *máximo divisor comum*, o conceito de *mínimo múltiplo comum* de dois ou mais inteiros é bem mais frequente em livros do ensino básico, aparecendo em problemas em que certos eventos se repetem. Uma motivação bem interessante para introduzir esse conceito poderia ser o exemplo seguinte.

Exemplo 2.5.1. *Ariel e Beriel vão a um restaurante e são atendidos por um garçon excêntrico que traz a pizza dividida em* 16 *pedaços dos quais eles comem* 10*. Outro dia repetem o programa mas pedem ao garçon que traga a pizza dividida em pedaços um pouco maiores. O garçon obedece e, das* 12 *fatias iguais, os amigos consomem* 8*. Ariel comenta que ele se sente "mais cheio" embora a quantidade de fatias consumidas foi menor. Isso pode ser verdade?*

Só faz sentido comparar as fatias quando essas são do mesmo tamanho. Para resolver isso podemos imaginar cada um dos 16 pedaços da primeira pizza sendo divididos em 3 sub-fatias iguais totalizando $3 \cdot 16 = 48$ fatias. Na segunda pizza dividimos cada pedaço em 4 outros iguais perfazendo $4 \cdot 12 = 48$. Como agora a quantidade e os tamanhos de todas as fatias são iguais, agora é só compará-las. As 10 fatias da primeira pizza tornam-se $10 \cdot 3 = 30$ novos pedaços enquanto que 8 fatias da segunda, $8 \cdot 4 = 32$ pedaços. Portanto, é verdade que eles consumiram mais no segundo dia.

Visto pela ótica acima, essa apresentação torna-se mais motivadora do que simplesmente pedir aos alunos para comparar ou somar $\frac{10}{16}$ e $\frac{8}{12}$. A necessidade de encontrar um múltiplo comum de 12 e 16 nos leva ao próximo tópico.

Definição 2.5.1. *O mínimo múltiplo comum de dois inteiros* a *e* b *é o menor inteiro positivo que é divisível por cada um deles. Denotamo-lo por* $[a, b]$*.*

Exemplo 2.5.2. $[2, 3] = 6, \quad [6, 8] = 24 \quad [14, 7] = 14.$

Por simplicidade, algumas vezes abreviamos o nome *mínimo múltiplo comum* por MMC.

Proposição 2.5.1. *O mínimo múltiplo comum* m *de dois inteiros divide todo múltiplo comum* n *daqueles números.*

Demonstração. Como $m = [a, b]$, temos a existência de inteiros q_1 e q_2 tais que $m = a \cdot q_1$ e $m = b \cdot q_2$. Dado que n também é múltiplo comum de a e b temos a existência de

inteiros r_1 e r_2 tais que $n = a \cdot r_1$ e $n = b \cdot r_2$.
Vamos mostrar que $m|n$. Pela divisão euclidiana, temos $n = m \cdot q + r$ com $0 \leqslant r < m$, daí vem

$$r = n - m \cdot q = a \cdot r_1 - (a \cdot q_1)q = a(r_1 - q_1 \cdot q)$$

Do mesmo modo obtemos

$$r = n - m \cdot q = b \cdot r_2 - (b \cdot q_2)q = b(r_2 - q_2 \cdot q)$$

Isso nos mostra que $r = 0$, pois caso contrário r seria um múltiplo comum de a e b menor do que m, o que é um absurdo devido a minimalidade de m. □

A proposição acima nos indica como construir a sequência dos múltiplos comuns positivos de dois inteiros: basta achar seu MMC e, a partir dele, tomar múltiplos. Mas como encontrá-lo? A prática mais comum é fatorar os números em questão e construir o produto dos fatores primos comuns com maior expoente. A propriedade abaixo tem aplicação mais teórica e não é menos importante.

Proposição 2.5.2. *Dados dois inteiros a e b, temos que $[a, b](a, b) = a \cdot b$.*

Demonstração. Tomando $m = \dfrac{a \cdot b}{(a, b)}$ vamos mostrar que ele é igual ao MMC de a e b. Temos claramente $m = a\dfrac{b}{(a, b)}$ e $m = b\dfrac{a}{(a, b)}$, isto é, m é múltiplo comum de a e b. Seja c um múltiplo comum de a e b, $c = n \cdot a = n' \cdot b$. Ao dividirmos ambos os termos anteriores por (a, b) ficamos com $n\dfrac{a}{(a, b)} = n'\dfrac{b}{(a, b)}$, mas $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)}$ são primos entre si, assim, $\dfrac{a}{(a, b)}$ divide n', acrescentando a esses termos o fator b ficamos com $m = b\dfrac{a}{(a, b)}$ divide $b \cdot n'$, isto é, $m|b \cdot n'$, portanto $m|c$ e $m \leqslant c$ nos mostrando ser m o menor múltiplo comum de a e b. □

Corolário 2.5.1. *Se a e b são número inteiros primos entre si, então $[a, b] = a \cdot b$.*

Demonstração. Basta fazer $(a, b) = 1$ no teorema acima e o resultado é imediato. □

Para uma natural continuação mais avançada nos tópicos desenvolvidos até aqui, inclusive com muitos exercícios de olimpíadas de Matemática veja [8].

3 CONGRUÊNCIAS

3.1 Introdução às Congruências

Os conceitos e propriedades vistos até agora darão o suporte necessário para o desenvolvimento dessa terceira parte que trata das congruências e algumas de suas aplicações.

- Qual é a 2013ª figura na sequência ♢, ♠, ♡, ♣, ♢, ♠, ♡, ♣,...?
- As datas 18 de abril e 18 de outubro caem no mesmo dia da semana?
- O número 3 541 067 892 é divisível por 9?
- Qual é o critério de divisibilidade por 11?
- Qual é o resto da divisão de 5^{110} por 6?

Não é raro um professor do ensino básico se deparar com algumas das questões anteriores que, apesar de sua variedade, trazem todas o mesmo pano de fundo: a necessidade de aplicação de uma nova ferramenta desenvolvida por Carl Friedrich Gauss $(1777-1855)$ e apresentada em seu livro *Disquisitiones Arithmeticae*. Originalmente escrito em latim, nessa obra sobre a Teoria dos Números, Gauss mostra que a Matemática desenvolvida no anel dos números inteiros pode dar origem a uma outra que acontece entre as classes de equivalência desse conjunto. Em outras palavras, é como se pudéssemos "dividir"o conjunto $\mathbb{Z}$ numa certa quantidade de subconjuntos infinitos chamados *classes de equivalência* em que qualquer elemento de um desses subconjuntos poderia representá-lo nas operações de adição ou multiplicação com qualquer outra classe de maneira que a soma e o produto permaneceriam consistentes, isto é, seriam invariáveis, não importando quais representantes foram escolhidos para cada classe. De maneira bem prosaica, é como se numa disputa, qualquer torcedor do Fortaleza ou Ceará pudessem representar igualmente bem seus times de futebol.

Vamos ao exemplo anterior do calendário. Tome um mês qualquer e escolha um dia da semana. Observe que os números nessa coluna são gerados somando setes àquele do topo. isso acontece devido ao posicionamento regular que faz os números serem distribuídos na mesma coluna a cada sete dias. Seremos um pouco exagerados agora. Imagine por economia que o ano de 2013 possua um só mês com 365 dias. Sobre essa maior quantidade de dias aquele padrão surgido há pouco se faz notar com mais clareza. Para completar nosso "passeio", imagine um círculo com sete lugares dispostos no sentido horário sobre ele e nomeados como, por exemplo, segunda-feira, terça-feira, ..., domingo. (Alguma semelhança não é mera coincidência). Comecemos pois, a distribuir os dias do nosso único mês nos lugares desse círculo. Facilmente observamos vários padrões subjacentes a cada um dos lugares nomeados agora por G_1, G_2, ..., G_6 e G_0.

- $G_1 = \{1, 8, 15, 22, 29, 36, \ldots\}$
- $G_2 = \{2, 9, 16, 23, 30, 37, \ldots\}$
- $G_3 = \{3, 10, 17, 24, 31, 38, \ldots\}$
- $G_4 = \{4, 11, 18, 25, 32, 39, \ldots\}$
- $G_5 = \{5, 12, 19, 26, 33, 40, \ldots\}$
- $G_6 = \{6, 13, 20, 27, 34, 41, \ldots\}$
- $G_0 = \{7, 14, 21, 28, 35, 42, \ldots\}$

Percebamos que na divisão euclidiana por sete, qualquer elemento do conjunto G_r deixa resto r e que elementos de um mesmo grupo diferem por múltiplos de sete. Essa será nossa definição de congruência.

Definição 3.1.1. *Sejam a, b e m inteiros com $m > 0$. Dizemos que a é congruente a b módulo m quando $m|(a-b)$. Denotamos essa condição por $a \equiv b(mod\ m)$. Caso contrário, escrevemos $a \not\equiv b(mod\ m)$.*

É uma interpretação geométrica da congruência de dois inteiros módulo m, aqueles números estarem separados na reta numérica por uma distância tal que um segmento de tamanho m cabe, de maneira justaposta, uma quantidade exata de vezes. No caso de "enrolar" a reta numérica numa disposição circular, formam-se apenas m posições inteiras coincidentes, serão essas as classes de equivalência.

Exemplo 3.1.1. $22 \equiv 14(mod\ 2)$ *pois* $2|(22-14)$*; como* $6 \nmid 15$ *temos que* $18 \not\equiv 3(mod\ 6)$.

Agora vamos voltar para as nossas perguntas no início dessa seção e tentar obter algumas respostas simples. Com relação à primeira, podemos começar observando que do dia 18 de abril a 18 de outubro há um total de: 13 dias em abril; 31 dias em maio; 30 em junho; 31 dias em julho; 31 em agosto; 30 em setembro e 18 em outubro, totalizando,

$$13 + 31 + 30 + 31 + 31 + 30 + 18 = 184\ dias$$

Qualquer que seja o dia da semana em 18 de abril, o dia 18 de outubro será o mesmo quando a diferença entre suas enumerações inteiras tomadas de modo contínuo for um múltiplo de 7. Como há 184 dias, essa diferença é 183, assim, pela divisão euclidiana, $183 = 7 \cdot 26 + 1$ indicando que o dia 18 de outubro não cai no mesmo dia mas está deslocado em uma data para o futuro.

