RAPHAEL ESCORSE CROTTI

TEORIA COMBINATÓRIA DOS NÚMEROS: UMA AMOSTRA DA RELAÇÃO EXISTENTE ENTRE A COMBINATÓRIA E A ARITMÉTICA.

Santo André, 2019

UNIVERSIDADE FEDERAL DO ABC

CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO

RAPHAEL ESCORSE CROTTI

TEORIA COMBINATÓRIA DOS NÚMEROS: UMA AMOSTRA DA RELAÇÃO EXISTENTE ENTRE A COMBINATÓRIA E A ARITMÉTICA.

Orientador: Prof. Dr. Jair Donadelli Junior

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre

ESTE EXEMPLAR CORRESPONDE A VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO RAPHAEL ESCORSE CROTTI, E ORIENTADA PELO PROF. DR. JAIR DONADELLI JUNIOR.

SANTO ANDRÉ, 2019

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Escorse Crotti, Raphael
Teoria Combinatória dos Números : Uma amostra da relação existente entre a Combinatória e a Aritmética / Raphael Escorse Crotti. — 2019.

84 fls. : il.

Orientador: Jair Donadelli Jr

Dissertação (Mestrado) — Universidade Federal do ABC, Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Santo André, 2019.

1. Combinatória. 2. Aritmética. I. Donadelli Jr, Jair. II. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, 2019. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do(a) autor(a) e com a anuência do(a) orientador(a).

Santo André ☐ 31 **de** maio **de** 2019

Assinatura do(a) autor(a): Raphael Escanso Gotti

Assinatura do(a) orientador(a):

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
profmat@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Raphael Escorse Crotti, realizada em 9 de abril de 2019:

Prof.(a) Dr.(a) **Jair Donadelli Júnior** (Universidade Federal do ABC) – Presidente

Prof.(a) Dr.(a) **Lucia Satie Ikemoto Murakami** (Universidade de São Paulo) – Membro Titular

Prof.(a) Dr.(a) **Rafael de Mattos Grisi** (Universidade Federal do ABC) – Membro Titular

Prof.(a) Dr.(a) **Marcelo Dias Passos** (Universidade Federal da Bahia) – Membro Suplente

Prof.(a) Dr.(a) **Rodrigo Roque Dias** (Universidade Federal do ABC) – Membro Suplente

AGRADECIMENTOS

Agradeço esse trabalho primeiramente a Deus, pois sem ele não teria forças para continuar.

Agradeço as pessoas que mais amo nessa vida, meus pais Elaine e Adão.

Agradeço ao meu orientador e professor Jair Donadelli Jr pelos ensinamentos, dedicação, paciência e companherismo.

Agradeço a todos os professores do PROFMAT da UFABC no qual tive a enorme honra de ter sido aluno: Ana Carolina Boero, Rafael Grisi, Maurício Firmino Silva Lima, Jair Donadelli Jr, Sinuê Dayan Barbero Lodovici, Jeferson Cassiano, Daniel Miranda e Marcus Antônio Mendonça Marrocos.

Agradeço a meu amigo de hoje e de sempre Marcelo Yamaki.

Agradeço as minhas queridas e amadas amigas do PROFMAT, Marilda e Juliana vocês são como uma família em meu coração.

Agradeço aos meus amigos de coração que fiz no Colégio da Fundação Santo André, em especial, Ingrid Herman, Ana Paula, Rodrigo Gomes, Elenir Sarro, Luiza Beraldo e Lígia Maria.

Agradeço aos meus amados alunos e ex-alunos do Colégio da Fundação Santo André, o carinho de vocês foi e sempre continuará sendo especial em meu coração.

Por fim, gostaria de salientar que o presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES)- Código de Financiamento 001.

RESUMO

Esse trabalho é dedicado ao estudo de uma área da Matemática atualmente conhecida como Teoria Combinatória dos Números. Demonstraremos alguns resultados da Teoria dos Números utilizando-se de ferramentas da Análise Combinatória, como por exemplo, o Princípio da Casa dos Pombos, que será explorado em um dos capítulos. Faremos uma menção à Teoria dos Grafos, para falarmos da Teoria de Ramsey e do Teorema de Schur. Finalizamos com a demonstração do Teorema de Van der Waerden, onde a prova será feita por indução e utilizando-se de argumentos combinatórios.

Palavras-chave: Análise Combinatória; Teoria dos Números; Teorema de Van der Waerden; Teoria de Ramsey.

ABSTRACT

This paper aims at studying an area of Mathematics known as Combinatorial Number Theory. We show a few results from Number Theory using tools from Combinatorial Analysis, such as the Pigeonhole Principle, which is explored in one of the chapters. We also refer to Graph Theory, in order to discuss Ramsey's Theory and Schur's Theorem. We finish by demonstrating Van der Waerden's Theorem, in which the test is inductive and uses combinatorial arguments.

Keywords: Combinatorial Analysis; Number Theory; Van der Waerden's Theorem; Ramsey's Theory.

LISTA DE FIGURAS

Figura 1 colar esticado. 4

Figura 2 colar formado por uma linha. 4

Figura 3 escolhas de pedras para formar o mesmo colar. 4

Figura 4 todos os 12 pentágonos estrelados. 6

Figura 5 polígonos formados pelas sequências descritas. 7

Figura 6 divisão do quadrado em quatro quadrados de lado 1. 10

Figura 7 marcando os 10 pontos. 15

Figura 8 representando a seis pessoas. 22

Figura 9 para o caso de cinco pessoas, podemos não ter um triângulo azul ou vermelho 23

Figura 10 representação de um grafo com 5 vértices e 7 arestas. 24

Figura 11 algumas possíveis representações de $G_{(5,5)}$. 24

Figura 12 representando um K_8. 25

Figura 13 representando o tabuleiro 3×3. 25

Figura 14 numerando as casas do tabuleiro. 26

Figura 15 representando as sequências descritas. 27

Figura 16 exemplo de grafo bicolorido e monocromático. 28

Figura 17 ligando os vértices com a cor azul 28

Figura 18 ligando os vértices com a cor vermelha 28

Figura 19 representando em grafos as possibilidades de uma festa com 3 pessoas. 29

Figura 20 as seis arestas azuis incidindo no vértice A. 31

Figura 21 K_{16} tricolorido sem um K_3 monocromático. 32

Figura 22 toda possível 2-coloração de [5]. 43
Figura 23 dois blocos com o mesmo padrão de cor. 43
Figura 24 caso $\varphi(a+2\Delta+2\delta) = M$ 45
Figura 25 blocos de W_0 elementos. 46
Figura 26 blocos de tamanho $w(3,c)$, representando os itens 1 e 2. 47
Figura 27 blocos de $2w(3,2)\cdot 2w(3,2^{2w(3,2)})$ 48
Figura 28 bloco $[W_0(1)]$ representado com seu primitivo. 50
Figura 29 exemplo de um bloco de tamanho $W_0(r)$. 51
Figura 30 representando PA de blocos monocromáticas que distam Δ'. . . 52
Figura 31 a primitivo das progressões aritméticas monocromáticas 54
Figura 32 representando a k-PA monocromática existente. 56

CONTEÚDO

Lista de Figuras xiii

INTRODUÇÃO 1

1 PEQUENO TEOREMA DE FERMAT E O TEOREMA DE WILSON 3
1.1 Demostração do Pequeno Teorema de Fermat 3
1.2 Teorema de Wilson 6

2 PRINCÍPIO DA CASA DOS POMBOS 9
2.1 Introdução 9
2.2 O Princípio da Casa dos Pombos na Aritmética 12
2.2.1 Demonstração do Teorema de Bézout 18

3 TEORIA DE RAMSEY 21
3.1 Teoria dos Grafos 21
3.2 Números de Ramsey 27
3.3 Teorema de Schur 34

4 TEOREMA DE VAN DER WAERDEN 39
4.1 Pilares da demonstração 41
4.1.1 Sobre as colorações 41
4.1.2 Divisão em blocos de $[W]$. 42
4.1.3 Provando a existência de $w(k,c)$ através de $w(k-1,c')$. 47
4.2 Demonstração do Teorema de Van der Waerden 49

5 CONCLUSÃO 57

A APÊNDICE A 59
A.1 Ordem Lexográfica 59
A.1.1 Indução em $\mathbb{N}\times\mathbb{N}$ 60

B APÊNDICE B 61
B.1 Grupo 61

C APÊNDICE C 63

Bibliografia 65

INTRODUÇÃO

Uma das características da Teoria dos Números é que vários de seus problemas e resultados podem requerer, para solução, a utilização de modo simultâneo de métodos algébricos, analíticos, topológicos e combinatórios, sendo esse último o foco desse trabalho. Em suma, iremos mostrar alguns resultados da Teoria dos Números, no que compete a parte Aritmética, que podem ser deduzidos utilizando-se de ferramentas da Análise Combinatória. Além disso, iremos falar sobre alguns teoremas e teorias de matemáticos importantes do final do século XIX, começo do século XX, tais como Frank Plumpton Ramsey (Cambridge, 1903 - Londres, 1930), Issai Schur (Mahilou - 1875, Tel Aviv - 1941) e Bartel Leendert Van Der Waerden (Amsterdã - 1903, Zurique - 1996). Veremos que a Teoria de Ramsey, em suma, diz que regularidades são inevitáveis em partições de subconjuntos dos Naturais. A área que relaciona Combinatória com a Teoria dos Números é atualmente conhecida como Teoria Combinatória dos Números.

No capítulo 1, iremos demonstrar o Pequeno Teorema de Fermat e o Teorema de Wilson, utilizando-se de argumentos combinatórios.

Já no capítulo 2, faremos uma menção ao Princípio da Casa dos Pombos (PCP), relevante ferramenta para a resolução de problemas em Combinatória. Mostraremos alguns problemas e teoremas da Aritmética que podem ser resolvidos utilizando o PCP, como por exemplo, a demonstração do Teorema de *Bézout*.

Caminhando para o capítulo 3, falaremos sobre uma parte da Teoria de Ramsey e também sobre um dos teoremas de Schur. De início começamos falando sobre a Teoria dos Grafos, estrutura da Combinatória da qual iremos usufruir para construir tal parte citada da Teoria de Ramsey. Podemos dizer que a Teoria de Ramsey é uma generalização do Princípio da Casa dos Pombos.

No capítulo 4, um dos vários teoremas sobre progressões aritméticas será provado, o Teorema de Van der Waerden, que afirma "existir progressões aritméticas de comprimento arbitrariamente grande ao longo dos naturais". A demonstração desse Teorema, também se baseará em argumentos e ferramentas da Combinatória, além da utilização do princípio da indução finita.

1

PEQUENO TEOREMA DE FERMAT E O TEOREMA DE WILSON

O Pequeno Teorema de Fermat e o Teorema de Wilson são dois resultados relevantes da Teoria dos Números. Suas demonstrações tradicionalmente não envolvem príncipios combinatórios. Para o Pequeno Teorema de Fermat que diz "*Se p é primo e a um inteiro positivo, então $p \mid (a^p - a)$*", a prova geralmente se baseia demonstrando que os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p, com p primo e depois usando a indução em a.

O Teorema de Wilson que diz "*Se p é primo, então* $(p-1)! \equiv -1 \pmod{p}$", tem sua validade verificada mostrando que o teorema é válido trivialmente para $p = 2$ e $p = 3$, e supondo $p \geq 5$, utiliza-se condições de soluções e propriedades de congruências.

Daremos aqui a demonstração de ambos os teoremas utilizando-se de ferramentas e argumentos combinatórios, como os métodos de contagem. As ideias centrais estão disponiveís em [3].

1.1 DEMOSTRAÇÃO DO PEQUENO TEOREMA DE FERMAT

Nessa seção convidamos o leitor para a apresentação e demonstração do Pequeno Teorema de Fermat. Inicialmente vamos mostrar um caso particular, onde provaremos que $5^7 \equiv 5 \pmod{7}$.

Suponha que temos linha e pedras de 5 tipos diferentes (que simplesmente numeraremos 1 a 5) para colocar na linha, formando um colar. Na linha cabem exatamente 7 pedras. Quantos colares podemos formar?

Primeiramente, imagine a linha do colar antes de amarrá-lo (veja figura 1). Há 5 escolhas para cada uma das 7 pedras a serem colocadas, de modo que há 5^7 maneiras de escolhermos as pedras para serem colocadas na linha.

Figura 1: colar esticado.

Agora, ao fecharmos o colar, podemos girá-lo de 7 maneiras (veja a figura 2). O colar resultante não se altera e note que outras sete escolhas de pedras podem formar o colar (veja a figura 3). Logo escolhas em ordens diferentes de pedras podem formar

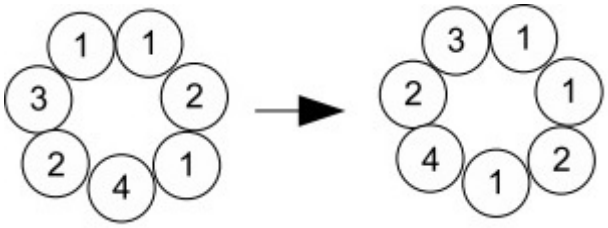

Figura 2: colar formado por uma linha.

o mesmo colar ao fechá-lo.

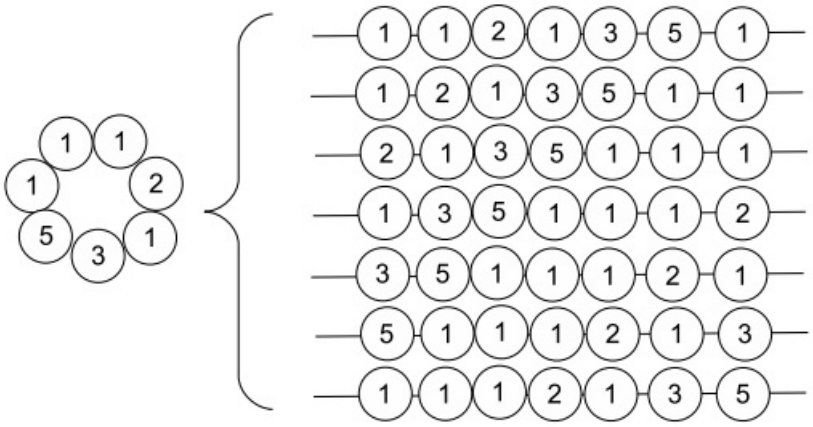

Figura 3: escolhas de pedras para formar o mesmo colar.

Assim, devemos dividir 5^7 por 7? Mas note que não vai dar inteiro! O que acontece é que os 5 colares com todas as pedras do mesmo tipo são formados pela mesma escolha de pedras. Logo, na verdade, devemos separar essas 5 escolhas primeiro e o que sobrou é dividido por 7, de modo que o total de colares é $5 + \frac{5^7-5}{7}$. Para o resultado ser inteiro, $5^7 - 5$ tem que ser múltiplo de 7, ou seja, $5^7 \equiv 5 \pmod 7$.

Essa breve demonstração, conforme dissemos no início na seção, trata-se de um caso particular do Pequeno Teorema de Fermat. Abaixo iremos demonstrá-lo usando raciocínio análogo.

Teorema 1. *Se p é primo e n um inteiro positivo, então $p \mid (n^p - n)$.*

Demonstração. Suponhamos que temos linha e pedras e que pretendemos colocar em cada linha exatamente p pedras. Podemos colorir cada uma das p pedras com um número n de cores. Quantas linhas (sequências de pedras) diferentes podemos formar? Como cada pedra pode ser colorida de n modos e cada linha tem p pedras, então é fácil verificar que pelo Princípio Multiplicativo temos um total de n^p linhas distintas.

Note que das n^p possibilidades temos exatamente n linhas que possuem somente uma cor, de sorte que separando estas à parte e juntando às duas extremidades de cada uma das $n^p - n$ linhas restantes, podemos formar $n^p - n$ colares.

Nós podemos alterar qualquer linha de pedras removendo uma pedra de uma das extremidades e colocando-a na outra extremidade. Esta alteração produz uma linha diferente sem alterar o colar resultante.

Agora seja k o menor número de vezes que esta alteração pode ser repetida até que a linha original seja reproduzida. Retirando obviamente as linhas onde todas as pedras são de uma mesma cor, podemos afirmar que $1 < k \leq p$. Observe que após $2k$ alterações o colar original será reproduzido novamente, de forma análoga para $3k$, $4k$, e assim por diante. Pelo algoritmo da divisão de Euclides existem h e r tais que $p = hk + r$, com $0 \leqslant r < k$.

Como uma linha é reproduzida após hk passos (alterações) e é também reproduzida após p passos, serão necessários r passos, após o *hk-ésimo* passo para se obter uma reprodução da coloração inicial. Como $r < k$ e k é o menor número positivo de passos necessários para a obtenção de uma reprodução, devemos ter necessariamente $r = 0$. Logo $p = hk$ e, portanto, $p = k$ uma vez que $k > 1$ e p é primo. Daí, as $n^p - n$ linhas podem ser agrupadas em grupos de p linhas cada, e é claro que cada grupo gera um colar diferente.

O número de colares distintos N multiplicado por p fornece o número de linhas que não são formados de uma única cor, que é $n^p - n$, ou seja, $pN = n^p - n$ o que implica $p \mid (n^p - n)$. □

1.2 TEOREMA DE WILSON

Agora veremos uma demonstração Combinatória do Teorema de Wilson.