Na segunda pergunta, sobre a ordenação das figuras, a determinação daquela que ocupa uma posição qualquer segue o mesmo raciocínio anterior.
Vejamos a sequência: ♢, ♠, ♡, ♣, ♢, ♠, ♡, ♣, ♢, ♠, ♡, ♣ ... a figura ♢ ocupa as posições $1, 5, 9, \ldots$ Vamos definir
$P_1 = \{1, 5, 9, 13, \ldots\}$ para representar as posições de ♢ e estender respectivamente para as outras figuras os conjuntos seguintes
$P_2 = \{2, 6, 10, 14, \ldots\}$
$P_3 = \{3, 7, 11, 15, \ldots\}$
$P_0 = \{4, 8, 12, 16, \ldots\}$
Vemos facilmente que as posições pertencentes ao conjunto P_r deixam resto r na divisão por 4. Agora é só investigar em qual classe está a 2013ª figura. A divisão euclidiana nos dá $2013 = 4 \cdot 503 + 1$ indicando o conjunto P_1 como aquele em que ela está, sendo ♢ tal figura.

Para uma abordagem mais simplificada dos outros exemplo são necessárias mais algumas outras propriedades das congruências.

Proposição 3.1.1. *Sejam a, b, c e m inteiros com $m > 0$. São válidas as propriedades abaixo:*

1. $a \equiv a (mod\ m)$
2. *Se* $a \equiv b (mod\ m)$ *então* $b \equiv a (mod\ m)$
3. *Se* $a \equiv b (mod\ m)$ *e* $b \equiv c (mod\ m)$ *então* $a \equiv c (mod\ m)$.

Demonstração. Para todo $a \in \mathbb{Z}$ vale $m|(a - a)$, isto é, $a \equiv a (mod\ m)$.

Se $a \equiv b(mod\ m)$ então $m|(a-b)$, mas também $m|(b-a)$ e assim, $b \equiv a(mod\ m)$.
Por fim, se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, temos $m|(a-b)$ e $m|(b-c)$, daí m divide a combinação inteira $m|[(a-b)+(b-c)]$, ou seja, $m|(a-c)$ e portanto, $a \equiv c(mod\ m)$. □

Proposição 3.1.2. *Se a, b, c, d e m são inteiros com $m > 0$, tais que $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$ então valem:*

1. $a + c \equiv b + d(mod\ m)$
2. $a \cdot c \equiv b \cdot d(mod\ m)$.

Demonstração. Dados os inteiros nas condições da proposição acima

1. Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $m|(a-b)$ e $m|(c-d)$, portanto $m|[(a-b)+(c-d)]$, ou seja, $m|[(a+c)-(b+d)]$ e isso mostra que $a + c \equiv b + d(mod\ m)$.
2. Como $m|(a-b)$ e $m|(c-d)$, também valem $m|(a-b)c$ e $m|(c-d)b$, e daí, $m|[(a-b)c+(c-d)b]$, que simplificando nos dá $m|(a \cdot c - b \cdot d)$ indicando ser $a \cdot c \equiv b \cdot d(mod\ m)$.

□

A propriedade acima nos mostra que podemos somar ou multiplicar membro a membro duas (ou uma quantidade finita) congruências. É esse fato que torna a matemática das congruências um todo consistente pois não importa quais representantes das classes de equivalência nós tomamos, seu resultado é sempre um representante da mesma classe invariável da soma ou produto.

Exemplo 3.1.2. *Na divisão por 7 já vista anteriormente temos $11 \equiv 4(mod\ 7)$ e $19 \equiv 5(mod\ 7)$, assim podemos escrever $30 = 11 + 19 \equiv 4 + 5 = 9 \equiv 2(mod\ 7)$ e também $209 = 11 \cdot 19 \equiv 4 \cdot 5 = 20 \equiv 6(mod\ 7)$.*

Corolário 3.1.1. *Se a, b, c e m são inteiros com $m > 0$ tais que $a \equiv b(mod\ m)$, então*

1. $a + c \equiv b + c(mod\ m)$
2. $a - c \equiv b - c(mod\ m)$
3. $a \cdot c \equiv b \cdot c(mod\ m)$.

Demonstração. Como $a \equiv b(mod\ m)$, basta observar que $c \equiv c(mod\ m)$ e $(-c) \equiv (-c)(mod\ m)$ e usar os itens da proposição anterior. □

Já percebemos que podemos adicionar ou multiplicar membro a membro duas congruências. Mas não podemos, em geral, cancelar um fator comum. A condição em que isso pode ser feito é dada pelo teorema seguinte.

Teorema 3.1.1. *Sejam a, b, c e m inteiros com $m > 0$ tais que $a \cdot c \equiv b \cdot c (mod\ m)$, então $a \equiv b (mod \frac{m}{(c,m)})$.*

Demonstração. De $a \cdot c \equiv b \cdot c (mod\ m)$ vem $m|(a \cdot c - b \cdot c)$, ou seja, $m|(a-b)c$. Dividindo ambos os números m e c pelo seu fator comum (c, m), temos $\frac{m}{(c,m)}|(a-b)\frac{c}{(c,m)}$, e tendo em vista que $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são inteiros e primos entre si, ocorre $\frac{m}{(c,m)}|(a-b)$ de onde vem $a \equiv b (mod\ \frac{m}{(c,m)})$. □

Exemplo 3.1.3. *Como $20 \equiv 12 (mod\ 8)$, escrevemos $5 \cdot 4 \equiv 3 \cdot 4 (mod\ 8)$. Daí, $5 \equiv 3 (mod\ \frac{8}{4})$ pois $(4, 8) = 4$.*

Há uma outra maneira bem comum de traduzir a sentença $a \equiv b (mod\ m)$ que é dizer *b é resíduo de a módulo m*. Essa nomeclatura será útil mais adiante.

Chamaremos de *sistema completo de resíduos* a todo conjunto com a menor quantidade de elementos representativos de todas as classes de congruências dadas módulo m.

Definição 3.1.2. *O conjunto dos números inteiros $\{r_1, r_2, \ldots, r_k\}$ é um sistema completo de resíduos módulo m se*

1. *$r_i \not\equiv r_j (mod\ m)$ quando $i \neq j$.*
2. *qualquer inteiro n é congruente a algum r_i módulo m.*

Exemplo 3.1.4. *Para $k \in \mathbb{Z}$, são sistemas completos de resíduos módulo 5:*
$\{0, 1, 2, 3, 4\}$; $\{6, 7, 8, 9, 10\}$; $\{k+0,\ k+1,\ k+2,\ k+3,\ k+4\}$.

Exemplo 3.1.5. *Para $k \in \mathbb{Z}$, são sistemas completos de resíduos módulo m:*
$\{0, 1, 2, \ldots, m-1\}$; $\{k+0,\ k+1,\ k+2, \ldots, k+(m-1)\}$.

Em todo sistema completo de resíduos há um único representante de cada uma das classes de equivalência em que foi particionado o conjunto $\mathbb{Z}$. Vamos assumir o fato óbvio, e passível de ser facilmente provado, que todos os sistemas completos de resíduos módulo m têm a mesma quantidade de elementos. Para detalhes veja [10] nas referências.

Dado um sistema completo de resíduos, há infinitos modos de construir outro sistema a partir daquele. Isso é mostrado no teorema seguinte.

Teorema 3.1.2. *Seja* $\{r_1, r_2, \ldots, r_m\}$ *um sistema completo de resíduos módulo* m*. Para todos os inteiros* a *e* k *com* $(a, m) = 1$*, temos que* $\{a \cdot r_1 + k, a \cdot r_2 + k, \ldots, a \cdot r_m + k\}$ *também é um sistema completo de resíduos módulo* m*.*

Demonstração. Usaremos o argumento usado por [8]. Como a quantidade de elementos num sistema completo de resíduo módulo m é constante, basta mostrar que quaisquer dois inteiros desse conjunto são incongruentes módulo m. Suponhamos por absurdo que haja dois elementos congruentes, isto é, $a \cdot r_i + k \equiv a \cdot r_j + k (mod\ m)$, assim também temos $a \cdot r_i \equiv a \cdot r_j (mod\ m)$. E como $(a, m) = 1$, cancelamos o termo comum a, ficando com $r_i \equiv r_j (mod\ m)$ e $i \neq j$. Mas isso é uma contradição com a hipótese de $\{r_1, r_2, \ldots, r_n\}$ ser um sistema completo de resíduos. □

Proposição 3.1.3. *Se* a, b, k *e* m *são inteiros com* $k > 0$ *e* $a \equiv b (mod\ m)$*, então* $a^k \equiv b^k (mod\ m)$*.*

Demonstração. Podemos utilizar indução sobre k ou então simplesmente o fato de $m|(a - b)$ implica $m|(a - b)(a^{k-1} + a^{k-2} \cdot b + \ldots + a \cdot b^{k-2} + b^{k-1})$, isto é, $m|(a^k - b^k)$ o que indica $a^k \equiv b^k (mod\ m)$. □

Para finalizar as propriedade das congruências, temos o teorema abaixo que relaciona dois inteiros congruentes a vários módulos. Em palavras mais simples, se a distância que separa dois inteiros na reta numérica pode ser subdividida numa quantidade exata de vezes utilizando um dado tamanho menor, e esse fato acontece com alguns tamanhos diferentes, então o MMC de todos esses tamanhos também divide a distância entre a e b.

Teorema 3.1.3. *Se* $a \equiv b (mod\ m_1), a \equiv b (mod\ m_2), \ldots, a \equiv b (mod\ m_k)$*, nas condições* $a, b, m_1, \ldots, m_k \in \mathbb{Z}$ *com* $m_i > 0, i = 1, 2, \ldots, k$*, decorre que* $a \equiv b (mod\ [m_1, m_2, \ldots, m_k])$*.*

Demonstração. Dadas as condições de congruências acima, temos as seguintes divisões exatas: $m_1|(a - b), m_2|(a - b) \ldots m_k|(a - b)$. Isso nos diz que $(a - b)$ é um múltiplo comum de $m_1, m_2, \ldots, m_k$, mas, por sua definição, o MMC desses número deve dividir qualquer múltiplo comum, assim, $[m_1, m_2, \ldots, m_k]|(a - b)$, portanto, $a \equiv b (mod\ [m_1, m_2, \ldots, m_k])$. □

Agora podemos voltar aos outros problemas propostos no início dessa seção.
Qualquer inteiro escrito na forma decimal $a_n \ldots a_1 a_0$ representa a soma das potências $a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$ onde $a_i \in \{0, 1, \ldots, 9\}$. Sabendo que $10 \equiv 1 (mod\ 9)$, temos então $10^k \equiv 1^k \equiv 1 (mod\ 9)$ para todo $k \in \mathbb{Z}, k > 0$. Multiplicando ambos os lados dessa última

congruência por a_k, vem $a_k \cdot 10^k \equiv a_k (mod\ 9)$. Somando-se membro a membro todas as congruências das potências que formam o número dado inicialmente, ele será congruente à soma dos números formados por seus algarismos individualmente,

$$N = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 \equiv a_n + \ldots + a_1 + a_0 (mod\ 9).$$

No caso de $N = 3\ 541\ 067\ 892$, a soma de seus "algarismos" é
$S = 3 + 5 + 4 + 1 + 0 + 6 + 7 + 8 + 9 + 2 = 45$ é congruente a zero, $N \equiv 45 \equiv 0 (mod\ 9)$. Assim nosso número é divisível por 9.

Em relação à divisibilidade de um número por 11 podemos começar observando que $10 \equiv (-1) (mod\ 11)$. Multiplicando essa congruência certa quantidade de vezes por ela própria temos

- $10^k \equiv (-1)^k \equiv (-1) (mod\ 11)$ para todo k inteiro e ímpar, enquanto que
- $10^k \equiv (-1)^k \equiv 1 (mod\ 11)$ para k inteiro par

Somando todas as congruências das potências que formam um dado inteiro, ficamos com

$$N = a_n \cdot 10^n + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0 - a_1 + a_2 - a_3 + \ldots (mod\ 11).$$

Portanto, basta reconhecer a qual resíduo, de zero a dez, a soma alternada $S_a = a_0 - a_1 + a_2 - a_3 + \ldots$ é congruente. No caso de $N = 132\ 769$ temos $S_a = 9 - 6 + 7 - 2 + 3 - 1 = 10$. Esse número 132 769 deixa resto resto 10 na divisão por 11. No caso da soma alternada gerar um valor menor que zero ou maior que dez, basta acrescentar ou subtrair múltiplos de onze até que o resultado fique na faixa esperada. Lembre-se que os elementos em cada classe diferem por múltiplos de onze e, assim, esse procedimento não altera a classe a que pertence o resultado original. Por exemplo, se $N = 516\ 243$, temos $S_a = 3 - 4 + 2 - 6 + 1 - 5 = -9$, e seu resto na divisão por 11 será então $r = -9 + 11 = 2$.

Vários outros critérios de divisibilidade podem ser demonstrados usando congruências. Recomendamos a leitura de [2], [4], [6] e [11].

Para responder ao último exercício, sobre a determinação do resto, na divisão de 5^{110} por 6, vemos facilmente que a visualização dessa potência através dos recursos comuns no ensino básico é impossível. O professor deve, portanto, usar meios indiretos nessa abordagem. Novamente as congruências aparecem para nos facilitar a vida. A partir do fato óbvio que $5 \equiv (-1) (mod\ 6)$, basta multiplicar membro a membro 110 dessas congruências para obter $5^{110} \equiv (-1)^{110} \equiv 1 (mod\ 6)$. O resto procurado nessa divisão é 1.

3.2 Congruências Lineares

Os professores do ensino básico, notadamente aqueles que trabalham com treinamento para olimpíadas de Matemática, sempre se deparam com problemas de agrupamentos dos tipos seguintes:

- Deseja-se arrumar 20 carros em filas de 3 ou de 5 carros. De quantos modos isso pode ser feito?
- Quantas quadras de basquete e de vôlei são necessárias para que 80 alunos joguem simultaneamente? e se forem 77 alunos?
- Para transportar 2000 alunos dispomos de ônibus e vans que levam respectivamente 40 e 15 alunos de cada vez. De quantos modos podemos fazer esse transporte? Qual a quantidade mínima de viagens? Se o custo de cada ônibus é o triplo de cada van, qual a melhor alternativa para o aluguel desses transportes?

Cada um dos problemas acima pode ser modelado por uma equação linear de variáveis inteiras em duas incógnitas do tipo $a \cdot x + b \cdot y = c$ com a, b e $c \in \mathbb{Z}$. Ao propor tais problemas a escolha dos coeficientes pode ser feita de modo a englobar todas as nuances possíveis, desde problemas que não apresentam solução até aqueles cuja infinitas soluções são submetidas a certas restrições ou limites.

Equações do tipo acima são chamadas Diofantinas devido sua aparição e estudo na obra *Arithmetica* de Diofanto. Um sábio brilhante que viveu por volta de 250 A.C. na cidade de Alexandria no Egito. Essa coleção de treze livros dos quais somente seis conseguiram sobreviver ao tempo e às destruições de tantas bibliotecas na antiguidade, possui ênfase na aritmética dos problemas determinados e indeterminados, o que faz dessa obra um ponto de referência na evolução das ideias matemáticas.

Diofanto teve uma influência maior sobre a teoria moderna dos números do que qualquer outro algebrista grego não geométrico. Em particular, Fermat foi levado ao seu célebre *último teorema* (veja [5]), quando procurou generalizar um problema que tinha lido na Arithmetica de Diofanto: dividir um dado quadrado em dois quadrados.

Definição 3.2.1. *Uma equação do tipo $a \cdot x + b \cdot y = c$ onde a, b e $c \in \mathbb{Z}$ é chamada equação diofantina linear a duas incógnitas.*

Existe algum processo ou algoritmo que podemos usar na tentativa de descobrir as soluções de tal equação?

Grande parte da resposta a essa pergunta é apresentada pelo próximo teorema. As demonstrações seguintes fundamentaram-se em [10].

Teorema 3.2.1. *A equação diofantina linear $a \cdot x + b \cdot y = c$ possui soluções inteiras se, e somente se $(a, b)|c$. Se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (\frac{b}{d})k$$
$$y = y_0 - (\frac{a}{d})k$$

onde k é um inteiro e $d = (a, b)$.

Demonstração. Suponha que a equação possua solução (x_0, y_0), assim, $a \cdot x_0 + b \cdot y_0 = c$. Como $d|a$ e $d|b$, temos que $d|c$.
Agora vamos provar a implicação recíproca. Como $d = (a, b)$, podemos escrevê-lo como $d = a \cdot x' + b \cdot y'$. Suponhamos que $d|c$, então podemos escrever $c = d \cdot q$. As duas últimas expressões nos dão $c = d \cdot q = (a \cdot x' + b \cdot y')q = a(x' \cdot q) + b(y' \cdot q)$, o que nos mostra uma solução da equação diofantina $x = x' \cdot q$ e $y = y' \cdot q$.

Para mostrar a segunda parte, verificaremos que dada uma solução particular (x_0, y_0), os pares da forma

$$x = x_0 + (\frac{b}{d})k$$
$$y = y_0 - (\frac{a}{d})k$$

são soluções pois

$$a \cdot x + b \cdot y = a(x_0 + (\frac{b}{d})k) + b(y_0 - (\frac{a}{d})k) = a \cdot x_0 + b \cdot y_0 = c$$

Então dada uma solução particular qualquer, podemos gerar a partir dela infinitas soluções. Agora vamos mostrar que todas as soluções são desse tipo.

Seja (x, y) uma solução genérica, isto é, $a \cdot x + b \cdot y = c$. Mas como $a \cdot x_0 + b \cdot y_0 = c$, obtemos subtraindo membro a membro, $a(x - x_0) + b(y - y_0) = 0$, ou seja, $a(x - x_0) = b(y_0 - y)$. Vamos dividir os dois membros dessa equação por $d = (a, b)$, ficamos com $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$. Isso nos mostra que $\frac{b}{d}|\frac{a}{d}(x - x_0)$, mas $(\frac{a}{d}, \frac{b}{d}) = 1$, o que nos dá $\frac{b}{d}|(x - x_0)$. Portanto, existe um inteiro k tal que $(x - x_0) = (\frac{b}{d})k$ ou seja, $x = x_0 + (\frac{b}{d})k$. Agora, substituindo em $a(x - x_0) = b(y_0 - y)$ vem $y = y_0 - (\frac{a}{d})k$, o que conclui a demonstração. □

Vamos retornar aos problemas no início dessa seção.
Cada arrumação dos 20 carros numa dada quantidade x de filas com 3 carros cada e y filas de 5 carros equivale a uma solução inteira e positiva da equação diofantina linear $3 \cdot x + 5 \cdot y = 20$. Como $(3, 5) = 1$ e $1|20$, essa equação possui infinitas soluções. Não é difícil encontrar uma solução particular visto que os valores numéricos são baixos. No caso mais geral, dada a equação $a \cdot x + b \cdot y = c$, utilizamos o processo das divisões sucessivas de Euclides para escrever o MDC, $d = (a, b)$, como combinação linear inteira $a \cdot x_0 + b \cdot y_0 = d$, e então multiplicamos ambos os lados dessa combinação linear pelo inteiro $\frac{c}{d}$. Com esse procedimento nós conseguimos uma solução particular.
Continuando nosso exemplo, após uma observação, conseguimos uma solução particular por tentativas $x_0 = 5$ e $y_0 = 1$. Portanto, uma expressão da solução geral é da forma $x = 5 + (\frac{5}{1})k$ e $y = 1 - (\frac{3}{1})k$. Como estamos interessados nos valores positivos fazemos $5 + 5k > 0$ e $1 - 3k > 0$, o que implica $-1 < k < \frac{1}{3}$. O único valor possível inteiro é $k = 0$, o que nos diz ser $(5, 1)$ a única solução em inteiros positivos desse problema.