Teorema 2. *Se p é primo, então* $(p-1)! \equiv -1$ *mod p.*

Demonstração. O teorema vale trivialmente para o caso $p = 2$. Pois note que

$$(2-1)! = 1 \equiv -1 \pmod 2.$$

Então suponhamos um primo p ímpar. Considere p pontos em um círculo distribuídos de tal forma que eles dividem o círculo em p arcos iguais. Quantos são os polígonos que podemos formar unindo estes pontos?(cruzamentos de arestas são permitidos). Estes polígonos são chamados *p-ágonos* estrelados pelo fato de seus vértices serem os vértices de um polígono regular convexo de p lados. A figura 4 abaixo mostra o caso em que $p = 5$.

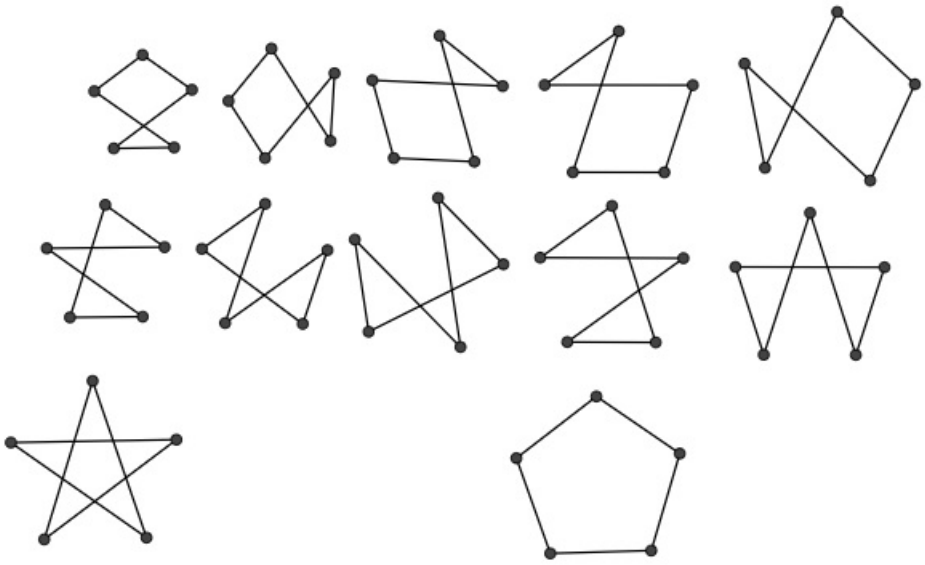

Figura 4: todos os 12 pentágonos estrelados.

Respondendo a pergunta, temos p escolhas para o primeiro vértice, $p-1$ para o segundo e assim sucessivamente. Logo é razoável imaginar que existem $p!$ tais polígonos. Mas note que podemos descrever cada um destes *p-ágonos* de $2p$ maneiras diferentes, isto é, iniciando em qualquer um dos p vértices e escolhendo uma ou outra das duas arestas naquele vértice como inicial. Portanto, nós obtemos, na realidade, $\frac{p!}{2p}$ diferentes *p-ágonos*.

Dos $\frac{p!}{2p}$ *p-ágonos*, exatamente $\frac{p-1}{2}$ ficam inalterados quando submetidos a uma rotação de um ângulo de $\frac{2\pi}{p}$ radianos. Estes são chamados *p-ágonos* estrelados regulares uma vez que são "estrelas" de p pontos onde cada ponto é o vértice de um ângulo de $\frac{(2k+1)\pi}{p}$ radianos, onde $0 \leq k \leq \frac{p-1}{2}$. No caso $p = 5$, existem duas de tais figuras, mostradas na terceira linha da Figura 4.

Para justificarmos esse número de $\frac{p-1}{2}$ polígonos estrelados, vamos considerar um caso particular, onde $p = 7$. Numeremos os vértices com os números $1, 2, \ldots, 7$ de modo que a sequência $1-2-3-4-5-6-7$ define o heptágono regular. Vamos formar polígonos pulando uma certa quantidade fixa de vértices, por exemplo, iniciamos pelos polígonos $1-2-3-4-5-6-7$, $1-3-5-7-2-4-6$ e $1-4-7-3-6-2-5$ (veja a figura 5).

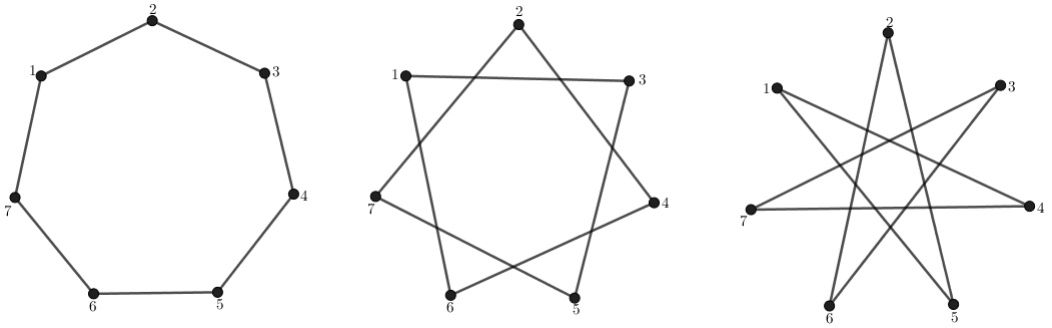

Figura 5: polígonos formados pelas sequências descritas.

Agora note que os polígonos $1-5-2-6-3-7-4$, $1-6-4-2-7-5-3$ e $1-7-6-5-4-3-2$ são, respectivamente, os mesmos de $1-4-7-3-6-2-5$, $1-3-5-7-2-4-6$ e $1-2-3-4-5-6-7$. Assim, temos um total de $3 = \frac{7-1}{2}$ polígonos estrelados.

Considere p pontos de modo que a sequência $1-2-3-\cdots-p$, defina o *p-ágono* regular. Formando os polígonos pulando uma certa quantidade fixa de vértices, como fizemos no caso $p = 7$, então temos que os polígonos resultantes são:

$$1-2-3-4-\cdots-(p-1)-p$$

$$1-3-\cdots-2-4-\cdots-(p-1)$$

$$1-4-\cdots-3-6-\cdots-(p-2)$$

$$\vdots$$

$$1-p-(p-1)-(p-2)\cdots-3-2$$

Assim teríamos $p-1$ polígonos estrelados, mas note que cada um deles foi contado duas vezes, isto porque os polígonos $1-2-3-4-\cdots-(p-1)-p$ e $1-p-(p-1)-(p-2)\cdots-3-2$, são os mesmos e assim sucessivamente, de sorte que temos um total de $\frac{p-1}{2}$ polígonos estrelados.

Os restantes $\frac{p!}{2p}-\frac{p-1}{2}$ *p-ágonos* estrelados pertencem a conjuntos de p elementos, onde cada elemento pode ser obtido por permutações sucessivas dos vértices, como por exemplo, as sequências $1-2-3-\cdots-(p-1)-p$, $2-3-\cdots-(p-1)-p-1$, $\cdots$, $p-1-2-3-\cdots-(p-1)$ geram os mesmos polígonos. Desta forma, o número total de conjuntos é

$$\frac{\frac{p!}{2p}-\frac{p-1}{2}}{p}=\frac{(p-1)!-(p-1)}{2p}$$

Como $2p \mid ((p-1)!-p+1)$, então $((p-1)!-p+1)=2pk$, com $k\in\mathbb{Z}$, daí

$$((p-1)!-p+1)=2pk \Rightarrow (p-1)!+1=2pk+p \Rightarrow p \mid ((p-1)!+1)$$

conforme queríamos demonstrar. □

O fato de p ser primo, possibilitou a demonstração feita acima. Gostaríamos de deixar um breve exemplo de quando p é composto, por exemplo, tomemos $p=8$. Numerando os vértices com os números $1,2,\ldots,8$ de modo que a sequência $1-2-3-4-5-6-7-8$ defina o octógono regular, então pulando uma certa quantidade fixa de vértices, de modo análogo ao que fizemos, temos, por exemplo, que algumas sequências como $1-3-5-7-1-3-5-7-\cdots-1-3-5-7$ ou $1-5-1-5-1-5-1-\cdots-1-5$ ocorreriam, de sorte que não teríamos os polígonos estrelados.

2

PRINCÍPIO DA CASA DOS POMBOS

2.1 INTRODUÇÃO

O princípio da casa dos pombos (PCP), embora tenha um enunciado relativamente simples, é um importante princípio combinatório. Ao longo deste capítulo mostraremos, por exemplo, problemas de Aritmética que serão resolvidos utilizando o PCP, bem como uma demonstração do Teorema de Bézout.

Teorema 3 (**O princípio da casa dos pombos**)**.** *Se $n+1$ pombos são colocados em n gaiolas, então alguma gaiola deverá conter pelo menos 2 pombos.*

Demonstração. Se o número máximo de pombos por gaiola for 1, teremos distribuído no máximo n pombos, o que é uma contradição. □

Esse princípio costuma, também, ser chamado de princípio das gavetas de Dirichlet, que pode ser enunciado como: se colocarmos n objetos em um número m de gavetas, $m < n$, então pelo menos uma gaveta deverá conter pelo menos dois objetos.

Utilizando essa ideia inteligível podemos garantir, por exemplo, que em um grupo com pelo menos 13 pessoas, teremos duas necessariamente fazendo aniversário no mesmo mês. Basta olharmos para os meses sendo as gaiolas (neste caso $n = 12$) e os pombos sendo as pessoas.

A afirmação do PCP é bastante intuitiva, não requer praticamente nenhum conhecimento prévio de algum assunto de matemática. Geralmente, a grande dificuldade encontrada nos exercícios de PCP é modelar o problema, isto é, saber quando e como utilizá-lo identificando quem serão os pombos e as gaiolas.

Vejamos alguns exemplos para melhor esclarecimento do que foi dito no parágrafo anterior.

Exemplo 1. *São escolhidos cinco pontos quaisquer no interior de um quadrado de lado 2. Então pelo menos um dos segmentos determinados por dois desses pontos tem comprimento no máximo* $\sqrt{2}$.

O fato de termos que provar a existência de pelo menos um dos segmentos determinados por dois desses pontos tenha comprimento máximo igual a $\sqrt{2}$, nos faz olharmos para esse número de outro jeito. Como $\sqrt{2}$ pode ser observado geometricamente? Podemos pensar que $\sqrt{2}$ é a diagonal de um quadrado de lado 1 que é exatamente a metade de 2.

Particionaremos o quadrado em quatro quadrados de lado 1, conforme a figura 6. Assim tomando cada um dos quadrados como as gaiolas e os pontos sendo os pombos, como existem 5 pombos e 4 gaiolas, logo pelo PCP, há em uma gaiola pelo menos dois pombos, isto é, em ao menos um dos quadrados devemos ter necessariamente 2 pontos. Como a maior distância entre dois pontos de um quadrado é dado quando estes são vértices da diagonal, assim esses pontos estão a uma distância máxima de $\sqrt{2}$. Desta forma, dados cinco pontos, como dois estarão em uma "mesma gaiola", eles determinam um segmento de comprimento, no máximo, igual a $\sqrt{2}$.

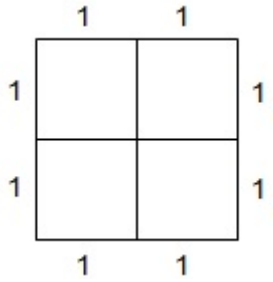

Figura 6: divisão do quadrado em quatro quadrados de lado 1.

Exemplo 2. *Em um reunião com n pessoas (*$n \geq 2$*), há sempre duas pessoas com o mesmo número de conhecidos. Neste exemplo assumimos que a relação de "conhece" é simétrica, ou seja, se a conhece b, então b conhece a.*

Divida essas n pessoas em n conjuntos $A_0, A_1, \ldots, A_{n-1}$ de modo que o conjunto A_j contém as pessoas que conhecem exatamente j pessoas. Daí se a pessoa não conhece ninguém ela pertence ao conjunto A_0, se tem um conhecido está no conjunto A_1 e

assim sucessivamente até chegarmos nas pessoas que conhecem todos, ou seja, as que pertencem ao conjunto A_{n-1}. Então temos n pombos (pessoas) para exatamente n gaiolas (que são os conjuntos de A_0 até A_{n-1}). Mas note que os conjuntos A_0 e A_{n-1} não podem ser ambos não vazios, isto porque se alguém não conhece ninguém é porque ninguém conhece todo mundo e reciprocamente se alguém conhece todo mundo é porque ninguém é desconhecido de todos. Portanto temos um total de n pessoas divididas em $n-1$ conjuntos e, logo, pelo PCP algum conjunto deve conter pelo menos duas pessoas.

Exemplo 3. *Suponhamos que em um auditório há 75 pessoas. Qual é o maior valor inteiro k para o qual possamos garantir que existe um mês em que pelo menos k dessas pessoas aniversariem?*

Sejam $x_1, x_2, \ldots, x_{75}$ as pessoas do auditório. Vamos distribuir de modo igualitário essas pessoas conforme a tabela abaixo, onde a pessoa x_i faz aniversário no mês representado nas colunas.

Janeiro	Fevereiro	Março	$\cdots$	Dezembro
x_1	x_2	x_3	$\cdots$	x_{12}
x_{13}	x_{14}	x_{15}	$\cdots$	x_{24}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_{61}	x_{62}	x_{63}	$\cdots$	x_{72}

Assim podemos distribuir uniformemente 6 pessoas para cada mês do ano, porém ainda faltam colocar três pessoas representadas por x_{73}, x_{74} e x_{75}. Logo teremos pelo menos 7 pessoas fazendo aniversário em algum dos meses do ano, portanto a resposta do problema é $k = 7$.

O exemplo acima sugere alguma generalização do princípio da casa dos pombos, isto porque temos um total de 12 gaiolas para 75 pombos e conseguimos dispor de modo igualitário apenas 72 deles, onde 72 é um múltiplo do número de gaiolas, já que $72 = 12 \cdot 6$, e como restaram 3 pombos concluímos então que em alguma gaiola teremos pelo menos 7 pombos.

Teorema 4. *(***Generalização do princípio da casa dos pombos**). Se n gaiolas são ocupadas por $nk+1$ pombos, então pelo menos uma gaiola deverá conter pelo menos $k+1$ pombos.

Demonstração. De fato, pois se cada gaiola contiver no máximo k pombos, pelo fato de termos n gaiolas, logo o número máximo de pombos distribuídos será de nk, o que é um absurdo. □

Veremos outro modo de enunciar o teorema 4, utilizando a notação $\lfloor x \rfloor$ para indicar o maior inteiro menor do que ou igual a x, onde $x \in \mathbb{R}$.

Teorema 5. *Se colocarmos em n gaiolas k pombos, então pelo menos uma gaiola deverá conter pelo menos $\left\lfloor \frac{k-1}{n} \right\rfloor + 1$ pombos.*

Demonstração. Suponhamos que em cada gaiola tenha no máximo $\left\lfloor \frac{k-1}{n} \right\rfloor$ pombos. Assim como são n gaiolas, teremos portanto no máximo $n \cdot \left\lfloor \frac{k-1}{n} \right\rfloor$ pombos no total, mas note que

$$\left\lfloor \frac{k-1}{n} \right\rfloor \leq \frac{k-1}{n}$$

portanto

$$n \cdot \left\lfloor \frac{k-1}{n} \right\rfloor \leq n \cdot \left(\frac{k-1}{n} \right) = k-1 < k$$

o que é uma contradição. □

Exemplo 4. *Em qualquer classe com 32 crianças, pelo menos 5 nasceram no mesmo dia da semana.*

Usando o Teorema 5, tomemos $n = 7$ e $k = 32$, daí

$$\left\lfloor \frac{32-1}{7} \right\rfloor + 1 = 4 + 1 = 5.$$

2.2 O PRINCÍPIO DA CASA DOS POMBOS NA ARITMÉTICA

Nessa seção abordaremos alguns problemas e resultados da Aritmética que podem perfeitamente serem resolvidas com a utilização do princípio da casa dos pombos.

Exemplo 5. *Dados sete números inteiros positivos, existem dois cuja soma ou a diferença é um múltiplo de 10.*

Vamos particionar esses sete números em seis conjuntos $A_0, A_1, \ldots, A_5$, onde um número x pertence ao conjunto A_j, se $x \equiv j$ ou $x \equiv -j \pmod{10}$. Lembrando

que todo inteiro positivo n pode ser escrito de forma única como $n = 10q + r$, com $q \in \mathbb{Z}$ e $r \in \{-5, -4, \ldots, 4\}$. Como temos sete números e seis conjuntos, pelo PCP, existe um conjunto com pelo menos dois números. Obviamente se tais números forem congruentes módulo 10, eles necessariamente terão o mesmo algarismos das unidades, bastando assim fazer a diferença entre eles. Caso os números sejam incongruentes módulo 10, pelo fato deles pertencerem ao mesmo conjunto A_j sua soma será múltiplo de 10, uma vez que um deles é côngruo a j módulo 10 e o outro é côngruo a $-j$ módulo 10.