Já o segundo problema, se chamarmos de x e y respectivamente as quantidades de quadras para jogos de basquete e vôlei, sua modelagem é dada por $10 \cdot x + 12 \cdot y = 80$. Como $(10, 12) = 2$, e claro, $2|80$, essa equação possui solução. Aqui também não é difícil perceber uma solução particular (qualquer uma serve) $x_0 = 8$ e $y_0 = 0$. Todas as soluções inteiras e positivas são dadas por $x = 8 + 6k$ e $y = -5k$ e sujeitas às restrições $8 + 6k \geqslant 0$ e $-5k \geqslant 0$. O valor de k deve ser um inteiro situado em $-\frac{4}{3} \leqslant k \leqslant 0$. Os únicos valores possíveis são $k = -1$ ou $k = 0$, o que nos dá as soluções $(2, 5)$ ou $(8, 0)$.
Se fossem 77 alunos, a equação $10 \cdot x + 12 \cdot y = 77$ não possuiria solução inteira pois $(10, 12) \nmid 77$ ou simplesmente porque a soma de dois inteiros pares não dá como resultado um ímpar.

Caso os problemas estejam submetidos a outras exigências sobre as soluções, basta encontrar suas expressões gerais e submetê-las às restrições tentando encontrar valores para os inteiros k que satisfaçam-nas.

A teoria das equações diofantinas está estreitamente relacionada com as congruências lineares, objeto do nosso próximo estudo.

Definição 3.2.2. *Chamamos de* congruência linear *aquela do tipo* $a \cdot x \equiv b(mod\ m)$ *em que* $a, b, m \in \mathbb{Z}$, $m > 0$ *e* x *é uma variável inteira.*

Uma congruência linear $a \cdot x \equiv b(mod\ m)$ possui solução x_0 se $m|(a \cdot x_0 - b)$, isto é, se existe um inteiro y tal que $a \cdot x_0 - b = m \cdot y$, ou seja, $a \cdot x_0 - m \cdot y = b$. Portanto, as

soluções de tais congruências também são soluções de uma equação diofantina.
A recíproca dessas implicações é imediata, evidenciando o conceito de *equação diofantina equivalente* a uma congruência linear.

Teorema 3.2.2. *A congruência linear $a \cdot x \equiv b(mod\ m)$ possui solução se, e somente se $(a, m)|b$. Nos casos em que existem soluções, há exatamente $d = (a, m)$ soluções incongruentes módulo m.*

Demonstração. Sabemos que o inteiro x é solução de $a \cdot x \equiv b(mod\ m)$ se, e somente se existe um inteiro y tal que $a \cdot x - m \cdot y = b$. Essa equação diofantina possui soluções $x = x_0 - (\frac{m}{d})k$ e $y = y_0 - (\frac{a}{d})k$ em que (x_0, y_0) é uma solução particular se, e somente se $d|b$, $d = (a, m)$.
Assim, $x = x_0 - (\frac{m}{d})k$ é uma expressão das infinitas soluções da congruência dada.
Vamos descobrir quais as condições em que $x_1 = x_0 - (\frac{m}{d})k_1$ e $x_2 = x_0 - (\frac{m}{d})k_2$ são congruentes módulo m.
Se $x_1 \equiv x_2(mod\ m)$ então $x_0 - (\frac{m}{d})k_1 \equiv x_0 - (\frac{m}{d})k_2(mod\ m)$. Isso implica que $(\frac{m}{d})k_1 \equiv (\frac{m}{d})k_2(mod\ m)$, e como $(\frac{m}{d})|m$ temos $(\frac{m}{d}, m) = \frac{m}{d}$, o que nos permite o cancelamento de $\frac{m}{d}$, resultando $k_1 \equiv k_2(mod\ d)$. Isso nos mostra que soluções incongruentes serão obtidas ao tomarmos valores incongruentes módulo d para o inteiro k, isto é, quando ele percorre um sistema completo de resíduos. □

Definição 3.2.3. *Duas soluções da congruência $a \cdot x \equiv b(mod\ m)$ são distintas quando forem incongruentes módulo m.*

Na demonstração anterior, fazendo $k = 0, -1, -2 \ldots -(d-1)$, as únicas soluções incongruentes da congruência acima são dadas por $x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$.

Definição 3.2.4. *Se a congruência $a.x \equiv 1(mod\ m)$ possui solução $\overline{a}$, essa será chamada de inverso de a módulo m.*

Não esqueçamos que existe inverso para a congruência acima se, e somente se $(a, m)|1$, e, naturalmente, quando m é primo há inverso quando a não é divisível por m.

Uma questão curiosa surge quando nos perguntamos sobre as condições em que o inverso de a é ele próprio. Quando m é primo é fácil a resposta.

Proposição 3.2.1. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso, isto é, $a^2 \equiv 1(mod\ p)$ se, e somente se, $a \equiv 1(mod\ p)$ ou $a \equiv (p-1)(mod\ p)$.*

Demonstração. Se a é o seu próprio inverso, então $a \cdot a \equiv 1(mod\ p)$, o que significa que $p|(a^2 - 1)$. Mas se $p|(a + 1)(a - 1)$, sendo p primo, $p|(a - 1)$ ou $p|(a + 1)$, o que implica $a \equiv 1(mod\ p)$ ou $a \equiv (-1)(mod\ p)$. Como $p - 1 \equiv (-1)(mod\ p)$, e todas as passagens acima são reversíveis, a demonstração está concluída. □

3.3 Teorema Chinês do Resto

Há, desde a antiguidade, problemas curiosos sobre a determinação de certas quantidades inteiras que satisfazem ao mesmo tempo várias condições de divisibilidade. Na China, por volta do século um de nossa era, o matemático Sun-Tsu (tradução quase onomatopeica) propôs a seguinte questão:

> Qual é o número que deixa restos 2, 3 e 2 quando dividido respectivamente por 3, 5 e 7?

A tradução, na linguagem das congruências para esse problema pode ser expressa nas condições seguintes:

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 5)$$
$$x \equiv 2(mod\ 7)$$

No ambiente da sala de aula é conveniente apresentar esse padrão de construção através de problemas mais próximos de situações reais, tal como o exemplo seguinte.

Exemplo 3.3.1. *Três satélites passarão sobre Fortaleza amanhã. O primeiro à* $1h$ *da madrugada, o segundo às* $4h$ *e o terceiro às* $8h$ *da manhã. Cada satélite tem um período diferente. O primeiro leva* 13 *horas para completar uma volta em torno da Terra, o segundo* 15 *horas e o terceiro* 19 *horas. Quanto tempo decorrerá, a partir da meia noite de hoje até que os satélites passem ao mesmo tempo sobre Fortaleza?*

O professor pode ainda, utilizando o gosto pela descoberta e desafio de alguns alunos, utilizar técnicas mais desafiadoras para motivar a apresentação desse assunto, como no próximo exemplo.

Exemplo 3.3.2. *Alberto pede a Roberto que pense num número inteiro positivo até* 1000*, depois faça as divisões desse número por* 7*,* 11 *e* 13 *e informe os restos obtidos respectivamente. Nessas condições, como pode Aberto obter o número pensado pelo amigo?*

Para responder tais questões vamos começar estudando os procedimentos de resolução de alguns sistemas de congruências lineares descritos na forma comumente conhecida por *Teorema Chinês do Resto.*

Teorema 3.3.1 (Teorema Chinês do Resto)**.** *O sistema de congruências lineares*

$$\begin{aligned} a_1 \cdot x &\equiv c_1 (mod\ m_1) \\ a_2 \cdot x &\equiv c_2 (mod\ m_2) \\ &\dots \\ a_r \cdot x &\equiv c_r (mod\ m_r) \end{aligned}$$

onde $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para* $i \neq j$ *e* $c_i \in \mathbb{Z}$ *possui uma única solução módulo* $M = m_1 \cdot m_2 \dots m_r$.

Demonstração. Uma consequência imediata de $(a_i, m_i) = 1$ é que cada congruência linear $a_i \cdot x \equiv c_i (mod\ m_i)$ possui uma única solução que denotaremos por b_i, isto é, $a_i \cdot b_i \equiv c_i (mod\ m_i)$.
Seja $M = m_1 \cdot m_2 \dots m_r$. Definamos os números Y_i como produto de todos dos fatores m_k tais que $k \neq i$, isto é, $Y_i = \prod_{k=1\ k\neq i}^{r} m_k$. Como $(m_i, m_j) = 1$ para $i \neq j$, temos de imediato $(Y_i, m_i) = 1$. Essa última condição nos garante que cada congruência $Y_i \cdot x \equiv 1 (mod\ m_i)$ possui uma única solução $\overline{y_i}$. Assim, $Y_i \cdot \overline{y_i} \equiv 1 (mod\ m_i)$ para $i = 1, 2 \dots r$.
Vamos mostrar explicitamente uma solução X do sistema de congruências.
O número $X = b_1 \cdot Y_1 \cdot \overline{y_1} + b_2 \cdot Y_2 \cdot \overline{y_2} + \dots + b_r \cdot Y_r \cdot \overline{y_r}$ é uma solução de cada uma das congruências do sistema acima e o motivo é bem simples, o fator m_i está presente em cada um dos termos Y_j acima, exceto no Y_i. Assim cada um daqueles é divisível por m_i, ou seja, congruente a zero módulo m_i. De modo simbólico,

$$a_i.X = a_i.b_1.Y_1.\overline{y_1} + a_i.b_2.Y_2.\overline{y_2} + \dots + a_i.b_r.Y_r.\overline{y_r} \equiv a_i.b_i.Y_i.\overline{y_i} (mod\, m_i) \equiv a_i.b_i.1 \equiv c_i (mod\, m_i)$$

(usamos o fato de que $Y_i \cdot \overline{y_i} \equiv 1 (mod\ m_i)$ e $a_i \cdot b_i \equiv c_i (mod\ m_i)$).
Vamos mostrar que essa solução é única módulo $M = m_1 \cdot m_2 \dots m_r$. Se $\overline{X}$ é uma solução qualquer do sistema, então
$a_i \cdot \overline{X} \equiv c_i \equiv a_i \cdot X (mod\ m_i)$ e como $(a_i, m_i) = 1$, cancelamos o fator a_i ficando com $\overline{X} \equiv X (mod\, m_i)$. Logo, $m_i | (\overline{X} - X)$ para todo $i = 1, 2 \dots r$. Assim, $(\overline{X} - X)$ é um múltiplo de cada m_i, logo ele é divisível por $[m_1, m_2, \dots, m_r]$. Mas o fato de ser $(m_i, m_j) = 1$ para $i \neq j$ nos diz também que $[m_1, m_2, \dots, m_r] = m_1 \cdot m_2 \dots m_r = M$. Do anteriormente exposto temos $\overline{X} \equiv X (mod\ M)$.
Mostramos assim que qualquer solução do sistema é congruente módulo M à solução dada. □

Vamos agora resolver as três questões propostas no início dessa seção.

No problema de Sun-Tsu, a solução b_i de cada congruência é encontrada facilmente pois é igual a cada c_i. Para as congruências

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 5)$$
$$x \equiv 2(mod\ 7)$$

temos as soluções $b_1 = 2$; $b_2 = 3$ e $b_3 = 2$. Do número $M = 3 \cdot 5 \cdot 7$ temos $Y_1 = 5 \cdot 7$; $Y_2 = 3 \cdot 7$ e $Y_3 = 3 \cdot 5$. Para encontrar os inversos desses últimos números resolvemos as equações seguintes,

$$5 \cdot 7 \cdot x \equiv 1(mod\ 3)$$
$$3 \cdot 7 \cdot x \equiv 1(mod\ 5)$$
$$3 \cdot 5 \cdot x \equiv 1(mod\ 7)$$

que são equivalentes respectivamente a

$$2 \cdot x \equiv 1(mod\ 3)$$
$$x \equiv 1(mod\ 5)$$
$$x \equiv 1(mod\ 7)$$

Essas soluções são encontradas testando facilmente os elementos de cada sistema completo de resíduos módulo m_i (nos casos em que há muitos elementos a serem testados construímos uma equação diofantina linear equivalente à congruência e procuramos sua solução). Determinamos assim os inversos $\overline{y_1} = 2$, $\overline{y_2} = 1$ e $\overline{y_3} = 1$. A solução geral módulo $M = 105$ é dada por

$$X = 2(5 \cdot 7)2 + 3(3 \cdot 7)1 + 2(3 \cdot 5)1 = 140 + 63 + 30 = 233$$

Uma solução mínima positiva é obtida retirando-se múltiplos inteiros de 105, em outras palavras, como $233 \equiv 23(mod\ 105)$, a solução mínima é 23 e a solução geral é dada por $X = 23 + 105 \cdot k$ onde $k \in \mathbb{Z}$.

No segundo exercício, bem mais contextualizado, o pano de fundo é o mesmo. Suponha que seja T o tempo em horas a partir da meia-noite em que os três satélites aparecerão simultaneamente. Para o primeiro satélite esse tempo é escrito como $T = 1 + 13 \cdot P_1$ em que P_1 é a quantidade de seus períodos completos, já que ele volta para a mesma posição sobre a cidade. Para os outros dois satélites temos $T = 4 + 15 \cdot P_2$ e $T = 8 + 19 \cdot P_3$. Traduzindo para a notação de congruências,

$$T \equiv 1(mod\ 13)$$
$$T \equiv 4(mod\ 15)$$
$$T \equiv 8(mod\ 19)$$

A solução de cada equação individual é $b_1 = 1$, $b_2 = 4$ e $b_3 = 8$. O número $M = 13.15.19$ nos informa que devemos achar as soluções de

$$15 \cdot 19 \cdot x \equiv 1(mod\ 13)$$
$$13 \cdot 19 \cdot x \equiv 1(mod\ 15)$$
$$13 \cdot 15 \cdot x \equiv 1(mod\ 19)$$

Por conseguinte, são equivalentes respectivamente às congruências

$$12 \cdot x \equiv 1(mod\ 13)$$
$$7 \cdot x \equiv 1(mod\ 15)$$
$$5 \cdot x \equiv 1(mod\ 19)$$

cujas soluções $\overline{y_1} = 12$, $\overline{y_2} = 13$ e $\overline{y_3} = 4$ determinamos após verificação rápida dos conjuntos completos de restos de cada congruência módulo m_i (ou resolvendo a equação diofantina equivalente à congruência dada).
Uma solução módulo $M = 13 \cdot 15 \cdot 19 = 3705$ é

$$X = 1(15 \cdot 19)12 + 4(13 \cdot 19)13 + 8(13 \cdot 15)4 = 3420 + 12844 + 6240 = 22504$$

A solução mínima vem de $22504 \equiv 274(mod\ 3705)$ e é dada por $X_{min} = 274$ horas, isto é, 11 dias e 10 horas. Após transcorrido esse tempo, os três satélites novamente se encontrarão sobre a cidade. A solução geral é expressa, com K inteiro positivo, por $T = 274 + 3705 \cdot K$, horas após a meia noite.

Para justificar a resposta do terceiro exercício, seja N um número inteiro positivo e tomemos seus restos conhecidos nas divisões por 7, 11 e 13 respectivamente como r_7, r_{11} e r_{13}. Nesse caso temos $M = 7 \cdot 11 \cdot 13 = 1001$, $Y_1 = 11 \cdot 13 = 143$, $Y_2 = 7 \cdot 13 = 91$ e $Y_3 = 7 \cdot 11 = 77$.
As equações

$$143 \cdot x \equiv 1(mod\ 7)$$
$$91 \cdot x \equiv 1(mod\ 11)$$
$$77 \cdot x \equiv 1(mod\ 13)$$

são respectivamente equivalentes às

$$3 \cdot x \equiv 1(mod\ 7)$$
$$3 \cdot x \equiv 1(mod\ 11)$$
$$12 \cdot x \equiv 1(mod\ 13)$$

cujas soluções são $\overline{y_1} = 5$, $\overline{y_2} = 4$ e $\overline{y_3} = 12$. Logo o sistema

$$x \equiv r_7(mod\ 7)$$
$$x \equiv r_{11}(mod\ 11)$$
$$x \equiv r_{13}(mod\ 13)$$

tem por solução

$$X \equiv 143 \cdot 5 \cdot r_7 + 91 \cdot 4 \cdot r_{11} + 77 \cdot 12 \cdot r_{13} \equiv 715 \cdot r_7 + 364 \cdot r_{11} + 924 \cdot r_{13}(mod\ 1001)$$

Basta então, ao professor fazer as operações anteriores com os restos fornecidos e, se necessário, retirar múltiplos de 1001 do resultado até encontrar o menor número positivo que satisfaça essa condição da congruência.

4 SOMAS DE DOIS QUADRADOS

4.1 Primos como Somas de Dois Quadrados

Qualquer egresso do ensino médio que demonstre mínimo interesse pela Matemática ou mesmo pelos aspectos importantes da história de nossa evolução científica deve lembrar do *"Último Teorema de Fermat"*. Seu enunciado simples que afirma não existirem soluções inteiras da equação $x^n+y^n = z^n$ para $n > 2$ resistiu a investidas sérias durante muitos anos por muitos cérebros geniais até sua completa demonstração após muito tempo de trabalho pelo inglês Andrew Wiles que conseguiu o feito utilizando como base uma conjectura feita pelos matemáticos Yutaka Taniyama e Goro Shimura (conhecida como conjectura Taniyama-Shimura) em 1995. Pierre de Fermat, um advogado francês do século XVII, não possuía menos talento para a Matemática que para a Jurisprudência. Trabalhava como magistrado na província de Toulousse e nas horas vagas se dedicava à Matemática. Seu interesse em estudar as propriedades dos números inteiros não era compartilhada com entusiasmo por outros matemáticos o que deve ter contribuído para ele nunca ter publicado formalmente seus resultados e apenas apareciam nas suas cartas a alguns poucos colegas que compartilhavam de sua atenção. Lembremos que a atividade desses estudiosos, num período em que não existiam revistas científicas, tinha por base círculos de discussão e uma constante troca de correspondências. Um bom texto sobre Fermat está em [5].

Entre vários outros resultados, há o *"Pequeno Teorema de Fermat"* o qual diz que $a^p - a$ é divisível por p para todos a inteiro e p primo. Em linguagem mais atual podemos afirmar que $a^p \equiv a(mod\ p)$.

Pela grande importância de Fermat no desenvolvimento do moderno campo de estudos que atualmente é conhecido por "teoria dos números", nessa etapa de nosso trabalho apresentaremos uma resposta a um de seus mais famosos resultados, isto é, vamos cons-

truir argumentos que nos deem respostas à pergunta: *Quais números podem ser escritos como somas de dois quadrados?*

Nossa tarefa passará pelo reconhecimento de que os primos positivos das formas $4m+1$ podem ser escritos como somas de quadrados enquanto que aqueles outros primos ímpares da forma $4m+3$ não. A demonstração dada mais adiante deve-se a Roger Heath-Brown em 1971 cuja publicação aparece na obra "*Fermat's two Squares Theorem*" de 1984. É uma demostração belíssima que usa conceitos geométricos e aplicações. Para mais detalhes ver [1]. É interessante observar que se exigirmos que tais números citados no início sejam quadrados perfeitos, o assunto poderá ser estudado através dos ternos pitagóricos, que são trios de números inteiros que satisfazem as condições do *Teorema de Pitágoras*.