Exemplo 6. *Qualquer conjunto de n números inteiros possui um subconjunto não vazio cuja soma dos elementos é divísivel por n.*

Denote por $a_1, a_2, \ldots, a_n$ os elementos desse conjunto e sejam as "somas parciais" $s_j = a_1 + a_2 + \cdots + a_j$ para todo $j = 1, \ldots, n$. Obviamente se algum s_j for divisível por n, então o problema estará resolvido. Caso contrário, note que ao dividirmos s_j por n obtemos os restos $1, 2, \ldots, n-1$. Como temos n somas parciais (pombos), logo pelo PCP teremos duas somas parciais s_j e s_k,com $j < k$, tais que $s_j \equiv s_k \pmod{n}$, daí $s_k - s_j \equiv 0 \pmod{n}$. Para descobrir quem é o conjunto note que

$$s_k - s_j = (a_1 + a_2 + \cdots + a_j + a_{j+1} + \cdots + a_k) - (a_1 + a_2 + \cdots + a_j) = a_{j+1} + \cdots + a_k,$$

de sorte que o subconjunto procurado é $\{a_{j+1}, a_{j+2}, \ldots, a_k\}$.

Iremos agora enunciar um teorema que trata da existência de subsequências crescentes ou decrescentes que podemos obter de qualquer sequência dada.

Teorema 6. *Toda sequência de $n \cdot m + 1$ números reais, contém uma subsequência crescente de comprimento ao menos $m + 1$ ou uma subsequência decrescente de comprimento ao menos $n + 1$.*

Para ilustrar, considere a seguinte sequência, com $3 \cdot 3 + 1$ termos, isto é, com $n = m = 3$.

$$55, 63, 57, 60, 74, 85, 16, 61, 7, 49 \tag{2.1}$$

Vamos encontrar a maior subsqüência crescente e decrescente de (2.1). Começando pela maior subsqüência decrescente, precisamos encontrar qual é a subsequência mais longa de (2.1) que termina com x, para $x = 55, 63, \ldots, 49$ (nessa ordem). Observe o quadro abaixo:

x	subsquência decrescente mais longa terminando em x
55	55
63	63
57	63,57
60	63,60
74	74
85	85
16	63,60,16
61	85,61
7	63,60,16,7
49	85,61,49

Vemos que a maior subsequência decrescente tem comprimento 4 e é representada por (63,60,16,7), onde $n = m = 3$ e $4 = 3 + 1$.

De modo análogo, vamos agora determinar a maior subsequência crescente.

x	subsequência crescente mais longa terminando em x
55	55
63	55,63
57	55,57
60	55,57,60
74	55,57,60,74
85	55,57,60,74,85
16	16
61	55,57,60,61
7	7
49	7,49

Encontramos nesse caso uma subsquência crescente de tamanho 5.

Façamos uma tabela contendo o comprimento da subsequência crescente mais longa terminando em x e o comprimento da subsequência decrescente mais longa terminando em x.

x	decrescente	crescente
55	1	1
63	1	2
57	2	2
60	2	3
74	1	4
85	1	5
16	3	1
61	2	4
7	4	1
49	3	2

Os valores da tabela podem ser vistos como coordenadas cartesianas, assim dispomos de 10 pontos

$$(1,1),(1,2),(2,2),(2,3),(1,4),(1,5),(3,1),(2,4),(4,1),(3,2).$$

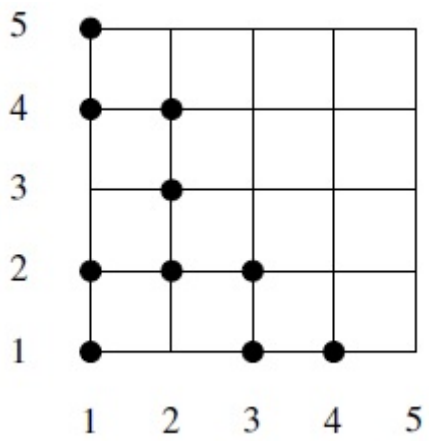

Figura 7: marcando os 10 pontos.

Se não houvesse uma subsequência crescente ou decrescente de comprimento 4, então todos os pontos caberiam em um tabuleiro 3×3 e dois pontos necessariamente teriam que estar na mesma "gaiola" pelo princípio da casas dos pombos, porém isso seria uma contradição, vejamos o motivo demonstrando o teorema 6.

Demonstração do Teorema 6. Considere uma sequência numérica com $n \cdot m + 1$ elementos, $z_1, z_2, \ldots, z_i, \ldots, z_j, \ldots, z_{n \cdot m+1}$. Suponha, por absurdo, que não haja uma sub-

sequência crescente contendo $m+1$ termos nem uma subsequência decrescente contendo $n+1$ termos, isto é, que as subsquências crescentes ou decrescentes tenham no máximo tamanho m ou n, respectivamente.

Sejam x_i e y_i o tamanho da maior subsequência decrescente e crescente, respectivamente, que termina em z_i, com $i \in \{1, 2, \ldots, n \cdot m + 1\}$. Note então que por hipótese devemos ter $0 < x_i \leq m$ e $0 < y_j \leq n$, de modo análogo ao caso $n = m = 3$, podemos considerar (x_i, y_i) como coordenadas cartesianas. Assim temos um total de $n \cdot m$ pares ordenados e $n \cdot m + 1$ números, daí pelo princípio da casa dos pombos devemos ter dois pontos z_i e z_j, tais que $(x_i, y_i) = (x_j, y_j)$.

Podemos supor sem perda de generalidade que $i < j$, iremos dividir em dois casos:

1ºcaso: $z_i < z_j$ (crescente). Chamando de $\ell = y_i$, considere $z_{\alpha_1}, z_{\alpha_2}, \ldots, z_{\alpha_\ell} = z_i$ a maior subsequência crescente até z_i, então note que a subsquência $z_{\alpha_1}, z_{\alpha_2}, \ldots, z_{\alpha_\ell}, z_j$ é crescente até z_j, logo $y_j \geq \ell + 1 > y_i$, o que é um absurdo.

2º caso: $z_j < z_i$(decrescente). De modo análogo, seja agora $k = x_i$ e considere $z_{\beta_1}, z_{\beta_2}, \ldots, z_{\beta_k} = z_i$ a maior subsequência decrescente terminando em z_i, então a subsequência $z_{\beta_1}, z_{\beta_2}, \ldots, z_{\beta_k}, z_j$ é decrescente até z_j, assim $x_j \geq k + 1 > x_i$, o que é um absurdo.

A contradição se deu em supormos que a maior subsquência crescente ou decrescente têm no máximo n ou m termos respectivamente, o que mostra o resultado. □

Mostraremos agora que cada número primo da forma $4k+1$ pode ser escrito como a soma de dois quadrados. Para isso, precisaremos dos seguintes lemas, onde o PCP será utilizado no lema 1.

Lema 1. *Sejam p um número primo e $u \in \mathbb{Z}$, tal que $p \nmid u$. Então existem inteiros x e y, não ambos nulos, tais que $-\sqrt{p} \leq x \leq \sqrt{p}$, $-\sqrt{p} \leq y, \leq \sqrt{p}$, e $(ux - y)$ é divisível por p, isto é, $ux \equiv y \pmod{p}$.*

Demonstração. Tome $k = \lfloor \sqrt{p} \rfloor + 1$, ou seja, $k - 1 \leq \sqrt{p} < k$. Considere os números da forma $ux - y$, com $x, y \in \{0, 1, \ldots, k-1\}$. Daí temos k^2 números (não necessariamente distintos), onde $k^2 > \sqrt{p} \cdot \sqrt{p} = p$, logo pelo PCP existem dois números não necessariamente distintos da forma $ux - y$ que deixam o mesmo resto na divisão por p.

Sejam então $0 \leq x_1, y_1, x_2, y_2 \leq k - 1 < \sqrt{p}$, tais que

$$ux_1 - y_1 \equiv ux_2 - y_2 \pmod{p} \tag{2.2}$$

Mostremos que $x_1 = x_2$ se, e somente se, $y_1 = y_2$. De fato, se $x_1 = x_2$, então de (2.2) temos $u(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$, daí temos que $0 \equiv y_1 - y_2 \pmod{p}$ o que implica em $y_1 = y_2$, já que $y_1, y_2 < \sqrt{p} < p$. Reciprocamente se $y_1 = y_2$, do fato de $p \nmid u$, então de (2.2) temos novamente que $u(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$, portanto $u(x_1 - x_2) \equiv 0 \pmod{p}$ o que acarreta em $x_1 = x_2$, também pelo fato de $x_1, x_2 < \sqrt{p} < p$.

Portanto devemos ter $x_1 \neq x_2$ e $y_1 \neq y_2$, de sorte que tomando $x = x_1 - x_2$ e $y = y_1 - y_2$, temos o resultado e claro que $|x_1 - x_2| \leq \sqrt{p}$ e $|y_1 - y_2| \leq \sqrt{p}$. □

Lema 2. *Se $p = 4k + 1$ é primo, então existe $u \in \mathbb{Z}$, tal que $u^2 \equiv -1 \pmod{p}$.*

Demonstração. Vamos particionar o conjunto $\{1, 2, \ldots, p-1\}$ em conjuntos da forma $C_k = \{k, p-k, \overline{k}, p-\overline{k}\}$, onde $\overline{k}$ é o inverso multiplicativo de $k \pmod{p}$, isto é, $k\overline{k} \equiv 1 \pmod{p}$. Como p é primo, então sabemos que para todo $k \in \{1, 2, \ldots, p-1\}$, $\overline{k}$ existe. Note que, $C_1 = \{1, p-1\}$ uma vez que o inverso de $1 \pmod{p}$ é 1, e do fato de $p - 1$ ser múltiplo de 4, então há de ter mais um conjunto C_m com 2 elementos, com $m \in \{2, \ldots, p-2\}$, ocorrendo esse fato quando $m \equiv p - \overline{m} \pmod{p}$, daí como $m\overline{m} \equiv 1 \pmod{p}$, temos

$$m \equiv -\overline{m} \pmod{p} \Rightarrow m^2 \equiv -m\overline{m} \pmod{p} \Rightarrow m^2 \equiv -1 \pmod{p} \quad \square$$

Teorema 7. *Todo primo p da forma $4k + 1$ pode ser escrito como a soma de dois quadrados.*

Demonstração. Sejam $p, u \in \mathbb{Z}$, tais que $u^2 \equiv -1 \pmod{p}$, com p primo da forma $4k + 1$. Usando o lema 1, sabemos que existem $x, y \in \mathbb{Z}^*$ tais que $xu - y$ é divisível por p, e ainda, $-\sqrt{p} \leq x \leq \sqrt{p}$, $-\sqrt{p} \leq y \leq \sqrt{p}$. Daí podemos concluir que $x^2 \leq p$ e $y^2 \leq p$, mas como p é primo, logo ambas as desigualdades são estritas, portanto $x^2 < p$ e $y^2 < p$ implica que $x^2 + y^2 < 2p$. Do fato de $xu \equiv y \pmod{p}$ e $u^2 \equiv -1 \pmod{p}$, devemos ter $x^2u^2 \equiv y^2 \equiv -x^2 \pmod{p}$, isto é, $x^2 + y^2$ é divisível por p, mas $x^2 + y^2 < 2p$, o que implica $p = x^2 + y^2$. □

A função "*fi*" *de Euler* $\varphi : \mathbb{N} \to \mathbb{N}$, em m, nos fornece a quantidade de números naturais entre 0 e $m - 1$ que são primos com m, é uma função importante da Teoria dos Números. Euler provou que se m, a são inteiros e primos entre si, com $m > 1$, então $a^{\varphi(m)} \equiv 1 \pmod{m}$, isto é, existe um número natural $d = \varphi(m)$ tal que $a^d \equiv 1 \pmod{m}$, onde $\varphi(m)$ é o menor natural que cumpre tal condição.

O cálculo de $\varphi(m)$, onde $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ é a decomposição de m em fatores primos, é dado por

$$\varphi(m) = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$

Recomendamos ao leitor [8] para verificar a prova desse resultado.

O fato de existir um inteiro positivo d tal que $a^d \equiv 1 \pmod{m}$ é extremamente útil para calcularmos restos da divisão de dois inteiros. Por exemplo, para achar o resto da divisão de 3^{70} por 8, podemos utilizar o fato de que 3 e 8 são primos entre si e portanto existe um d tal que $3^d \equiv 1 \pmod{8}$. Temos que $d = 2$, daí

$$3^{70} = (3^2)^{35} \equiv 1^{35} = 1 \pmod{8}$$

ou seja, o resto da divisão de 3^{70} por 8 é 1.

Veremos agora uma prova utilizando o PCP da existência de tal inteiro positivo d.

Lema 3. *Se a e m são primos entre si, então existe um inteiro positivo d, tal que $a^d \equiv 1 \pmod{m}$.*

Demonstração. Considere os restos da divisão por m das seguintes potências de a:

$$a, a^2, a^3, \ldots$$

Há m restos possíveis que são um dos elementos do conjunto $\{0, 1, \ldots, m-1\}$. Tome $l > m$ e portanto pelo PCP devem existir dois números em $a, a^2, a^3, \ldots, a^m, \ldots, a^l$, que deixam o mesmo resto na divisão por m. Sejam a^i e a^j, sendo $i, j \in \{1, 2, \ldots, l\}$ com $j > i$. Então como por hipótese a e m são primos entre si, logo:

$$a^j \equiv a^i \pmod{m} \Rightarrow a^{j-i} \equiv 1 \pmod{m}$$

de sorte que podemos tomar $d = j - i$. □

2.2.1 *Demonstração do Teorema de Bézout*

A demonstração de que dados a, b e c números inteiros, se $a \mid bc$ e mdc(a, b) = 1, então $a \mid c$, nos textos de Teoria dos Números, geralmente, depende do Teorema de Bézout diretamente ou indiretamente. Esse fato segue do Teorema Fundamental da Aritmética o qual, por sua vez, usa o Teorema de Bézout na prova da unicidade da decomposição em fatores primos. Uma prova da unicidade da decomposição em fatores

primos, enunciado no Teorema Fundamental da Aritmética, sem o usar o Teorema de Bézout é dado no Apêndice C.

Vamos apresentar uma demonstração do Teorema de Bézout utilizando o PCP.

Teorema 8. *Seja* $d = \text{mdc(a,b)}$ *o máximo divisor comum entre os números naturais* a *e* b*. Então existem* $x, y \in \mathbb{Z}$*, tais que* $ax + by = d$*.*

Demonstração. Sejam $m, n \in \mathbb{N}$ tais que $a = md$ e $b = nd$. Note que toda solução x, y de $ax + by = d$ é solução de $mx + ny = 1$, valendo a recíproca. Assuma $\text{mdc(a,b)} = 1$ e considere o conjunto $A = \{a, 2a, \ldots, ba\}$. Afirmamos que existe algum elemento em A que deixa resto 1 quando dividido por b. De fato, suponha por absurdo que não exista, então teríamos b números em A deixando $b - 1$ restos distintos na divisão por b, daí pelo PCP, dois deles, digamos ia e ja, com $b > j > i \geq 1$, devem deixar o mesmo resto quando divididos por b, de sorte que $(j - i)a$ é divisível por b. Como $\text{mdc(a,b)} = 1$, logo $(j - i)$ é divisível por b, mas $b > j - i > 0$, o que é um absurdo. Assim, algum dos números em A deixa resto 1 quando divididos por b. Digamos que esse número é ax, logo $ax - 1$ é um múltiplo de b, isto é, existe $y \in \mathbb{Z}$, tal que $ax - 1 = by$, o que prova o resultado. □

Para demais resultados do Princípio da Casa dos Pombos (PCP), não necessariamente envolvendo Aritmética, recomendamos a leitura de [2] e [4].

3

TEORIA DE RAMSEY

Neste capítulo introduziremos a Teoria de Ramsey, da qual originou-se de um artigo produzido pelo matemático, economista e filosófo britânico Frank Plumpton Ramsey (Cambridge, 1903 - Londres, 1930) em 1928, e publicado só após a sua morte em 1930, na *Proceendings of the London Mathematical Society*. Intitulado de "*On a problem of formal logic*", cuja a tradução é "Sobre um problema de lógica formal", o artigo tratava de métodos para determinar a consistência de uma fórmula lógica e inclui alguns teoremas sobre Análise Combinatória que levaram a uma nova área de estudo conhecida como Teoria de Ramsey. Podemos dizer também que a Teoria de Ramsey é um ramo de matemática que estuda condições sobre os quais certa "ordem" precisa aparecer. O matemático Theodore Samuel Motzkin (Berlim, 1908 - Los Angeles, 1970), disse que "a desordem completa é impossível", fazendo referência a Teoria de Ramsey.

Inicialmente, devemos nos concentrar sobre algumas definições sobre a Teoria dos Grafos, já que essa estrutura é um dos meios no qual podemos construir uma parte da Teoria de Ramsey.

3.1 TEORIA DOS GRAFOS

Vamos considerar inicialmente o seguinte exemplo.