Nesse capítulo, a fim de não tornar cansativa ou até pedante a notação algébrica, omitiremos na maior parte da vezes o sinal indicativo da multiplicação mas cuja presença ficará bem percebida nas expressões.

Vamos primeiramente observar que dentre os números primos positivos p, o único par é 2 e que os **primos ímpares** podem ser classificados, observando sua divisão euclidiana por 4 de acordo com as condições:

- Nenhum número primo deixa resto zero por razões óbvias.
- Alguns deixam resto 1, e nesse caso podemos escrevê-los como $p = 4m + 1$.
- Nenhum deixa resto 2, pois nesse caso teríamos $p = 4m + 2 = 2(2m + 1)$, e então, p seria par.
- Alguns deixam resto 3, e nesse caso podemos escrevê-los como $p = 4m + 3$.

Resumindo, todo primo pertence a uma das três classes: $p = 2$ ou p é impar e assume uma das formas $4m + 1$ ou $4m + 3$.

Agora vamos introduzir alguns fatos interessantes e úteis.

Proposição 4.1.1. *O conjunto dos números do tipo* $4m+1$ *é fechado para a multiplicação. Em outras palavras, o produto de inteiros da forma* $4m+1$ *é ainda um número dessa forma.*

Demonstração. Basta observar que
$(4m + 1)(4m' + 1) = 16mm' + 4m + 4m' + 1 = 4(4mm' + m + m') + 1 = 4m'' + 1.$ □

Proposição 4.1.2. *Há infinitos primos positivos da forma* $p = 4m + 3$.

Demonstração. Suponhamos por absurdo que haja uma quantidade finita desses números $p_1 < p_2 < \ldots < p_k$ com p_k o maior deles. Definamos $N_k = 2^2 \cdot 3 \cdot 5 \ldots p_k - 1$ como o produto de todos os primos de 2 (somente esse ao quadrado) até p_k, menos uma unidade. É claro que o produto acima é par, assim determina N_k ímpar.
Agora nos perguntamos: N_k é da forma $4m + 1$ ou $4m + 3$?
Observemos que $N_k = 4 \cdot 3 \cdot 5 \ldots p_k - 1$, ou seja, $N_k \equiv -1(mod\ 4)$, isto é, $N_k \equiv 3(mod\ 4)$ e, portanto, assume a forma $N_k = 4m + 3$.
Se N_k só contivesse fatores primos da forma $4m + 1$ ele não poderia ser da forma $4m + 3$ em vista da proposição acima. Assim, N_k deve possuir ao menos um fator $p_{k'}$ da forma $4m+3$. Mas esse fator $p_{k'}$, ao dividir ambos, N_k e o produto $2^2 \cdot 3 \cdot 5 \ldots p_k$, divide também 1, o que é um absurdo. Assim, a hipótese da finitude dos números primos da forma $4m+3$ é falsa. □

Teorema 4.1.1 (Fermat)**.** *Todo número primo da forma* $p = 4m + 1$ *pode ser escrito como soma de dois quadrados.*

Demonstração. Essa prova proposta por Heath-Brown contém três involuções, isto é, transformações $f : \mathbb{Z}^3 \to \mathbb{Z}^3$ tais que $f \circ f = I$.
Dado um número primo positivo p da forma $4m + 1$ definamos o conjunto
$\mathbb{S} = \{(x, y, z) \in \mathbb{Z}^3;\ 4xy + z^2 = p,\ x > 0,\ y > 0\}$ formado pelas ternas ordenadas (x, y, z) que fornecem p de acordo com a lei de formação $4xy + z^2 = p$. Afirmamos que esse conjunto é finito. De fato, como $x \geqslant 1$ e $y \geqslant 1$, devemos ter $x \leqslant \dfrac{p}{4}$ e $y \leqslant \dfrac{p}{4}$, pois, caso contrário, teríamos (supondo, por exemplo) de $x > \dfrac{p}{4}$ e $y \geqslant 1$, $xy > \dfrac{p}{4}$ e assim, $4xy > p$, o que nos daria $4xy + z^2 > p$, um absurdo. Assim existe somente uma quantidade finita de valores possíveis para x e y. E fixados esses números, só há, no máximo, dois valores para z devido $z^2 = p - 4xy$, um positivo e outro negativo.

- A primeira involução é dada por $f_1 : \mathbb{S} \to \mathbb{S}$ tal que $f_1(x, y, z) = (y, x, -z)$, em palavras, f_1 permuta os valores de x e y e troca o sinal de z. É bem evidente que $f_1 \circ f_1 = I_{\mathbb{S}}$ pois $f_1 \circ f_1(x, y, z) = f_1(y, x, -z) = (x, y, -(-z)) = (x, y, z) = I(x, y, z)$. Uma característica de f_1 é que essa função não possui pontos fixos, pois $f_1(x, y, z) = (x, y, z)$, implica que $(y, x, -z) = (x, y, z)$, isto é, $x = y$ e $z = 0$, o que nos dá $p = 4xy$ pois $z^2 = 0$. Isso é impossível visto que p não é par. Além disso, f_1 leva as soluções que pertencem a $T = \{(x, y, z) \in \mathbb{S}; z > 0\}$ nas soluções de $T' = \{(x, y, z) \in \mathbb{S}; z < 0\}$. Também, f_1 inverte os sinais de $x - y$ e de z; logo, leva as soluções que pertencem a

$U = \{(x, y, z) \in \mathbb{S}; (x-y)+z > 0\}$ nas soluções em $U' = \{(x, y, z) \in \mathbb{S}; (x-y)+z < 0\}$, para isso basta verificar que não há solução com $(x - y) + z = 0$, pois acarretaria $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$, o que é um absurdo já que p não é quadrado perfeito.

Resumindo, a função f_1 leva os conjuntos T e U em seus complementos, como também permuta os elementos de $T\backslash U$ com $U\backslash T$, isto é, existe o mesmo número de soluções em T que não estão em U tanto quanto de soluções em U que não estão em T. Assim, ***T* e *U* têm a mesma quantidade de elementos**. Veja a figura 1.

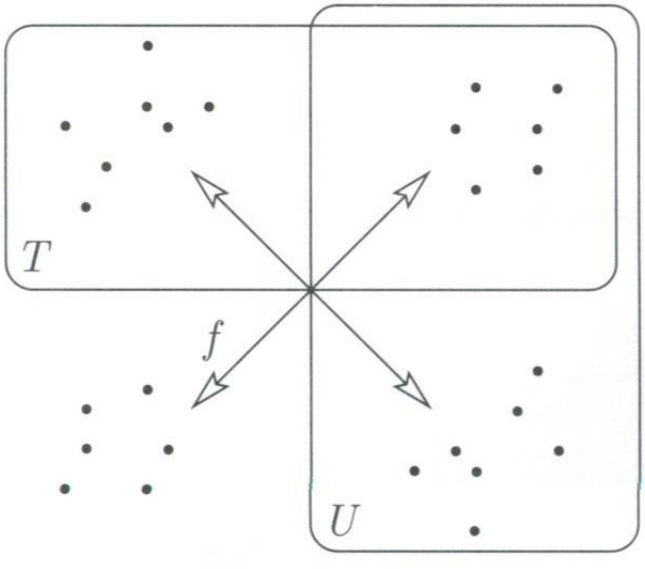


Figura 1: Involução dada pela aplicação f_1

- Agora vamos definir a segunda involução no conjunto
  $U = \{(x, y, z) \in \mathbb{S}; (x - y) + z > 0\}$ dada por $f_2 : U \to U$ tal que $f_2(x, y, z) = (x - y + z, y, 2y - z)$. Vamos verificar que essa função é, de fato, bem definida. Isto é, leva elementos de U em U.

  Seja uma solução (x, y, z) em U. Então sua imagem $(x - y + z, y, 2y - z)$ é tal que $(x - y) + z > 0$, $y > 0$ e $4(x - y + z)y + (2y - z)^2 = 4xy + z^2$, de modo que $f_2(x, y, z) \in \mathbb{S}$ e, mais especificamente, $(x - y + z) - y + (2y - z) = x > 0$, isto é, $f_2(x, y, z) \in U$.

  Também f_2 é uma involução, pois $f_2 \circ f_2(x, y, z) = f_2(x - y + z, y, 2y - z) = ((x - y + z) - y + (2y - z), y, 2y - (2y - z)) = (x, y, z) = I(x, y, z)$.

  Finalmente, f_2 possui um ponto fixo, pois $f_2(x, y, z) = (x, y, z)$ acarreta $(x - y + z, y, 2y - z) = (x, y, z)$ e $y = z$. Mas então, $p = 4xy + z^2 = 4xy + y^2 = (4x + y)y$. Como a única possibilidade para y é ser igual a 1 (caso contrário p seria composto,

uma contradição com o fato de p ser primo), podemos assumir que $y = z = 1$ tornando $p = 4x + 1$ e daí, $x = \dfrac{p-1}{4}$. Isso mostra que f_2 possui o ponto fixo $(\dfrac{p-1}{4}, 1, 1)$.

A conclusão que chegamos é da **quantidade ímpar de elementos em U** devido existir uma involução com exatamente um ponto fixo nesse conjunto.