Exemplo 7. *Mostre que em uma festa com seis pessoas, há sempre um grupo de três pessoas tais que todas se conhecem ou todas não se conhecem. Admita que a relação de conhecer é simétrica, ou seja, a conhece b se, e somente se, b conhece a.*

Considere as seis pessoas representadas pelos pontos A,B,C,D,E e F. Cada um dos 15 possíveis segmentos determinados por dois desses pontos, será pintado de duas cores,

azul e vermelho. Caso as pessoas se conheceçam então o segmento que os liga será pintado de azul, caso contrário de vermelho.

Fixando o ponto A, temos que 5 segmentos possuem como extremidade esse ponto, agora note que temos disponíveis duas cores para pintar tais segmentos, logo pelo princípio da casa dos pombos, existem pelo menos 3 segmentos que devem ser pintados de uma mesma cor. Digamos, sem perda de generalidade, que seja azul. Observe a figura 8.

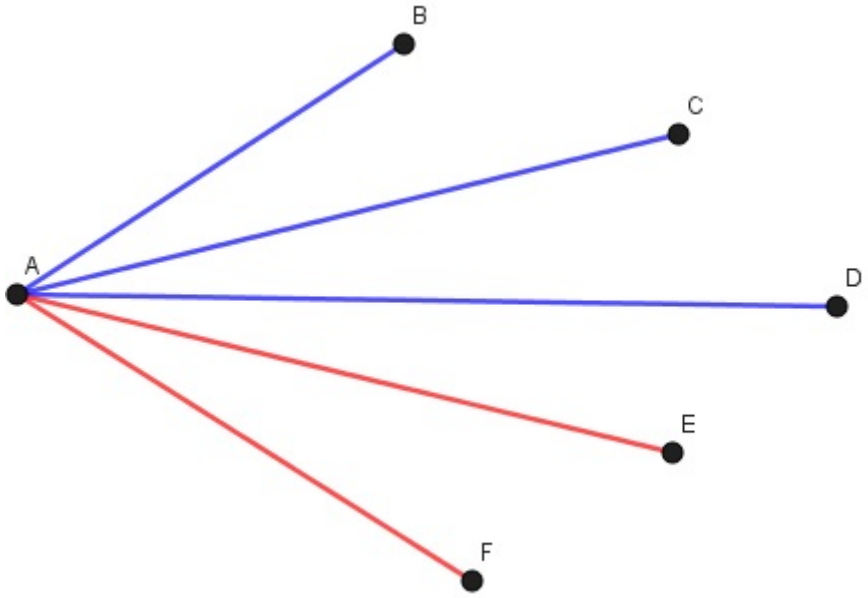

Figura 8: representando a seis pessoas.

Considerando o triângulo BDC, por exemplo, temos que, se algum de seus lados for azul, então necessariamente teremos um triângulo azul, o que implica que as três pessoas representadas por tais vértices se conhecem. Caso contrário, devemos ter então todos os lados do triângulo BDC pintados de vermelho, daí teremos três pessoas que não se conhecem.

Importante ressaltar que o exemplo anterior, não vale para o caso com 5 pessoas. De fato, veja a figura 9, abaixo.

A resolução desse exemplo, nos faz refletir sobre o quanto foi útil a modelagem do problema chamando as pessoas de pontos e ligando-as através de segmentos co-

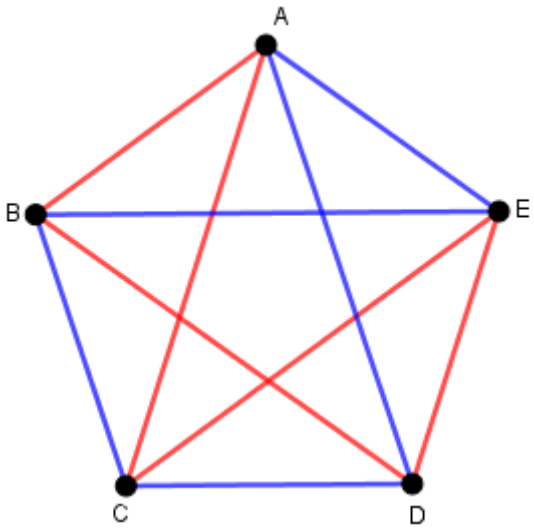

Figura 9: para o caso de cinco pessoas, podemos não ter um triângulo azul ou vermelho

loridos de azul ou vermelho, para representar se duas pessoas se conheciam ou não, respectivamente. Essa "linguagem" utilizada nos dá uma noção do que é um grafo. De sorte que essa ferramenta é de primordial importância para abstrair e resolver certos problemas de combinatória.

Um *grafo* $G = (\mathcal{V}, \mathcal{A})$ é constituído por dois conjuntos finitos e não vazios, $\mathcal{V}$ e $\mathcal{A}$ de vértices e arestas, respectivamente. Cada aresta é um par não ordenado de vértices distintos (conjunto de cardinalidade 2). Se uma aresta corresponde ao par de vértices $\{i, j\}$, dizemos então que i e j são as extremidades da aresta.

O número de vértices e arestas são parâmetros importantes do grafo em questão. Denotemos por $G_{(n,m)}$ o grafo que possui n vértices e m arestas, assim o grafo da figura 10 é denotado por $G_{(5,7)}$.

É possível fazer uma representação geométrica no plano de um grafo, de modo conveniente para cada situação. Na figura 11, temos possíveis representações de um grafo $G_{(5,5)}$.

Na representação de um grafo, o fato de duas arestas se cruzarem não implica a colocação de um vértice nesse ponto de interseção, de sorte que as arestas consideradas serão aquelas que unem dois vértices (conforme a figura 10). O número de vértices é denominado a ordem do grafo e chamamos de grau de um vértice v o número de arestas que incidem naquele vértice, que denotamos por $gr(v)$. Se dois vértices formam

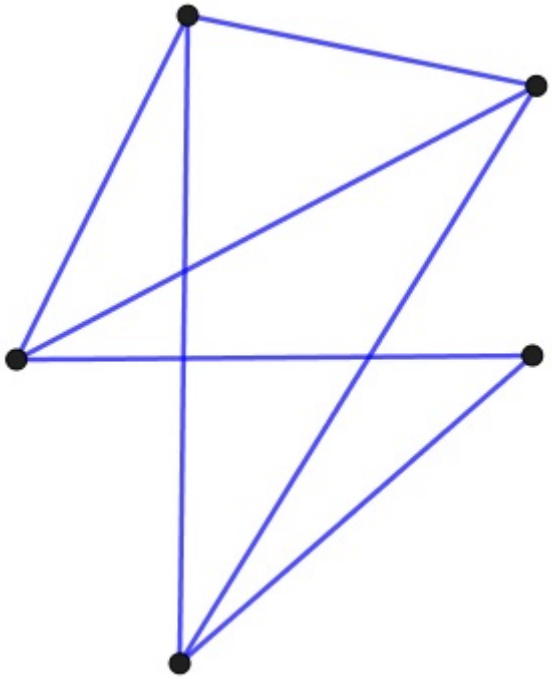

Figura 10: representação de um grafo com 5 vértices e 7 arestas.

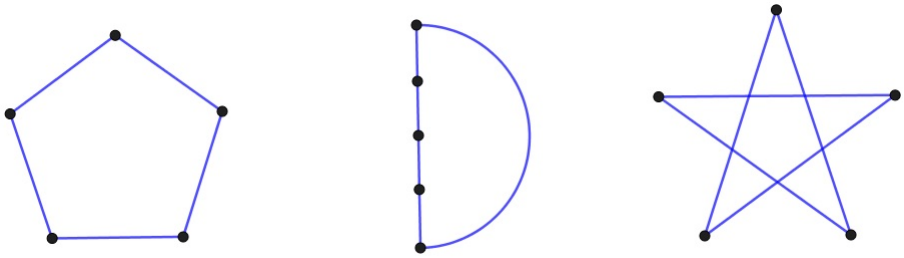

Figura 11: algumas possíveis representações de $G_{(5,5)}$.

uma aresta eles são chamados de adjacentes e se duas arestas incidem em um mesmo vértice, então elas são adjacentes.

Um *subgrafo* $\mathcal{G}' = (\mathcal{V}', \mathcal{A}')$ de um grafo $G = (\mathcal{V}, \mathcal{A})$ é um grafo tal que $\mathcal{V}' \subseteq \mathcal{V}$ e $\mathcal{A}' \subseteq \mathcal{A}$.

Um grafo é dito completo se cada par de vértices é adjacente. A notação utilizada para um grafo completo com n vértices é K_n, em homenagem ao matemático polonês *Kazimerz Kuratowski*. Note que o número total de arestas de um K_n é dado por $C_{n,2} = \frac{n \cdot (n-1)}{2}$, (já que esse é o número de subconjuntos de 2 elementos que podemos formar

através de um conjunto com n elementos). Com isso um K_n pode ser representado por um polígono regular de n vértices e suas arestas são os lados e as diagonais do polígono.

Exemplo 8. *Um K_8 pode ser representado como na figura abaixo.*

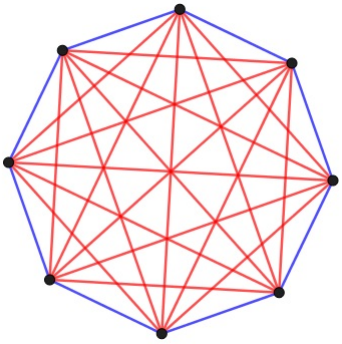

Figura 12: representando um K_8.

Conforme vimos no exemplo 7, a linguagem de grafos pode ser extremamente útil na resoluções de alguns problemas de combinatória. Vejamos um problema proposto em 1512 pelo matemático italiano *Paolo Guarini de Forli* (1464-1520).

Exemplo 9. *Considerando um tabuleiro de xadrez 3×3 com quatro cavalos, sendo dois brancos e dois pretos, dispostos nos cantos, conforme a figura 13, é possível passar os cavalos brancos para os cantos de baixo e os cavalos pretos para os de cima?*

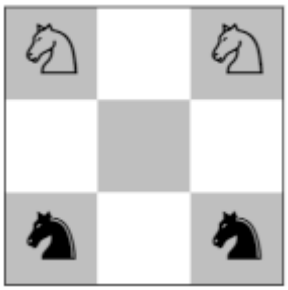

Figura 13: representando o tabuleiro 3×3.

Aqui vale ressaltar ao leitor, que o movimento do cavalo no xadrez é em "L", isto é, podendo andar duas casas na horizontal ou vertical e mais uma na perpendicular.

Uma das estratégias mais eficazes para resolver problemas, não somente de modo geral, mas principalmente em matemática é transformá-lo em um problema equivalente onde o contexto fique mais simples. Iremos numerar as casas do tabuleiro acima de 1 até 9, conforme a figura 14.

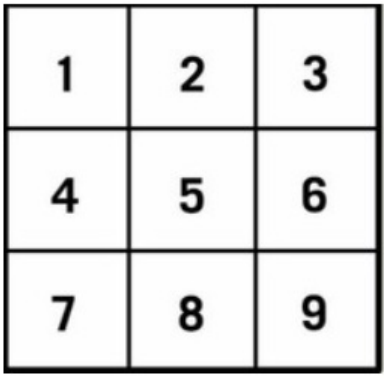

Figura 14: numerando as casas do tabuleiro.

Nas posições 1 e 3 estão localizados os cavalos brancos nas 7 e 9 os pretos. De acordo com a regra da movimentação do cavalo note que, o que está no posição 1, pode ir para a posição 6 ou 8. Usaremos a notação $1 \mapsto 6$ para dizer que o cavalo pulou da posição 1 para a 6. Vamos nos concentrar na movimentação do cavalo da cor branca que está na posição 1, conforme vimos existem duas possibilidades para o mesmo pular de casa. Supondo que ele pulou para a posição 6 (o caso pulou para a posição 8 é análogo), então teremos $1 \mapsto 6$, ao chegar na casa 6 podemos voltar até a casa 1 (que não convém) ou ir até a casa 7. Entretanto na casa 7, temos um cavalo preto e como dois cavalos não podem ocupar simultaneamente a mesma casa, precisamos necessariamente tirar esse cavalo dessa posição. Existem duas opções para ele, ir até a casa 2 (que está vazia) ou até a casa 6 (onde já se encontra um cavalo branco), logo coloquemos o cavalo preto na casa 2, isto é, $7 \mapsto 2$. Raciocinando de modo semelhante para o outro cavalo preto, teremos que deslocá-lo da posição 9 para a posição 4 e o cavalo branco da posição 3 para 8. Assim temos a seguinte sequência: $1 \mapsto 6$, $7 \mapsto 2$, $9 \mapsto 4$ e $3 \mapsto 8$. Assim podemos montar um grafo $G_{(8,8)}$.

Ao repetir quatro vezes essa sequência, teremos os cavalos que estavam nas posições 1,3,7 e 9 estarão, respectivamente, nas posições 9,7, 3 e 1, e portanto, teremos o desejado.

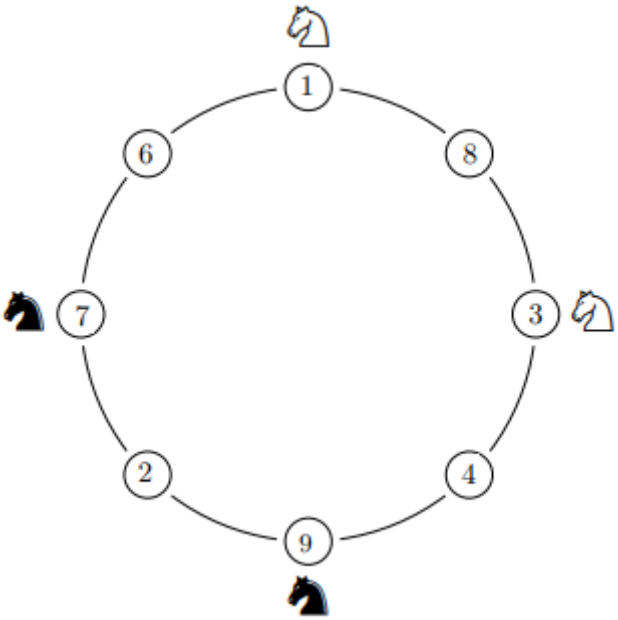

Figura 15: representando as sequências descritas.

3.2 NÚMEROS DE RAMSEY

Nesta seção falaremos sobre o Teorema de Ramsey para grafos utilizando-se duas cores e, em seguida, para um número k arbitrário de cores.

Definição 1. *Um grafo é chamado bicolorido quando suas arestas são pintadas de exatamente duas cores distintas.*

Definição 2. *Um grafo qualquer que tenha todas as arestas de uma mesma cor, será chamado de monocromático.*

Na figura 16 temos um K_4 bicolorido (pintado de azul e vermelho) e um K_5 monocromático (pintado de verde).

Teorema 9 (**Teorema de Ramsey para duas cores**)**.** *Dados dois números naturais $s, t \geq 2$, existe um número natural n_0, tal que qualquer grafo completo bicolorido (digamos azul e vermelho) de ordem $n \geq n_0$, contém um subgrafo completo monocromático azul de ordem s ou vermelho de ordem t. Denotaremos o menor natural que cumpra essa condição de $R(s, t)$, chamado número de Ramsey.*

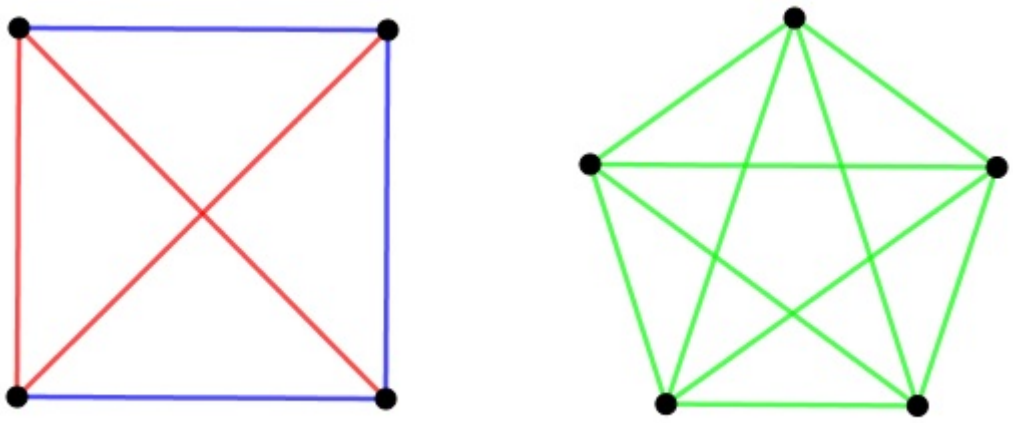

Figura 16: exemplo de grafo bicolorido e monocromático.

Em outras palavras o *Número de Ramsey* $R(s,t)$ é a ordem do menor grafo completo que, quando bicolorido, deve conter um K_s azul ou K_t vermelho.

Qual é o valor de $R(2,2)$? Ou seja, qual é o menor número de vértices que precisamos para garantir que caso pintássemos quaisquer dois destes vértices, teríamos necessariamente uma aresta azul ou vermelha? Obviamente dois pontos seriam suficientes, portanto $R(2,2) = 2$.

Figura 17: ligando os vértices com a cor azul

Figura 18: ligando os vértices com a cor vermelha

Façamos agora uma ánalise sobre o número $R(3,2)$. Queremos saber qual é o menor número de vértices para o qual possamos garantir que três desses estejam ligados por arestas azuis (triângulo monocromático) ou dois deles estejam ligados por arestas vermelhas. Podemos pensar em três pessoas como os vértices e liga-lós utilizando a cor azul quando se conhecerem e a cor vermelha, caso contrário, assim como fizemos no

exemplo 7. Portanto, em resumo, qual deve ser o menor número de pessoas possíveis presentes em uma festa, para o qual possamos garantir que três delas se conheçam (mutualmente) ou duas delas se desconheçam mutualmente?

Note que, em uma festa com três pessoas, todas se desconhecem (conhecem) mutualmente, ou existem duas pessoas que se desconhecem (conhecem) também mutualmente, logo $R(3,2) = 3$.

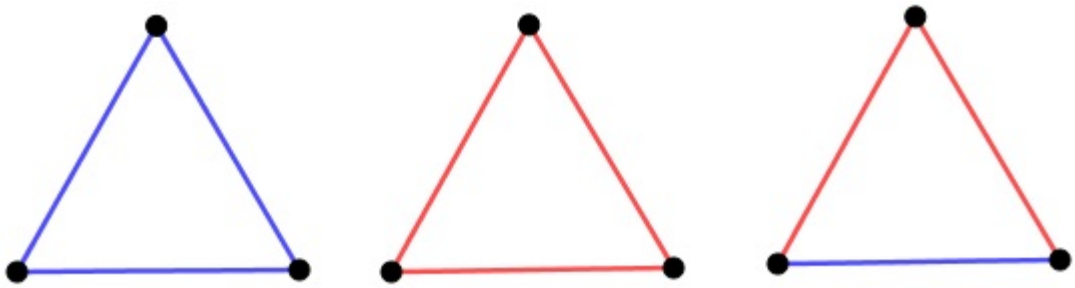

Figura 19: representando em grafos as possibilidades de uma festa com 3 pessoas.

Veremos agora alguns resultados importantes que podemos deduzir sobre tais números.

Lema 4. *Para todo inteiro $a \geq 2$, têm-se $R(a,2) = a$.*

Demonstração. De fato, considere um grafo completo com a vértices. Ou temos que todas as arestas são azuis, ou caso, contrário teremos pelo menos dois vértices ligados com uma aresta vermelha. Em outras palavras, em uma reunião com a pessoas, ou todas se conhecem, ou existem duas que se desconhecem. □

Lema 5. *Quaisquer que sejam os inteiros r e s , com $r,s \geq 3$, têm-se $R(s,t) = R(t,s)$.*

Demonstração. O resultado se dá trivialmente pelo fato de podermos trocar as cores de cada aresta. □

Provaremos por indução em s e t, a existência de $R(s,t)$, suscitado no teorema 9. A prova se baseará em que esse número é limitado pela soma de dois outros números de Ramsey. Por hipótese indutiva, iremos supor a existência dos números $R(s-1,t)$ e $R(s,t-1)$ e mostraremos que

$$R(s,t) \leq R(s-1,t) + R(s,t-1)$$

Demonstração. Evidentemente que $R(2,t) = 2 = R(s,2)$, conforme os dois últimos lemas.

Suponha que $R(s-1,t)$ e $R(s,t-1)$ existam e tome um grafo completo bicolorido (azul e vermelho) com n vértices, denotado K_n, para $n = R(s-1,t) + R(s,t-1)$. Tomando q como um desses vértices, podemos formar os seguintes conjuntos: o conjunto A, determinado pelas arestas adjacentes a q com as cores azuis e o conjunto V, determinado pelas arestas adjacentes a q com as cores vermelhas. Note que como K_n é grafo completo, portanto $A \cap V = \emptyset$, de sorte que $|A|+|V| = n-1$.

Afirmamos que $|A| \geq R(s-1,t)$ ou $|V| \geq R(s,t-1)$. De fato, suponhamos por absurdo que não, ou seja que $|A| < R(s-1,t)$ e $|V| < R(s,t-1)$, mas daí teríamos $|A| \leq R(s-1,t)-1$ e $|V| \leq R(s,t-1)-1$, portanto $|A|+|V| \leq R(s-1,t)+R(s,t-1)-2$, o que acarreta em $|A|+|V| \leq n-2$, o que é uma contradição.

Suponhamos então que $|A| \geq R(s-1,t)$ (o outro caso é análogo). Pela definição do número de Ramsey, temos duas possibilidades: Se A possuir um grafo completo K_t vermelho, não há mais o que provar. Caso contrário, A deve possuir um sub-grafo completo K_{s-1} azul, e adicionando ao vértice q, teremos um K_s azul.

Assim acabamos de provar que $n = R(s-1,t) + R(s,t-1)$ acarreta a existência de um K_s ou um K_t, em qualquer bicoloração do K_n, isto é, existe um número $R(s,t)$, tal que $R(s,t) \leq R(s-1,t) + R(s,t-1)$. □

A ideia de resolução do problema da festa com seis pessoas pode ser ampliada. Vamos substituir conhecer por amar, desconhecer por odiar e acrescentar que duas pessoas possam ser indeferentes entre si.

Exemplo 10. *Mostre que em uma festa com 17 pessoas, podemos encontrar três pessoas que se amam, três que se odeiam ou três que são indeferentes entre si.*

Consideremos as 17 pessoas como sendo os vértices de um grafo completo K_{17}, denotando-os pelas letras do alfabeto de A até Q. Dois vértices que estejam ligados por arestas de cores azul, vermelho e amarelo, indicam que tais pessoas se amam, odeiam e são indiferentes entre si, respectivamente. Pelo princípio da casa dos pombos, deve existir um vértice tal que pelo menos seis das arestas que incidem nele, devem ser todas da mesma cor. Digamos que seja A tal vértice e que as arestas que ligam B,C,D,E,F e G até A sejam azuis (sem perda de generalidade).

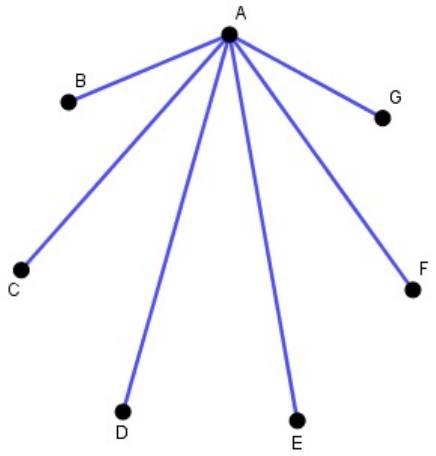

Figura 20: as seis arestas azuis incidindo no vértice A.

Assim se alguma das arestas entre B, C, D, E, F ou G for azul, então teremos um triângulo monocromático azul. Logo o grafo K_6 de vértices $B, C, \ldots, G$ é bicolorido (vermelho ou amarelo), que conforme o exemplo 7, implica na existência de um K_3 monocromático.

Temos no exemplo acima o Teorema de Ramsey para três cores, ou seja, $R(3,3,3) \leq 17$. Podemos estender essa teoria para qualquer número k de cores e denotando o número de Ramsey por $R(a_1, a_2, \ldots, a_k)$. Caso $a_i = a$, $\forall i = 1, 2, \ldots, k$, usaremos a notação $R_k(a)$, isto é, no exemplo 10, a notação seria $R(3,3,3) = R_3(3) \leq 17$.

Caso o número de pessoas na festa fosse 16, então não poderíamos garantir que três delas se amam, odeiam ou são indeferentes entre si. De fato, na figura 21 temos um K_{16} tricolorido sem a existência de um K_3 monocromático, onde os pontos $A, B, \ldots, P$ representam as pessoas e as cores utilizadas são azul, vermelho e amarelo.

Importante ressaltar que devido a grande complexidade de calcular os números de Ramsey, $R(3,3,3) = 17$ é o único conhecido com mais de duas cores. Alguns números já determinados são $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$, $R(3,6) = 18$, $R(3,7) = 23$, $R(3,8) = 28$, $R(3,9) = 36$, $R(4,4) = 18$ e $R(4,5) = 25$. Entretanto existem estimativas para o números de Ramsey (para maiores informações recomendamos ao leitor a leitura de [12]).

Podemos generalizar o teorema de Ramsey para um número qualquer de cores. Para fazer isso, vamos inicialmente estabelecer algumas notações e definições a serem usa-

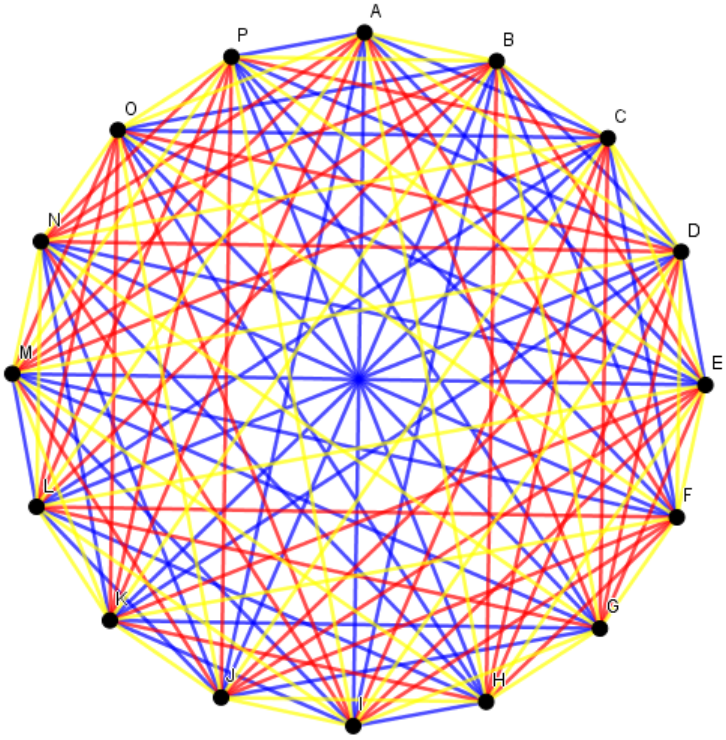

Figura 21: K_{16} tricolorido sem um K_3 monocromático.

das, não somente nessa generalização, mas bem como em outros teoremas e definições que iremos mostrar. Denotemos por $[a;b]$ ao conjunto $\{a, a+1, \ldots, b\}$, com $a < b$, para representar os inteiros c tais que $a \leq c \leq b$. Caso $a = 1$, simplifiquemos para $[1;b] = [b]$. Algumas vezes utilizaremos números tais como $1, 2, \ldots$, para representar diferentes cores.

Definição 3. *Uma k-coloração, com $k \in \mathbb{N}$, de um conjunto S é uma função $\varphi : S \to [k]$, onde $[k] = \{1, 2, \ldots, k\}$.*

Podemos também considerar uma k-coloração de φ de um conjunto S, a partição em k subconjuntos $S_1, S_2, \ldots, S_k$, onde o conjunto S_j é $\{x \in S; \varphi(x) = j\}$.

Definição 4. *Dizemos que uma coloração φ é monocromática em um conjunto S, quando φ é constante em S.*

Exemplo 11. *Seja $\varphi : [6] \to [2]$ definida por $\varphi(1) = \varphi(2) = \varphi(3) = \varphi(4) = 1$ e $\varphi(5) = \varphi(6) = 2$. Logo dizemos que φ é uma 2-coloração de $[6]$ que é monocromática em $\{1, 2, 3, 4\}$ e também em $\{5, 6\}$.*

Vamos agora enunciar a extensão do teorema de Ramsey para um número k de cores.

Teorema 10. *Dados k números naturais $a_i \geq 2$, com $i = 1, 2, \ldots, k$, existe um número natural n_0, tal que para toda k-coloração das arestas do K_n, com $n \geq n_0$, existirá subgrafo K_{a_i} monocromático da cor i, para algum i.*

Demonstração. Por indução em k. Para $k = 2$ o resultado é verificado conforme vimos no Teorema de Ramsey para duas cores. Assuma $R(a_1, a_2, \ldots, a_{k-1})$ e agora para provar $R(a_1, a_2, \ldots, a_k)$ usaremos a indução em $(a_1, a_2, \ldots, a_k) \in \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$.

Temos que $R(a_1, a_2, \ldots, a_{k-1}, 2) = R(a_1, a_2, \ldots, a_{k-1})$, com $a_j \geq 2$, $\forall j = 1, 2, \ldots, k-1$. De fato, considere um grafo completo K_n, sendo $n = R(a_1, a_2, \ldots, a_{k-1}, 2)$. Vamos pintar as arestas de K_n utilizando-se $k-1$ cores distintas mais a cor preta. Então note que há duas possibilidades: nenhuma das arestas de K_n é pintada de preta ou deve haver dois vértices cuja a aresta que os conectam é preta. Além disso, $R(a_1, a_2, \ldots, a_k) = R(a_{\delta(1)}, a_{\delta(2)}, \ldots, a_{\delta(k)})$, sendo δ qualquer permutação do conjunto $\{1, 2, \ldots, k\}$, pois essas permutações mudariam apenas a cor dos subgrafos.

Assuma que $R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k)$ existe, $\forall i = 1, 2, \ldots, k$ e conforme feito no teorema 9 vamos mostrar a existência de $R(a_1, a_2, \ldots, a_k)$ provando que

$$R(a_1, a_2, \ldots, a_k) \leq \sum_{i=1}^{k} (R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k)) - k + 2$$

Tomemos um grafo completo K_n, k-colorido nas arestas com n vértices para

$$n = \sum_{i=1}^{k} (R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k)) - k + 2.$$

Seja p um dos vértices de K_n. Assim são formados os conjuntos $A_1, A_2, \ldots, A_k$ dos vértices que possuem p como a outra extremidade e cuja às arestas que os conectam são pintadas das cores $1, 2, \ldots, k$. Agora note que, $A_i \cap A_j = \emptyset$, $\forall i \neq j$ e $\sum_{i=1}^{k} |A_i| = n - 1$.

Suponhamos por absurdo que $|A_i| < R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k)$, $\forall i = 1, 2, \ldots, k$. Lembrando que se $x, y \in \mathbb{N}$ com $x < y$, então $x \leq y - 1$, teremos portanto que

$$\sum_{i=1}^{k} |A_i| \leq \sum_{i=1}^{k} (R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k) - 1)$$

daí,

$$\sum_{i=1}^{k} |A_i| \leq (n + k - 2) - k = n - 2 < n - 1$$

o que é uma contradição. Então, necessariamente, existe algum $i \in \{1,2,\ldots,k\}$, tal que $|A_i| \geq R(a_1, a_2, \ldots, a_i - 1, \ldots, a_k)$. Suponha que $|A_1| \geq R(a_1 - 1, a_2, \ldots, a_k)$, temos duas possibilidades. Se A_1 conduzir a qualquer grafo completo K_{a_i} monocromático, da cor $i = 2,3,\ldots,k$, o teorema está provado. Caso contrário, se A_1 induzir um K_{a_1-1} monocromático da cor 1, basta juntar p a esses $n-1$ vértices e teremos um K_{a_1} monocromático da cor 1.

A análise dos outros conjuntos é feita de maneira inteiramente análoga ao que fizemos. □

3.3 TEOREMA DE SCHUR

Teoremas de partição em conjuntos não apareceram pela primeira vez na Teoria de Ramsey. Alguns resultados já haviam sido estudados por matemáticos como David Hilbert (Konisberg - 1862, Göttingen - 1943), Issai Schur (Mahilou - 1875, Tel Aviv - 1941) e Bartel Leendert Van Der Waerden (Amsterdã - 1903, Zurique - 1996), que podemos dizer foram os pioneiros conhecidos na área que hoje é chamada de Teoria de Ramsey.

Apresentaremos agora um teorema, demonstrado por Schur, que é um dos resultados iniciais da teoria de Ramsey.

Teorema 11 (Teorema de Schur). *Dado qualquer $r \geq 1$, existe um menor inteiro positivo $s = s(r)$ tal que, para qualquer r-coloração de $[s]$, existe uma solução monocromática para $x + y = z$. O número $s = s(r)$ que cumpre essa propriedade é chamado de número de Schur.*

Demonstração. Dado r, tome $s = R(3,3,\ldots,3) = R_r(3)$. Pela definição do número de Ramsey, sabemos que deve existir um triângulo monocromático com alguma das r cores possíveis em toda r-coloração das arestas do K_s. Seja $\varphi : [s] \to [r]$ uma coloração arbitrária de $[s]$. Defina a cor da aresta $\{i,j\}$ como sendo a cor do número $|j-i|$ e consideremos o triângulo monocromático existente em K_s. Chamando de a, b e c os vértices desse triângulo monocromático, com $a < b < c$, note que a cor das arestas $\{a,b\}$, $\{b,c\}$ e $\{a,c\}$ são iguais, de sorte que $|b-a|$, $|c-b|$ e $|c-a|$ representam a mesma cor, logo tomando $x = b-a$, $y = c-b$ e $z = c-a$, temos:

$$(b-a) + (c-b) = (c-a) \Rightarrow x + y = z$$

provando assim o teorema. □

Definição 5. *O triplo $\{x, y, z\}$ de inteiros positivos, tal que $x + y = z$ é chamado de triplo de Schur.*

Fazemos agora a seguinte indagação: quanto vale $s(2)$? Isto é, qual é o menor inteiro positivo $s = s(2)$ tal que qualquer 2-coloração de $[s]$ existe uma solução monocromática $x + y = z$. Notemos inicialmente que $s(2) > 4$. De fato, colorindo os elementos de $[4] = \{1, 2, 3, 4\}$, digamos com as cores azul e vermelho, onde 1 e 4 são coloridos de vermelho e 2 e 3 de azul, não temos um triplo de Schur monocromático, isto é, não existem $x, y, z \in \{1, 2, 3, 4\}$ de mesma cor, tais que $x + y = z$.