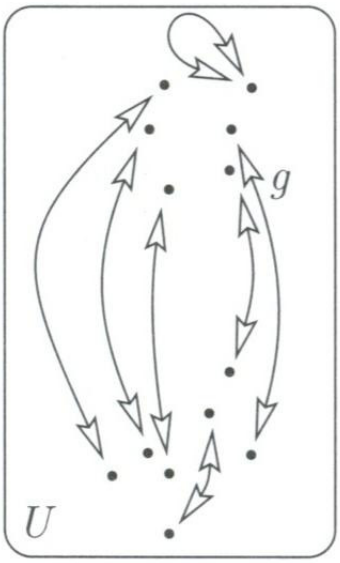
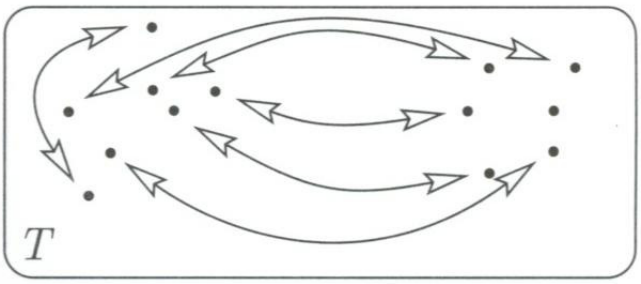


Figura 2: Involução dada pela aplicação f_2

- A terceira involução que estudaremos é aquela que permuta os elementos x e y sobre o conjunto T, isto é, $f_3 : T \to T$ tal que $f_3(x, y, z) = (y, x, z)$. Essa aplicação é bem definida e é uma involução pois dado $(x, y, z) \in T$, $f_3 \circ f_3(x, y, z) = f_3(y, x, z) = (x, y, z) = I(x, y, z)$. Tendo em mente que os conjuntos T e U possuem uma quantidade ímpar de elementos e que f_3 é uma involução sobre T, chegamos a conclusão que essa função deve possuir algum ponto fixo (ou mais propriamente, uma quantidade ímpar desses pontos. Veja a figura 3), isto é, deve existir algum $(x, y, z) \in T$ com $x = y$ tal que $p = 4xy + z^2 = 4x^2 + z^2 = (2x)^2 + z^2$ assim, nosso número primo escolhido no início dessa demonstração pode ser escrito como soma de dois quadrados.

□

Observe que a quantidade de pontos fixos de f_3 determina as formas de representação de p como soma de dois quadrados. Poderíamos cogitar a existência de vários modos de fazê-lo, mas na verdade essa maneira é única e pode ser vista em [9].



Em um conjunto finito de cardinalidade ímpar, toda involução apresenta um ponto fixo.

Figura 3: Involução dada pela aplicação f_3

Já sabemos que todo primo ímpar da forma 4m+1 é escrito como soma de dois quadrados. Mas o que podemos dizer sobre um inteiro qualquer? Quais condições deve satisfazer um inteiro positivo a fim de ser escrito daquela forma?

Esse é o assunto da próxima seção.

4.2 Inteiros como Somas de Dois Quadrados

Para ampliar a abordagem da seção anterior e incluir inteiros não necessariamente primos e desenvolver a análise das condições necessárias e suficientes que permitem sua representação como soma de dois quadrados, precisamos de alguns resultados prévios, tais como o seguinte lema, cuja demonstração encontra-se em [1].

Lema 4.2.1. *A equação $x^2 \equiv -1(mod\ p)$ possui duas soluções em $\{1, 2, \ldots, p-1\}$ quando p é primo da forma $4m+1$; uma solução quando $p = 2$ e nenhuma solução quando p é primo da forma $4m+3$.*

Demonstração. Para $p = 2$ basta tomar $x = 1$, pois $1^2 \equiv -1(mod\ 2)$. Para p ímpar, construímos a relação de equivalência no sistema de restos $\{1, 2, \ldots, p-1\}$ que é formada identificando cada elemento x com seu simétrico aditivo $-x$ e multiplicativo $\overline{x}$ em $\mathbb{Z}_p$. Assim, as classes de equivalência irão conter quatro elementos $\{x, -x, \overline{x}, -\overline{x}\}$ salvo nas condições em que alguns desses coincidirem. Vamos analisar essas condições.

- $x \equiv -x(mod\ p)$ é impossível para p ímpar pois isso implicaria $p|2x$. Mas como $(p, 2) = 1$ teríamos $p|x$ com $1 \leqslant x \leqslant p-1$, o que é impossível.

- $x \equiv \overline{x}(mod\ p)$ é equivalente a $x^2 \equiv 1(mod\ p)$. Para ver isso basta multiplicar ambos os termos da primeira congruência por x ou escrever o número 1 na segunda congruência como $x \cdot \overline{x}$ e cancelar o fator x primo com p. Aquela última congruência possui claramente a solução $x = 1$. Se y for outra solução da mesma congruência, então $y^2 \equiv 1(mod\, p)$, isto é, $p|(y^2-1)$ ou seja, $p|(y+1)(y-1)$. Assim, $y \equiv -1(mod\, p)$ ou $y \equiv 1(mod\, p)$. Como $p-1 \equiv -1(mod\, p)$, temos que a outra solução será $y = p-1$ em $\mathbb{Z}_p$.
  Analisando as possibilidades das soluções possíveis temos:

  1. Se $x = 1$, então $-x = p-1$, pois $1 + (p-1) = p \equiv 0(mod\ p)$. Também $\overline{x} = 1$ e $-\overline{x} = -1 \equiv p-1(mod\ p)$.
  2. Se $x = p-1$, então $-x = 1$, $\overline{x} = p-1$ e $-\overline{x} = -(p-1) = -p+1 \equiv 1(mod\ p)$.

  Em qualquer caso temos que a classe de equivalência gerada é $\{1, p-1\}$.

- $x \equiv -\overline{x}(mod\, p)$ é equivalente a $x^2 \equiv -1(mod\, p)$. Essa equação pode não ter solução (veja por exemplo, $x^2 \equiv -1(mod\ 7)$ não possui solução em $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$).

Caso possua uma solução x_0 e se y_0 seja outra solução, então $y_0^2 \equiv x_0^2 \equiv -1(mod\ p)$ e assim, $p|(x_0^2 - y_0^2)$, ou seja, $p|(x_0 - y_0)$ ou $p|(x_0 + y_0)$. Das congruências $y_0 \equiv x_0(mod\ p)$ ou $y_0 \equiv -x_0 \equiv p - x_0(mod\ p)$ vem as possíveis soluções: x_0 ou $p - x_0$.
Analisando ambas as situações:

1. Se $x = x_0$, então $-x = p - x_0$ pois $x_0 + p - x_0 = p \equiv 0(mod\ p)$. Também, $\overline{x} = -x_0 \equiv p - x_0$ e $-\overline{x} = x_0$.
2. Se $x = p - x_0$, então $-x = x_0$, $\overline{x} = -p + x_0 \equiv x_0$ e $-\overline{x} = p - x_0$.

Em ambos os casos temos a classe de equivalência $\{x_0, p - x_0\}$.

- os casos $-x \equiv \overline{x}(mod\ p)$, $-x \equiv -\overline{x}(mod\ p)$ e $\overline{x} \equiv -\overline{x}(mod\ p)$ são equivalentes aos casos $x \equiv -\overline{x}(mod\ p)$, $x \equiv \overline{x}(mod\ p)$ e $x \equiv -x(mod\ p)$. Para ver isso basta multiplicar as congruências dadas por -1, -1 e x^2 respectivamente.

O conjunto $\{1, 2, \ldots, p-1\}$ tem $p-1$ elementos, uma quantidade par e nós o particionamos em quádruplas (classes de equivalência com quatro elementos) mais um ou dois pares (classes de equivalência com dois elementos). Para $p = 4m + 3$, ou seja, $p - 1 = 4m + 2$, obtemos somente o único par $\{1, p - 1\}$; o resto são quádruplas e, assim, $s^2 \equiv -1(mod\ p)$ não tem solução. Para $p = 4m + 1$, ou seja, $p - 1 = 4m$, tem que existir o segundo par, e ele contém as duas soluções de $s^2 \equiv -1(mod\ p)$ que estávamos procurando. □

Exemplo 4.2.1. *Para $p = 11$ (p da forma $4m + 3$) a partição é $\{1, 10\}$, $\{2, 9, 6, 5\}$, $\{3, 8, 4, 7\}$.*

Exemplo 4.2.2. *Para $p = 13$ (p da forma $4m + 1$) a partição é $\{1, 12\}$, $\{2, 11, 7, 6\}$, $\{3, 10, 9, 4\}$, $\{5, 8\}$. O par $\{5, 8\}$ fornece as soluções de $x^2 \equiv -1(mod\ 13)$.*

Agora podemos demonstrar o seguinte resultado

Teorema 4.2.1. *Um número natural N pode ser representado como uma soma de dois quadrados se, e somente se, todo fator primo da forma $4m + 3$ aparece com expoente par na decomposição de N em primos.*

Demonstração. Essa primeira parte da demonstração encontra-se em [1]. Para facilitar a discussão, chamaremos um inteiro n de *representável* quando ele puder ser escrito como soma de dois quadrados, isto é, $n = x^2 + y^2$ para algum $x, y \in \mathbb{Z}$. Observemos inicialmente alguns resultados básicos

- Os inteiros 1 e 2 são representáveis pois $1 = 1^2 + 0^2$ e $2 = 1^2 + 1^2$.

- Já mostramos anteriormente que todo primo da forma $4m + 1$ é representável.
- Se dois números $n_1 = a_1^2 + b_1^2$ e $n_2 = a_2^2 + b_2^2$ são representáveis, então seu produto é representável. Pois $n_1 n_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = a_1^2 a_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + b_1^2 b_2^2 = (a_1 a_2)^2 + 2a_1 a_2 b_1 b_2 + (b_1 b_2)^2 + (a_1 b_2)^2 - 2a_1 a_2 b_1 b_2 + (a_2 b_1)^2 = (a_1 a_2 + b_1 b_2)^2 + (a_1 b_2 - a_2 b_1)^2$.
- Se um inteiro $n = a^2 + b^2$ é representável então seu produto por qualquer inteiro ao quadrado é representável pois $nz^2 = (a^2 + b^2)z^2 = (az)^2 + (bz)^2$.