Assim como os números de Ramsey, devido a alta complexidade computacional em calcular tais números, apenas quatro deles são conhecidos, são eles: $s(1) = 2$, $s(2) = 5$, $s(3) = 14$ e $s(4) = 45$. Vamos mostrar que $s(2) = 5$, entretanto para o caso $s(3) = 14$, vamos deixar um exemplo garantindo que $s(3) > 13$.

Proposição 1. $s(2) \leq 5$

Demonstração. Tome uma 2-coloração arbitrária de $[5] = \{1, 2, 3, 4, 5\}$, utilizando-se das cores azul e vermelho. Suponha que não há um triplo de Schur monocromático e também que o número 1 é pintado vermelho, sem perda de generalidade. Agora note que $1 + 1 = 2$, então o número 2 deve ser pintado de azul. Como $2 + 2 = 4$, logo o número 4 deve ser pintado de vermelho, consequetemente do fato de $1 + 4 = 5$, assim o número 5 dever ser pintado de azul. Faltou apenas pintarmos o número 3, caso colorimos de vermelho teremos um triplo $\{1, 3, 4\}$, e se colorimos de azul, teremos um triplo $\{2, 3, 5\}$, de sorte que em ambos os casos temos um triplo de Schur monocromático.

Em particular, como vimos que $s(2) > 4$, portanto $s(2) = 5$. □

Para o caso $s(3)$, temos que $s(3) > 13$. De fato, tome uma 3-coloração de $[13] = \{1, 2, \ldots, 13\}$, com as cores vermelho, azul e marrom, onde $1, 4, 10, 13$ são coloridos de vermelho, $2, 3, 11, 12$ de azul e $5, 6, 8, 9$ de marrom e deixaremos o número 7 sem colorir. A sequência abaixo ilustra a situação.

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13$$

Note que independentemente da coloração do número 7, não teremos um triplo de Schur monocromático, ou seja, $s(3) > 13$.

Inspirado no Último Teorema de Fermat, Schur também demonstrou que a equação $x^n + y^n \equiv z^n \pmod{p}$ possui solução não trivial no conjunto dos inteiros não nulos

módulo p, com p primo. Denotando por $\mathbb{Z}_p^*$ tal conjunto, então $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, onde $\overline{j} = \{j + kp; k \in \mathbb{Z}\}$ e $j \in \{1, 2, \ldots, p-1\}$.

Teorema 12. *Para todo inteiro positivo n, existe um primo p_0, tal que para todo primo $p \geq p_0$, a equação $x^n + y^n \equiv z^n \pmod{p}$, possui uma solução não trivial em $\mathbb{Z}_p^*$.*

Demonstração. Tome n um inteiro positivo e seja p_0 um primo, tal que $p_0 \geq s(n)$. Fixe um primo $p \geq p_0$ e considere o grupo multiplicativo $\mathbb{Z}_p^*$ (ver Apêndice B). Sabemos que tal grupo deve possuir um gerador g, ou seja, dado $t \in \mathbb{Z}_p^*$, então temos que $t = g^m$, para algum inteiro positivo m. Portanto note que todo elemento t de $\mathbb{Z}_p^*$ pode ser escrito como g^{nk+r}, com $0 \leq r < n$ e k um inteiro positivo.

Tome uma n-coloração φ em $\mathbb{Z}_p^*$ dada por $\varphi(t) = r$, onde t e r, são tais que $t = g^{nk+r}$. Pelo teorema 11, existem x_1, x_2 e $x_3 \in \mathbb{Z}_p^*$ tais que, $\varphi(x_1) = \varphi(x_2) = \varphi(x_3)$, com $x_1 + x_2 = x_3$, daí $x_1 + x_2 \equiv x_3 \pmod{p}$ e temos que:

$$g^{k_1 n+r} + g^{k_2 n+r} \equiv g^{k_3 n+r} \pmod{p} \tag{3.1}$$

Como todo elemento de $\mathbb{Z}_p^*$ é invertível, logo para g^r existe um g' , tal que $g^r g' \equiv 1 \pmod{p}$. Assim tomando $x = g^{k_1}, y = g^{k_2}$ e $z = g^{k_3}$, segue de 3.1 que:

$$\left(g^{k_1}\right)^n \cdot g^r + \left(g^{k_2}\right)^n \cdot g^r \equiv \left(g^{k_3}\right)^n \cdot g^r \pmod{p} \Rightarrow x^n + y^n \equiv z^n \pmod{p}$$

conforme queríamos provar. □

Consideremos as soluções não triviais da equação $x^n + y^n \equiv z^n \pmod{p}$ para n fixo e p variado. Vejamos alguns exemplos.

Seja $n = 1$, portanto temos a equação $x + y \equiv z \pmod{p}$. Note que quando $p = 2$, nunca temos uma solução não trivial, pois $1 + 1 \equiv 0 \pmod{2}$. Além disso, caso $p > 2$ sempre teremos uma solução não trivial, já que $1 + 1 \equiv 2 \pmod{p}$.

Agora considere $n = 2$, logo temos $x^2 + y^2 \equiv z^2 \pmod{p}$. Note que quando $p = 2$, assim como no caso $n = 1$, não temos uma solução não trivial, pois $1^2 + 1^2 \equiv 0 \pmod{2}$. Caso $p = 3$, também não encontramos uma solução não trivial, a saber que $1^2 \equiv 1 \pmod{3}$ e $2^2 \equiv 1 \pmod{3}$, daí

$$1^2 + 1^2 \equiv 1^2 + 2^2 \equiv 2^2 + 2^2 \equiv 2 \neq z^2 \pmod{3}.$$

Para $p = 5$, têm-se que $1^2 \equiv 4^2 \equiv 1 \pmod{5}$ e $2^2 \equiv 3^2 \equiv 4 \pmod{5}$, e portanto não temos uma solução não trivial, uma vez que

$$1^2 + 1^2 \equiv 4^2 + 4^2 \equiv 1^2 + 4^2 \equiv 2 \neq z^2 \pmod{5}$$

e também,

$$2^2 + 2^2 \equiv 3^2 + 3^2 \equiv 3^2 + 2^2 \equiv 3 \neq z^2 \pmod 5.$$

E finalmente para $p \geq 7$, sempre teremos uma solução não trivial, pois $3^2 + 4^2 \equiv 5^2 \pmod p$.

Para $n = 3$, isto é, $x^3 + y^3 \equiv z^3 \pmod p$, novamente se $p = 2$, então não temos solução não trivial, já que $1^3 + 1^3 \equiv 0 \pmod 2$. Se $p = 3, 5$ ou 7, analisemos os casos:

- Quando $p = 3$, temos $1^3 \equiv 1$ e $2^3 \equiv 2 \pmod 3$, de sorte que temos a solução não trivial $1^3 + 1^3 \equiv 2^3 \pmod 3$.
- Quando $p = 5$, temos $1^3 \equiv 1$, $2^3 \equiv 3$, $3^3 \equiv 2$ e $4^3 \equiv 4 \pmod 5$, de sorte que temos a solução não trivial $1^3 + 2^3 \equiv 4^3 \pmod 5$.
- Quando $p = 7$, temos $1^3 \equiv 1$, $2^3 \equiv 1$, $3^3 \equiv 6$, $4^3 \equiv 1$, $5^3 \equiv 6$ e $6^3 \equiv 6 \pmod 7$ e neste caso não temos soluções não triviais.

Recomendamos ao leitor [10] para demais exemplos, casos particulares e condições de existência de soluções não triviais de $x^n + y^n \equiv z^n \pmod p$.

4

TEOREMA DE VAN DER WAERDEN

Os Teoremas de Schur e Ramsey lidam em sua essência com partições de conjuntos. E conforme dito no capítulo anterior alguns matemáticos do final do século XIX, começo do século XX, já haviam estudados problemas de coloração sobre os inteiros, sendo um deles Bartel Leerndert Van der Waerden, que foi um matemático holandês percusor da Álgebra Moderna do século XX. Estudou matemática na Universidade de Amsterdã, onde fez sua tese de doutorado referente a uma questão de Geometria Algébrica, foi bastante influenciado pelo matemático austríaco Emil Artin (Viena - 1898, Hamburgo - 1962) e pela matemática alemã Emmy Noether (Erlange - 1882, Bryn - 1935). Noether inclusive foi considerada a mulher mais importante da história da matemática por grandes nomes da história da Ciência, um deles Albert Einsten.

O teorema de Van der Waerden, demonstrado em 1927, é um dos resultados importantes da Teoria Combinatória dos Números, tratando de uma coloração finita qualquer do conjunto dos números naturais. Este teorema diz que sempre é possível encontrar uma progressão aritmética monocromática de comprimento arbitrariamente grande, isto é, existe um conjunto $X \subset \mathbb{N}$, tal que X contém tal progressão.

A demonstração desse teorema foi de relevância para os diversos avanços nos estudos de progressões aritméticas em subconjuntos dos números naturais. Podemos destacar um teorema provado pelos matemáticos Ben Green (Bristol - 1977) e Terence Tao (Adelaide - 1975), em 2004, no qual se diz que "existem progressões aritméticas de comprimento arbitrariamente longo no conjunto dos números primos".

Com os trabalhos desenvolvidos por Ramsey, Schur, Van der Waerden, entre outros matemáticos, pode-se dizer que um vasto campo da matemática foi criado ao longo do século XX, área atualmente conhecida como Teoria Combinatória dos Números.

A demonstração do Teorema de Van der Waerden será feita usando argumentos combinatórios. As ideias centrais, bem como uma prova do Teorema utilizando Teoria Ergódica estão presentes em [11] e [7].

Exemplo 12. *Vamos colorir de dois modos arbitrários os números* $\{1,2,\ldots,9\}$ *utilizando duas cores, vermelho ou azul.*

$$1,2,3,4,5,6,7,8,9$$

$$1,2,3,4,5,6,7,8,9$$

Note que na primeira sequência os números $1,3$ e 5 e na segunda $1,5$ e 9 formam uma progressão aritmética de razão 2 e 4 respectivamente, ambas com três elementos.

Poder-se-ia questionar se para toda coloração dos números $\{1,2,\ldots,9\}$ utilizando a cor vermelha ou azul, seria sempre possível formar uma progressão aritmética de três termos.

Veremos que o Teorema de Van der Waerden é uma extensa generalização do exemplo 12 e, antes de enunciarmos, fixaremos algumas definições sobre progressões aritméticas e colorações.

Definição 6. *Uma progressão aritmética de comprimento k, que abreviamos por k-PA, é uma sequência de k números naturais que são igualmente espaçados, isto é, da forma*

$$a, a+\delta, a+2\delta, \ldots, a+(k-1)\delta \text{ , com } a,\delta \in \mathbb{N}.$$

Definição 7. *Dada uma coloração φ de $\mathbb{N}$, chamamos de k-PA monocromática a uma progressão aritmética de comprimento k tal que todos os elementos são da mesma cor, isto é*

$$\varphi(a) = \varphi(a+\delta) = \varphi(a+2\delta) = \cdots = \varphi(a+(k-1)\delta).$$

Teorema 13 (Teorema de Van der Waerden). *Dados $k, c \in \mathbb{N}$, existe $W \in \mathbb{N}$, tal que para toda c-coloração $\varphi : [W] \to [c]$, existe uma k-PA monocromática.*

Note que se o teorema é válido para W, então para todo $W' \geq W$ o teorema também vale. Definimos o número de Van der Waerden $w(k,c)$ em que k é o número de elementos da progressão e c é a quantidade de cores, como sendo o menor elemento do conjunto não vazio $X = \{W \in \mathbb{N}; \text{vale o teorema 13}\}$. A existência desse número é garantida pelo princípio da boa ordenação, uma vez que X é não vazio e está contido em $\mathbb{N}$.

Vejamos algumas propriedades imediatas desses números, para quaisquer k e c:

- $w(k,1) = k$, já que temos somente um modo de pintar os k elementos.
- $w(1,c) = 1$, imediato já que temos apenas 1 elemento para colorir.
- $w(2,c) = c+1$, uma vez que pelo PCP, devemos ter ao menos $c+1$ elementos para garantir que pelo menos dois deles estão coloridos com a mesma cor, pois temos c cores distintas disponíveis e conjuntos com dois elementos sempre formam PA.

Assim como os números de Ramsey, a estimativa desses números se torna cada vez mais trabalhosa de acordo com a quantidade de elementos e cores em questão. Alguns dos poucos números de Van der Waerden conhecidos são: $w(3,2) = 9$, $w(3,3) = 27$, $w(3,4) = 76$, $w(4,2) = 35$, $w(5,2) = 178$ e $w(6,2) = 1132$.

Recomendamos ao leitor [9] para maiores informações sobre estimativas desses números.

4.1 PILARES DA DEMONSTRAÇÃO

Para demonstrar o teorema 13, faremos nessa seção algumas considerações que serão facilitadoras na prova do teorema. Em resumo, iremos apresentar a divisão de um conjunto $[W] = \{1,2,\ldots,W\}$ em blocos de acordo com uma determinada regra, depois faremos sucessivas construções desse tipo e por fim usaremos a indução sobre os parâmetros (k,c) dos números de Van der Waerden através da ordem lexicográfica de $\mathbb{N}\times\mathbb{N}$ (ver Apêndice A). Não demonstraremos o teorema de Van der Waerden para W ótimo, isto é, $w(k,c)$.

4.1.1 *Sobre as colorações*

Como usual, uma c-coloração de $[W]$ é uma função $\varphi : [W] \to [c]$, entretanto para demonstrar o teorema de Van der Waerden usaremos a seguinte estratégia: o conjunto $[W]$ é particionado em $k = \frac{W}{n}$ blocos $B_1, B_2, \ldots, B_k$, consecutivos de tamanho n, para algum natural n, para W múltiplo de n. Essa partição é denotada por $[B_k] = \{B_1, B_2, \ldots, B_k\}$ e a c-coloração de $[W]$ induz uma c^n-coloração $\chi : [B_k] \to [c]^n$, a cor χ para o bloco $B = \{a+1, a+2, \ldots, a+n\}$ é

$$\chi(B) = \left(\varphi(a+1), \varphi(a+2), \ldots, \varphi(a+n)\right).$$

Definição 8. *Dizemos que* $B_i = \{a+1, a+2, \ldots, a+n\}$ *e* $B_j = \{b+1, b+2, \ldots, b+n\}$ *têm o mesmo padrão de cor (mesma cor), se* $\chi(B_i) = \chi(B_j)$*, isto é,*

$$(\varphi(a+1), \varphi(a+2), \ldots, \varphi(a+n)) = (\varphi(b+1), \varphi(b+2), \ldots, \varphi(b+n))$$

ou seja, se $\varphi(a+l) = \varphi(b+l)$*, para todo* $l \in \{1, 2, \ldots, n\}$*.*

Exemplo 13. *Considere o conjunto* $[20] = \{1, 2, \ldots, 20\}$ *e seja* $\varphi : [20] \to [3]$ *uma coloração qualquer. Particionemos* $[20]$ *em* 4 *blocos de* 5 *elementos consecutivos.*

$$\{1,2,3,4,5\}, \{6,7,8,9,10\}, \{11,12,13,14,15\}, \{16,17,18,19,20\}.$$

Temos que os blocos $\{1,2,3,4,5\}$ *e* $\{11,12,13,14,15\}$ *possuem o mesmo padrão de cor.*

Proposição 2. *Sejam* $n, c \in \mathbb{N}$*, onde* n *e* c *são as quantidades de elementos em cada bloco e de cores disponíveis, respectivamente. Tomando* $W \geq n \cdot (c^n + 1)$*, com* W *múltiplo de* n*, e particionando o conjunto* $[W]$ *em blocos consecutivos, cada um deles com* n *elementos, então existem dois blocos* B_i *e* B_j *com o mesmo padrão de cor. E considerando mais* $n \cdot c^n$ *elementos, há um bloco* B_k*, tal que* $|j - i| = |k - j|$*.*

Demonstração. Dividindo o conjunto $[W]$ em blocos de n elementos consecutivos,

$$\{1, 2, \ldots, n\}, \{n+1, n+2 \ldots, 2n\}, \ldots, \{W-(n-1), W-(n-2), \ldots, W\}$$

temos $\frac{W}{n}$ blocos e, como cada um deles pode ser colorido de c^n modos distintos, se $\frac{W}{n} \geq (c^n + 1)$, isto é, $W \geq n \cdot (c^n + 1)$, então pelo príncipio da casa dos pombos, devem existir dois blocos B_i e B_j, onde $1 \leq i < j \leq c^n + 1$, com o mesmo padrão de cor. Tomando mais $n \cdot c^n$ elementos, teremos que a sequência de blocos será $\{B_1, B_2, \ldots, B_{c^n}, B_{c^n+1}, \ldots, B_{2c^n}\}$, garantindo assim tal terceiro bloco igualmente espaçado. □

4.1.2 *Divisão em blocos de* $[W]$.

Vamos apresentar a divisão de $[W]$ em blocos com um número n de elementos, para assim demonstrar a existência de alguns números de Van der Waerden, começando por $w(3,2)$. Denotemos por $d = |j - i|$ a distância entre o bloco B_i e B_j, $\Delta = d \cdot |B_i| = d \cdot n$, a distância entre elementos correspondentes de blocos de mesmo padrão de cor e δ a razão da PA existente em cada bloco.

Seja $\varphi : [W] \to \{V, A\}$ uma 2-coloração qualquer de $[W]$, onde V e A representam respectivamente as cores Vermelho e Azul. Um elemento que não possuir uma cor especificada, será chamado de neutro e denotado por N.

Suponha que não há uma 3-PA monocromática. Note que se dividirmos $[W]$ em blocos de cinco elementos, ou seja, $n = 5$, então pelo princípio da casa dos pombos existirá pelo menos três elementos igualmente espaçados, de modo que os dois primeiros com a mesma cor. Isto porque nas três primeiras posições alguma cor repete e como a maior distância possível entre tais elementos de mesma cor é dois, então pelo fato de termos cinco elementos, podemos encontrar tal terceiro elemento igualmente espaçado (veja figura 22).

VVVVV	VAVVA	VVAAA	AAVAV
VVVVA	AVVVA	VAVAA	AAAVV
VVVAV	VVAAV	AVVAA	VAAAA
VVAVV	VAVAV	VAAVA	AVAAA
VAVVV	AVVAV	AVAVA	AAVAA
AVVVV	VAAVV	AAVVA	AAAVA
VVVAA	AVAVV	VAAAV	AAAAV
VVAVA	AAVVV	AVAAV	AAAAA

Figura 22: toda possível 2-coloração de [5].

Pela proposição 2, se $W \geq 5 \cdot (2^5 + 1) = 165$, então existirão dois blocos com o mesmo padrão de cor, e com mais $5 \cdot 2^5$ elementos, teremos um terceiro igualmente espaçado.

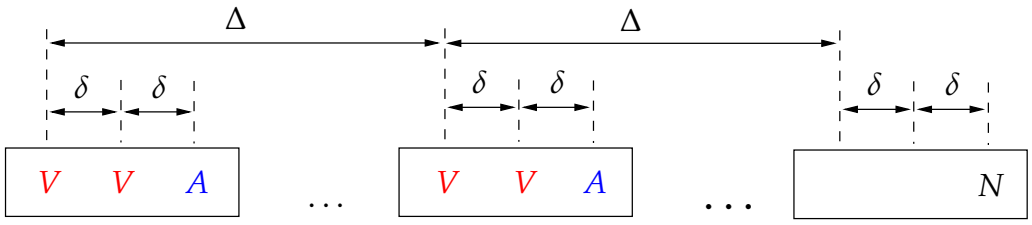

Figura 23: dois blocos com o mesmo padrão de cor.

Analisando os possíveis casos para N e considerando a, $a + \delta$ e $a + 2\delta$ é a progressão aritmética $V - V - A$ no bloco B_i, temos que:

- Se $\varphi(a+2\Delta+2\delta) = V$, então teremos que $\varphi(a) = \varphi(a+\Delta+\delta) = \varphi(a+2\Delta+2\delta) = V$, de sorte que temos uma 3-PA monocromática de razão r, tal que $r = \Delta+\delta$, contradição.
- Se $\varphi(a+2\Delta+2\delta) = A$, então teremos que $\varphi(a+2\delta) = \varphi(a+2\delta+\Delta) = \varphi(a+2\delta+2\Delta) = A$, de sorte que temos uma 3-PA monocromática de razão r, tal que $r = \Delta$, contradição.

Logo em ambos os casos temos uma 3-PA monocromática utilizando as cores vermelha e azul.

Sejam $W \in \mathbb{N}$ e $\varphi : [W] \to \{V, A, M\}$, onde as letras V,A e M representam as cores vermelha, azul e marrom respectivamente. Provaremos agora a existência de um W limitante superior para $w(3,3)$. Assim como para $w(3,2)$, suponha que não há uma 3-PA monocromática. Como $c = 3$, note que se dividirmos $[W]$ em blocos de 7 elementos, pelo princípio da casa dos pombos, uma cor deve aparecer pelo menos três vezes, de sorte que divindo $[W]$ em blocos de 7 elementos consecutivos, sendo W múltiplo de 7, temos:

$$\{1,2,3,4,5,6,7\}, \ldots, \{W-6, W-5, W-4, W-3, W-2, W-1, W\}.$$

Afirmamos que em cada um desses $\frac{W}{7}$ blocos irá ocorrer três elementos igualmente espaçados tal que os dois primeiros possuem a mesma cor. De fato, temos que nas quatro primeiras posições alguma cor repete, digamos a vermelha. Como a maior distância entre dois elementos quaisquer dentre esses que ocupam as quatro primeiras posições é 3, isso ocorre quando os elementos considerados são o primeiro e o quarto, pelo fato da sequência ter 7 elementos, então sempre é possível encontrar tal terceiro elemento igualmente espaçado dentro do bloco, (veja δ da figura 24).

Voltando à divisão de $[W]$ em blocos de 7 elementos, temos que cada bloco pode ser colorido de $3^7 = 2187$ modos distintos, assim para que ocorra dois blocos de mesma coloração precisamos, pelo princípio da casa dos pombos, de pelo menos 2188 blocos. Para que ocorra, com certeza, um terceiro bloco igualmente espaçado com os dois anteriores (veja Δ da figura 24), necessitamos de mais $3^7 = 2187$ blocos, daí como cada bloco contém 7 elementos, o número de elementos W para o qual esses fatos ocorram deve ser tal que:

$$W \geq 7 \cdot 2187 + 7 + 7 \cdot 2187 = 7 \cdot (2 \cdot 3^7 + 1) = 30625.$$

Enunciemos agora um pequeno lema para nos auxiliar na demonstração de $w(3,3)$.

Lema 6. *Existe* $[W_0] \in \mathbb{N}$*, tal que, para toda* 3*-coloração* (V,A,M) *de* $[W_0]$*, se não existe* 3*-PA monocromática, então existem duas* 3*-PA's tais que elas possuem os dois primeiros elementos da mesma cor e o têm o terceiro elemento em comum, isto é, são da forma* $V-V-M$ *ou* $A-A-M$*.*

Demonstração. Como vimos acima nos dois parágrafos anteriores, sejam Δ e δ de acordo com as notações da figura 24.

Considere W_0, tal que, para todo $W \geq W_0$, para algum a, tenha-se:

1. $\varphi(a) = \varphi(a+\delta) = \varphi(a+\Delta) = \varphi(a+\Delta+\delta) = V$;
2. $\varphi(a+2\delta) = \varphi(a+\Delta+2\delta) = A$;
3. $a+2\Delta+2\delta \in [W]$.

Vimos que caso $\varphi(N) = V$ ou $\varphi(N) = A$, então teremos uma 3-PA monocromática. Então $\varphi(a+2\Delta+2\delta) = M$, de sorte que teremos duas 3-PA's com o mesmo terceiro elemento (veja a figura 24). De fato temos $\varphi(a) = \varphi(a+\Delta+\delta) = V$ e $\varphi(a+2\Delta+2\delta) = M$, assim temos uma 3-PA de razão $r = \Delta+\delta$, e também $\varphi(a+2\delta) = \varphi(a+\Delta+2\delta) = A$ e $\varphi(a+2\Delta+2\delta) = M$, de sorte que têm-se uma 3-PA de razão $r = \Delta$. □

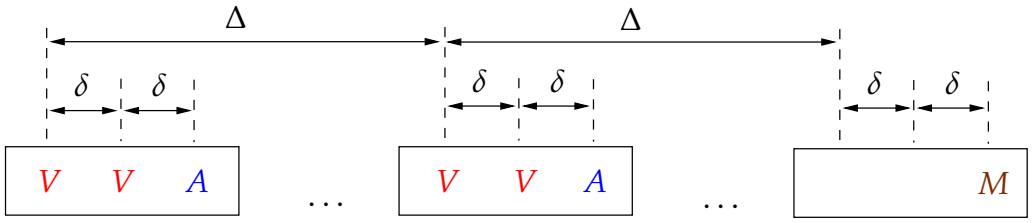

Figura 24: caso $\varphi(a+2\Delta+2\delta) = M$

Vamos particionar o conjunto $[W] = \{1,2,\ldots,W\}$ em blocos de W_0 elementos, com $W \geq W_0 \cdot (2 \cdot 3^{W_0}+1)$ e W_0 de acordo com as condições do lema 6, isto é,

$$\{1,2,\ldots,W_0\},\{W_0+1,W_0+2,\ldots,2W_0\},\ldots,\{W_0-(W_0-1),W-(W_0-2),\ldots,W\}.$$

Olhando para $[W]$ como um conjunto de blocos, sendo cada um de comprimento W_0, temos que cada bloco pode ser colorido de 3^{W_0} modos distintos e como $W \geq W_0 \cdot (2 \cdot 3^{W_0}+1)$, temos então que devem existir três blocos, B_i ,B_j e B_k, tais que eles

devem ser igualmente espaçado sendo os dois primeiros, B_i e B_j com o mesmo padrão de cor. Aplicando o lema 6 nesses dois primeiros blocos e sejam Δ, δ e δ', de acordo com as notações da figura 25, e considerando $\varphi(a) = V$ e $\varphi(b) = A$, onde $a, a+\delta$ e $a+2\delta$ e $b, b+\delta'$ e $b+2\delta'$ são as progressões aritméticas $V-V-M$ e $A-A-M$, respectivamente, contidas nos blocos B_i e B_j, temos:

- Se $\varphi(a+2\Delta+2\delta) = V$, então note que $\varphi(a) = \varphi(a+\Delta+\delta) = \varphi(a+2\Delta+2\delta) = V$, de sorte que teremos uma 3-PA monocromática de razão r, tal que $r = \Delta+\delta$, contradição.
- Se $\varphi(b+2\Delta+2\delta') = A$, então note que $\varphi(b) = \varphi(b+\Delta+\delta') = \varphi(b+2\Delta+2\delta') = A$, de sorte que teremos uma 3-PA monocromática de razão r, tal que $r = \Delta+\delta'$, contradição.
- Se $\varphi(a+2\Delta+2\delta) = M$, então note que $\varphi(a+2\delta) = \varphi(a+2\delta+\Delta) = \varphi(a+2\delta+2\Delta) = M$, de sorte que teremos uma 3-PA monocromática de razão r, tal que $r = \Delta$, contradição.

Logo em todos os casos têm-se uma 3-PA monocromática, garantindo assim a existência de $w(3,3)$.

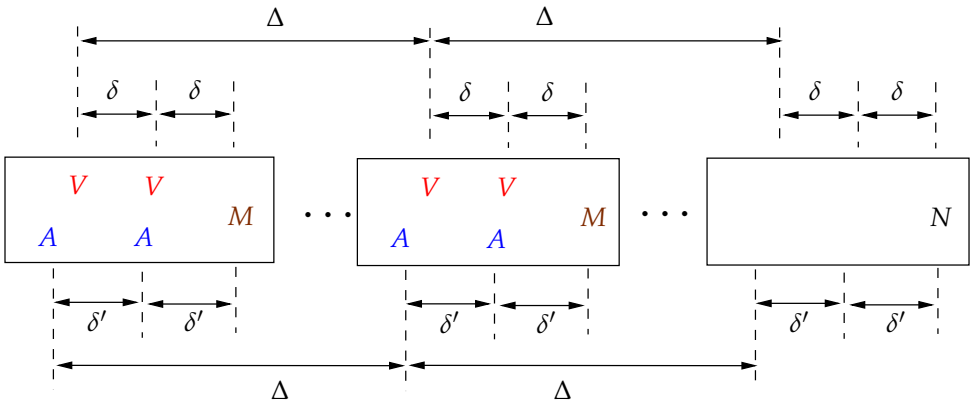

Figura 25: blocos de W_0 elementos.

Assim provamos o seguinte resultado.

Teorema 14. *Seja* $\varphi : [W] \to \{V, A, M\}$, *com* $W \geq W_0 \cdot (2 \cdot 3^{W_0} + 1)$, *sendo* W_0 *de acordo com as condições do lema 6. Então existem* $a, \delta \in \mathbb{N}$, *tais que:*

$$\varphi(a) = \varphi(a+\delta) = \varphi(a+2\delta).$$

4.1.3 *Provando a existência de $w(k,c)$ através de $w(k-1,c')$.*

A ideia agora será provar a existência de um $w(k,c)$ através de um $w(k-1,c')$, sendo c' um valor suficientemente grande e usaremos a ordem lexicográfica de $\mathbb{N}\times\mathbb{N}$, ou seja,

$$(1,1)\prec(1,2)\prec\cdots\prec(2,1)\prec(2,2)\prec\cdots\prec(3,1)\prec(3,2)\prec\cdots$$

conforme dissemos no início deste capítulo.

Em resumo, podemos usar o $w(2,c')$ para provarmos $w(3,c'')$, então usaremos $w(3,c''')$ para provar $w(4,c)$ e assim por diante para quaisquer c,c',c'' e c'''. Assim podemos supor a existência de $w(k-1,c'),\forall c'$, para provarmos $w(k,c)$. Lembramos que $w(1,c)=1$ e $w(2,c)=c+1$, para todo c.

Vamos mostrar a existência de um limitante W para $w(4,2)$, utilizando $w(3,c)$ para um valor arbitário de c. Entretanto antes de prosseguirmos, enunciamos um importante lema que será usado posteriormente na demonstração de $w(4,2)$.

Lema 7. *Seja $c\in\mathbb{N}$ e assuma $w(3,c)$. Então para todo $W\geq 2w(3,c)$, existem $a,\delta\in\mathbb{N}$, tais que*

1. $\varphi(a)=\varphi(a+\delta)=\varphi(a+2\delta)$;
2. $a+3\delta\in[2w(3,c)]$.

Demonstração. O item (1) é trivial, já que temos um $w(3,c)$. No item (2) pelo fato de termos $2w(3,2)$, então é claro que $a+3\delta\in[2w(3,c)]$. □

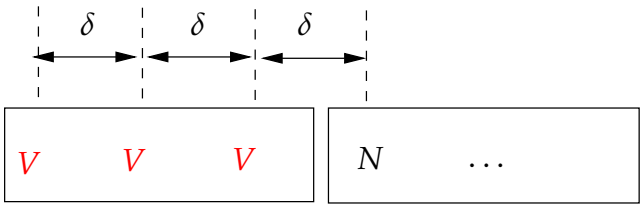

Figura 26: blocos de tamanho $w(3,c)$, representando os itens 1 e 2.

O teorema a seguir irá garantir a existência de $w(4,2)$.

Teorema 15. *Se $W_0\geq 2w(3,2)\cdot 2w(3,2^{2w(3,2)})$, então para qualquer coloração $\varphi:[W_0]\to\{V,A\}$, existem $a,\delta\in\mathbb{N}$ tais que*

$$\varphi(a)=\varphi(a+\delta)=\varphi(a+2\delta)=\varphi(a+3\delta).$$

Demonstração. Basta provar para $W_0 = 2w(3,2) \cdot 2w(3, 2^{2w(3,2)})$. Suponha que não há uma 4-PA monocromática. Vamos tomar $2w(3, 2^{2w(3,2)})$ blocos de tamanho $2w(3,2)$

$$\{1, 2, \ldots, 2w(3,2)\}, \{2w(3,2)+1, \ldots, 4w(3,2)\}, \ldots, \{W_0 - (2w(3,2)-1), \ldots, W_0\}.$$

Deste modo particionamos o conjunto $[W_0] = \{1, 2, \ldots, W_0\}$ em blocos de $2w(3,2)$ elementos, tal que, $\frac{W_0}{2w(3,2)} = 2w(3, 2^{2w(3,2)})$.

Consideremos um desses blocos B, digamos $B = \{a_1, a_2, \ldots, a_{2w(3,2)}\}$, onde cada $a_i =$ V ou A, $\forall i$, tal que $1 \leq i \leq 2w(3,2)$.

Note que existem $2^{2w(3,2)}$ modos distintos de se colorir o bloco B. Tome $\chi : B_i \to [2^{2w(3,2)}]$ uma coloração do bloco B_i. Olhando para $[W_0]$ como uma sequência desses blocos B_i's, isto é,

$$[B_{2w(3,2^{2w(3,2)})}] = \{B_1, B_2, \ldots, B_{w(3,2^{2w(3,2)})}, \ldots, B_{2w(3,2^{2w(3,2)})}\}$$

e observando que ao multiplicarmos $2w(3,2)$ e $w(3, 2^{2w(3,2)})$ por 2, estaremos garantindo o lema 7, podemos aplicar o lema tanto na coloração no bloco B como na sequência $B_1, B_2, \ldots, B_{w(3,2^{2w(3,2)})}, \ldots, B_{2w(3,2^{2w(3,2)})}$, conforme a figura 27.