Seja a decomposição em fatores primos do número $N = 2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r} \cdot q_1^{\beta_1} \dots q_s^{\beta_s}$, onde cada $p_i \equiv 1 (mod\ 4)$ e $q_j \equiv 3 (mod\ 4)$.
O produto $2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r}$ é representável pois é formada por produtos de números representáveis. Como cada expoente β_j é par então podemos escrever $\beta_j = 2\beta'_j$, e assim, $N = 2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r} (q_1^{\beta'_1} \dots q_s^{\beta'_s})^2$ é representável por ser o produto de uma parte representável pelo quadrado de um inteiro.
Optamos por usar na prova da implicação recíproca o argumento utilizado em [10].
Vamos supor que $N = 2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r} \cdot q_1^{\beta_1} \dots q_s^{\beta_s}$ seja representável e que algum β_j seja ímpar. Sem perda de generalidade podemos assumir β_1 ímpar. Seja $d = (a, b)$ onde $N = a^2 + b^2$, então $a = dk_1$ e $b = dk_2$ com $(k_1, k_2) = 1$. Daí temos

$$N = 2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r} \cdot q_1^{\beta_1} \dots q_s^{\beta_s} = a^2 + b^2 = (dk_1)^2 + (dk_2)^2 = d^2(k_1^2 + k_2^2) = d^2 k$$

Como estamos supondo β_1 ímpar, ao dividirmos N por d^2, β_1 será diminuído de uma quantidade par, determinando que o expoente de q_1 em k ainda será ímpar. Logo, $q_1 | k$ e como $(k_1, k_2) = 1$ podemos concluir que $(q_1, k_1) = (q_1, k_2) = 1$, pois admitindo que $(q_1, k_1) = q_1$, isto é, $q_1 | k_1$, e como $q_1 | k$, teríamos de $k = k_1^2 + k_2^2$, $q_1 | k_2^2$, logo $q_1 | k_2$ pois q_1 é primo. Uma contradição com o fato de $(k_1, k_2) = 1$.
Retomando o fato de $(q_1, k_1) = (q_1, k_2) = 1$, logo existe x tal que a congruência $k_1 \cdot x \equiv k_2 (mod\ q_1)$ admite solução e, portanto

$$0 \equiv k \equiv k_1^2 + k_2^2 \equiv k_1^2 + k_1^2 \cdot x^2 \equiv k_1^2(1 + x^2) (mod\ q_1)$$

Como $q_1 \nmid k_1^2$, decorre então $x^2 + 1 \equiv 0 (mod\ q_1)$, ou seja, $x^2 \equiv -1 (mod\ q_1)$ com $q_1 \equiv 3 (mod\ 4)$. Essa congruência não possui solução em virtude do Lema anterior. Assim, a hipótese de algum β_j ser ímpar conduziu a uma contradição. Portanto todo expoente β_j deve ser par. □

Por fim, completaremos essa apresentação com o seguinte resultado da infinitude dos primos da forma $4n + 1$. Mas antes precisaremos do lema seguinte.

Lema 4.2.2. *Nenhum número da forma* $4m + 3$ *pode ser escrito como soma de dois quadrados.*

Demonstração. O quadrado de qualquer número par é $(2k)^2 = 4k^2 \equiv 0(mod\ 4)$, enquanto que o quadrado de um ímpar, $(2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 \equiv 1(mod\ 4)$. Assim qualquer soma de dois quadrados é congruente apenas a $0 + 0 = 0$, $0 + 1 = 1$ ou $1 + 1 = 2$ módulo 4. □

Proposição 4.2.1. *Há infinitos primos da forma* $4m + 1$.

Demonstração. Suponha por absurdo que exista apenas uma quantidade finita desses números, sendo p_k seu maior elemento. Definamos o número $M_k = (3 \cdot 5 \cdot 7 \ldots p_k)^2 + 2^2$. Esse número, pelo lema acima, é congruente a 1 módulo 4. Nenhum dos primos positivos menores do que ou iguais a p_k podem dividir M_k. pois

- no caso de $2|M_k$ teríamos $2|(3 \cdot 5 \ldots p_k)^2$, um absurdo pois todos os fatores do quadrado são ímpares.
- caso um fator ímpar até p_k dividisse M_k, então esse fator dividiria 2^2, gerando outra contradição.

Portanto todos os fatores primos p_i de M_k são maiores que p_k, logo são da forma $4m + 3$. Como $2 \not\equiv 0(mod\ p_i)$, podemos achar um elemento x' tal que $2x' \equiv 1(mod\ p_i)$, e assim obtemos sucessivamente

$$\begin{gathered} M_k \equiv 0(mod\ p_i) \\ (3 \cdot 5 \cdot 7 \ldots p_k)^2 + 2^2 \equiv 0(mod\ p_i) \\ (3 \cdot 5 \cdot 7 \ldots p_k)^2 x'^2 + (2x')^2 \equiv 0(mod\ p_i) \\ [(3 \cdot 5 \cdot 7 \ldots p_k)x']^2 \equiv -1(mod\ p_i) \end{gathered}$$

Um absurdo pois a congruência $x^2 \equiv -1(mod\ p_i)$ não tem solução, com $p_i \equiv 3(mod\ 4)$.

A hipótese inicial da existência de uma quantidade finita dos primos da forma $4n + 1$ conduz a uma contradição, demonstrando assim a proposição. □

5 CONCLUSÃO

A elaboração desse trabalho teve como substrato principal os conteúdos ministrados em algumas disciplinas do PROFMAT no núcleo da UFC para a turma 2011.1, como também procedimentos que comecei a desenvolver em meu trabalho como professor do ensino médio juntos a classes cujos alunos, em sua maior parte, possuem deficiências gravíssimas em formação Matemática que, não raras vezes, poderiam ser classificados como analfabetos funcionais visto que pouco ou nada conseguiram aprender após vários anos de estudo no ensino fundamental.

A maneira geral sugerida aqui, de como os assuntos podem ser expostos aos nossos alunos, ressaltando metodicamente a construção dos conceitos, visualizando as operações, seus axiomas e propriedades através de arranjos visuais e, principalmente, introduzindo a necessidade do desenvolvimento dos assuntos através de problemas contextualizados favorece sobremaneira a atenção, a participação ativa e a busca heurística por soluções que, se a princípio mostram-se inválidas, mas de maneira persistente as tentativas seguintes possuem notáveis graus de aproximação e acerto, culminando com a apreensão do assunto sistematizado de acordo com o nível evolutivo da classe em si própria. Alguns alunos cujos interesses e aptidões para as disciplinas exatas, e mais propriamente a Matemática, podem ser desafiados com certos problemas intrincados cuja solução fica bastante simplificada com a utilização das congruências lineares. A apresentação das condições suficientes que um número inteiro requer para ser escrito como soma de dois quadrados, pode ser apresentada àqueles poucos alunos excepcionais que já se destacam em atividades tais como a OBMEP, OBM ou clubes de Matemática.

É bem claro que não há receitas prontas para tentar reconquistar o gosto, algumas vezes já transformado em aversão, pela Matemática, quando as realidades duras do dia a dia cobram posturas pragmáticas de nossos alunos. A dúvida que a educação possa melhorar suas vidas muitas vezes é transformada em fortes desconfianças. Neste contexto, algumas iniciativas pioneiras como a organização desse curso de Mestrado Profissional para professores de Matemática do ensino básico, vêm contrabalançar certas tendências

de conformismo com os baixos índices de desempenho. Costumo sempre dizer, quando me refiro ao grupo de visionários que gestaram esse projeto, que nossa sociedade reconhecerá a importância do PROFMAT quando tiver que forçosamente perceber a melhoria dos níveis discentes em formação Matemática como reflexo imediato daqueles professores que tentam fazer sua parte no processo de resgate da educação pública brasileira. Para essa grande tarefa, tornou-se fundamental o amparo da CAPES e o engajamento de uma equipe nacional de professores universitários altamente competente em qualidade técnica profissional e formação moral. Sem essas condições nós e, em última análise, nossos alunos não teríamos obtido condições significativas de progredir em nosso trabalho árduo na educação pública que está apenas começando.

Que esse trabalho possa contribuir com novas perspectivas de atuação docente frente aos grandes desafios que todos os professores de escolas públicas diariamente experimentam.

REFERÊNCIAS

[1] AIGNER, Martin ; ZIEGLER, Günter M. *As provas estão no livro*. São Paulo : Edgard Blucher, 2002.

[2] DANTE, Luiz Roberto. *Restos, congruência e divisibilidade*. RPM, n.10, p.33-40, 1987.

[3] FOMIN, Dimitri ; GENKIN, Sergey ; ITENBERG, Ilia. *Mathematical circles : Russian experience*. Providence : American Mathematical Society, 1996.

[4] FREIRE, Benedito T. V. *Congruência, divibilidade e adivinhações*. RPM, n.22, p.4-10, 1992.

[5] GOUVÊA, F. Q. *Em busca da demonstração maravilhosa*. RPM, n.15, p.14, 1989.

[6] HEFEZ, Abramo. *Elementos de aritmética*. Rio de Janeiro : SBM, 2006.

[7] LIMA, Elon Lages et al. *Temas e problemas elementares*. Rio de Janeiro : SBM, 2005.

[8] MUNIZ NETO, Antonio Caminha. *Tópicos de matemática elementar : teoria dos números*. Rio de Janeiro : SBM, 2012. v.5

[9] NIVEN, Ivan ; ZUCKERMAN, Herbert. *An introduction to the theory of numbers*. New York : John Wiley, 1972.

[10] SANTOS, J. P. de O. *Introdução à teoria dos números*. Rio de Janeiro : IMPA, 1998.

[11] UMBELINO JÚNIOR, Arnaldo. *Divibilidade por 7*. RPM, n.43, p.38-39, 2000.