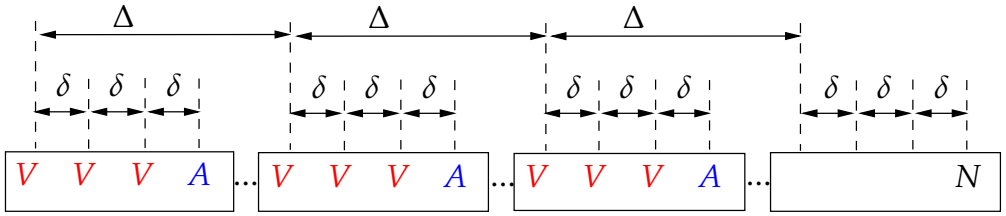

Figura 27: blocos de $2w(3,2) \cdot 2w(3, 2^{2w(3,2)})$

Assim, existem $a, \delta, \Delta \in \mathbb{N}$ tais que

- $\varphi(a) = \varphi(a+\delta) = \varphi(a+2\delta) =$ *V*;
- $\varphi(a+\Delta) = \varphi(a+\Delta+\delta) = \varphi(a+\Delta+2\delta) =$ *V*;
- $\varphi(a+2\Delta) = \varphi(a+2\Delta+\delta) = \varphi(a+2\Delta+2\delta) =$ *V*;
- $\varphi(a+3\delta) = \varphi(a+\Delta+3\delta) = \varphi(a+2\Delta+3\delta) =$ *A*;
- $a+3\Delta+3\delta \in [W_0]$, com $\varphi(a+3\Delta+3\delta) = N$.

Analisando as possíveis cores de $a+3\Delta+3\delta$, têm-se que:

- Se $\varphi(a+3\Delta+3\delta) =$ *V*, então $\varphi(a) = \varphi(a+\Delta+\delta) = \varphi(a+2\Delta+2\delta) = \varphi(a+3\Delta+3\delta) =$ *V*, de sorte que temos uma 4-PA monocromática de razão r, tal que $r = \Delta + \delta$;

- Se $\varphi(a+3\Delta+3\delta) = A$, então $\varphi(a+3\delta) = \varphi(a+\Delta+3\delta) = \varphi(a+2\Delta+3\delta) = \varphi(a+3\Delta+3\delta) = A$, de sorte que temos uma 4-PA monocromática de razão r, tal que $r = \Delta$.

Logo em ambos os casos temos uma 4-PA monocromática, o que é uma contradição.

□

4.2 DEMONSTRAÇÃO DO TEOREMA DE VAN DER WAERDEN

Após os resultados apresentados na seção anterior, estamos pronto para a prova completa do Teorema de Van der Waerden. A demonstração seguirá naturalmente de um lema que iremos provar a seguir, que diz: "Dado um W_0 suficientemente grande, quando tomamos uma c-coloração qualquer $\varphi : [W_0] \to [c]$, então teremos uma k-PA monocromática ou um número arbitrário de $(k-1)$-PA's monocromáticas, todas de diferentes cores".

Chamaremos de *primitivo* um número inicial, para o qual todo primeiro elemento das PA's monocromáticas estão há uma distância de acordo com suas respectivas razões, podendo ou não fazer parte delas.

Exemplo 14. *Observe as sequências abaixo.*

$$1,2,3,4,5,6,7,8,9$$

$$1,2,3,4,5,6,7,8,9$$

Temos que o número 2 *é primitivo em ambas as* 3*-PA's monocromáticas* $(4,6,8)$*, porém em uma delas ele pertence a PA monocromática e na outra não.*

Lema 8. *Tome $k,c \in \mathbb{N}$, com $k \geq 3$, e $r \in \mathbb{N}$. Assuma que para todo c, $w(k-1,c)$ está definido. Então para todo $r \leq c$, existe um $W_0(r)$, tal que para toda coloração $\varphi : [W_0(r)] \to [c]$, acontece uma, e somente uma, das seguintes afirmações:*

1. *Existem $a,\delta \in \mathbb{N}$, tais que*

$$\varphi(a) = \varphi(a+\delta) = \varphi(a+2\delta) = \cdots = \varphi(a+(k-1)\delta)$$

ou seja uma k-PA monocromática.

2. *Existe um primitivo* $a \in \mathbb{N}$ *e* $\delta_1, \delta_2, \ldots, \delta_r \in \mathbb{N}$ *tais que*

$$\varphi(a+\delta_1) = \varphi(a+2\delta_1) = \cdots = \varphi(a+(k-1)\delta_1)$$
$$\varphi(a+\delta_2) = \varphi(a+2\delta_2) = \cdots = \varphi(a+(k-1)\delta_2)$$
$$\vdots$$
$$\varphi(a+\delta_r) = \varphi(a+2\delta_r) = \cdots = \varphi(a+(k-1)\delta_r)$$

Isto é, temos $(k-1)$-PA's monocromáticas todas de diferentes cores, ou seja, para todo $i \neq j$, temos $\varphi(a+\delta_i) \neq \varphi(a+\delta_j)$.

Demonstração. A prova será por indução sobre r. Definimos $W_0(r)$ para ser o menor número que satisfaz o lema. Mostraremos que $W_0(r)$ possui um limite superior.

Caso $r = 1$, mostraremos que $W_0(1) \leq 2w(k-1,c)$. Seja $\varphi : [2w(k-1,c)] \to [c]$ uma coloração qualquer, vamos dividir $[W_0(1)]$ em duas partes de comprimento $w(k-1,c)$. A cardinalidade da segunda metade garante uma $(k-1)$-PA monocromática e a cardinalidade da primeiro metade garante um primitivo $a \in [W_0(1)]$ com respeito a tal PA, ou seja, temos a, a' e $\delta \in \mathbb{N}$, com $a = a' - \delta$, tais que (veja figura 28):

$$\varphi(a') = \varphi(a'+\delta) = \cdots = \varphi(a'+(k-2)\delta) = V$$
$$\varphi(a) = N$$

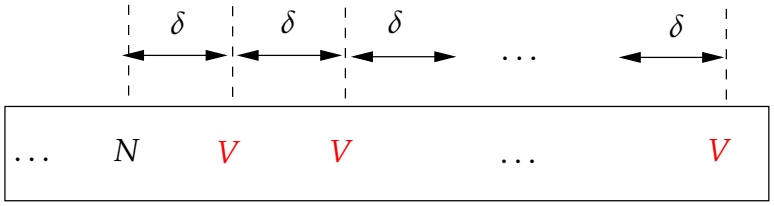

Figura 28: bloco $[W_0(1)]$ representado com seu primitivo.

Temos duas possilidades: caso $\varphi(a) = \varphi(a')$, então note que $a' - \delta, a', a' + \delta, \ldots, a' + (k-2)\delta$ é uma monocromática k-PA que satisfaz a afirmação 1. Caso $\varphi(a) \neq \varphi(a')$, como estamos com a segunda metade de $[W_0(1)]$, isto é, $w(k-1,c)$, logo por definição temos uma $k-1$ monocromática satisfazendo assim a afirmação 2.

Suponha que $W_0(r)$ existe, mostremos que $W_0(r+1) \leq U$, para algum U. Considere

$$U = 2W_0(r)w(k-1, c^{W_0(r)}),$$

tome $\varphi : [U] \to [c]$ uma coloração arbitária de $[U]$. Assim de maneira análoga ao que fizemos no caso $r = 1$, vamos dividir $U = 2W_0(r)w(k-1, c^{W_0(r)})$ em duas partes de cardinalidade $W_0(r)w(k-1, c^{W_0(r)})$. Fixemos nossos estudos para a segunda metade, para garantirmos a existência de nosso primitivo.

A segunda metade de $[U]$ é formada por exatamente $w(k-1, c^{W_o(r)})$ blocos de comprimento $W_0(r)$. Vamos denotá-los por $B_1, B_2, B_3, \ldots, B_{w(k-1,c^{W_0(r)})}$. A figura 29 representa a forma de um desses blocos, onde $C_1, C_2, \ldots, C_r$ representam as PA's em cada uma das possíveis r cores e a' é o primitivo delas.

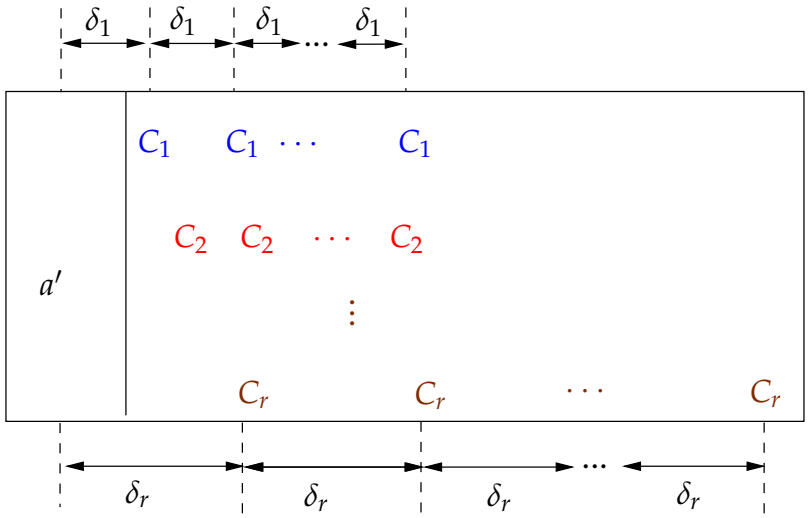

Figura 29: exemplo de um bloco de tamanho $W_0(r)$.

Como temos c cores e $W_0(r)$ elementos em cada bloco, logo existem $c^{W_0(r)}$ modos distintos de colorir cada um desses blocos. Tome $\chi : \left[B_{w(k-1,c^{W_0(r)})}\right] \to [c^{W_0(r)}]$ a coloração desses blocos. Por definição de $w(k-1, c^{W_o(r)})$, temos uma $(k-1)$-PA monocromática de blocos, todos de mesmo padrão de cor sob χ. Daí, existem $\alpha, \Delta' \in \mathbb{N}$ tais que: (veja a figura 30)

$$\chi(B_\alpha) = \chi(B_\alpha + \Delta') = \cdots = \chi(B_\alpha + (k-2)\Delta')$$

Olhemos para o bloco B_α que é colorido de uma das $c^{W_0(r)}$ formas e tem comprimento $W_0(r)$ que por hipótese de indução satisfaz as afirmações 1 ou 2 do lema. Estudemos ambos os casos.

- **1°caso**: Se a afirmação 1 vale, então teremos uma k-PA monocromática e obviamente $W_0(r+1)$ também está definido.

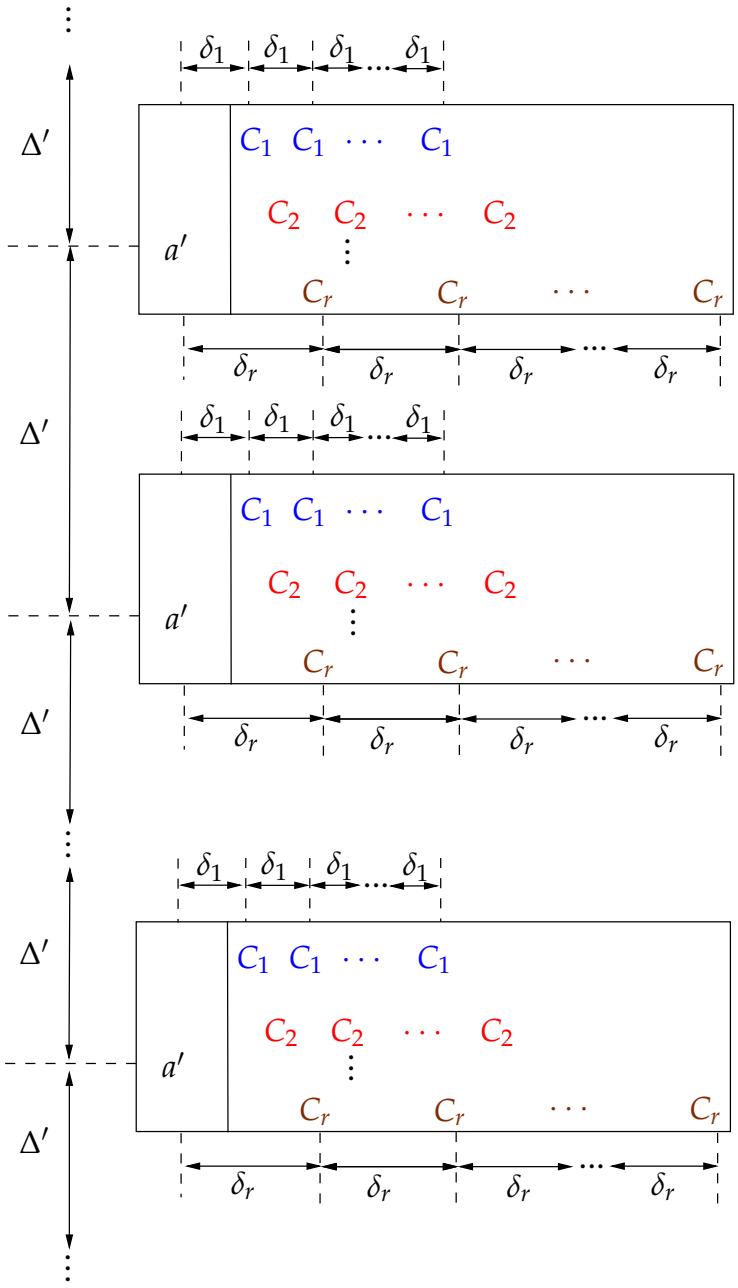

Figura 30: representando PA de blocos monocromáticas que distam Δ'.

- **2°caso**: Se a afirmação 2 vale, então teremos $(k-1)$ - PA's monocromáticas, todas de cores distintas e portanto existem $a', \delta_1, \delta_2, \ldots, \delta_r \in \mathbb{N}$ tais que:

$$\{a', a'+\delta_1, a'+2\delta_1, \ldots, a'+(k-1)\delta_1\} \subseteq B_\alpha$$

$$\{a', a'+\delta_2, a'+2\delta_2, \ldots, a'+(k-1)\delta_2\} \subseteq B_\alpha$$

$$\vdots$$

$$\{a', a' + \delta_r, a' + 2\delta_r, \ldots, a' + (k-1)\delta_r\} \subseteq B_\alpha$$

ou seja, uma k-PA no bloco dos quais, com exceção, do primitivo a', os $(k-1)$ termos subsequentes possuem a mesma cor, isto é,

$$\varphi(a' + \delta_1) = \varphi(a' + 2\delta_1) = \cdots = \varphi(a' + (k-1)\delta_1) = C_1$$

$$\varphi(a' + \delta_2) = \varphi(a' + 2\delta_2) = \cdots = \varphi(a' + (k-1)\delta_2) = C_2$$

$$\vdots$$

$$\varphi(a' + \delta_r) = \varphi(a' + 2\delta_r) = \cdots = \varphi(a' + (k-1)\delta_r) = C_r$$

onde cada um dos C_i's, com $1 \leq i \leq r$ são todas as possíveis cores e note que $C_i \neq \varphi(a')$, pois senão teríamos uma k-PA monocromática. Como a distância entre os blocos de mesma coloração sobre χ é Δ' e pelo fato de cada um desses blocos possuir exatamente $W_0(r)$ elementos, então a distância Δ entre dois elementos correspondentes de mesma cor é $\Delta = \Delta' \cdot W_0(r)$, daí temos progressões aritméticas monocromática formadas por um elemento de cada bloco, isto é,

$$\varphi(a' + \delta_1) = \varphi(a' + \Delta + \delta_1) = \cdots = \varphi(a' + (k-2)\Delta + \delta_1) = C_1;$$

$$\varphi(a' + \delta_2) = \varphi(a' + \Delta + \delta_2) = \cdots = \varphi(a' + (k-2)\Delta + \delta_2) = C_2;$$

$$\vdots$$

$$\varphi(a' + \delta_r) = \varphi(a' + \Delta + \delta_r) = \cdots = \varphi(a' + (k-2)\Delta + \delta_r) = C_r.$$

Lembramos que estamos com a segunda metade de U, assim garantimos um primitivo na primeira metade. Seja a tal primitivo, onde $a = a' - \Delta' \cdot W_0(r)$, consideremos a' o primitivo do primeiro bloco de $w(k-1, c^{W_0(r)})$, veja a figura 31. Então temos que

$$\varphi(a + \Delta + \delta_1) = \varphi(a + 2\Delta + 2\delta_1) = \cdots = \varphi(a + (k-1)\Delta + (k-1)\delta_1) = C_1;$$

$$\varphi(a + \Delta + \delta_2) = \varphi(a + 2\Delta + 2\delta_2) = \cdots = \varphi(a + (k-1)\Delta + (k-1)\delta_2 = C_2;$$

$$\vdots$$

$$\varphi(a + \Delta + \delta_r) = \varphi(a + 2\Delta + 2\delta_r) = \cdots = \varphi(a + (k-1)\Delta + (k-1)\delta_r) = C_r.$$

Cada uma dessas r progressões monocromáticas possuem uma cor diferente. Agora analisando a progressão aritmética dos primitivos de cada um dos $w(k-1, c^{W_0(r)})$ blocos existentes na segunda metade de $[U]$, isto é, $\{a + \Delta, a + 2\Delta, \ldots, a + (k-1)\Delta\}$, note

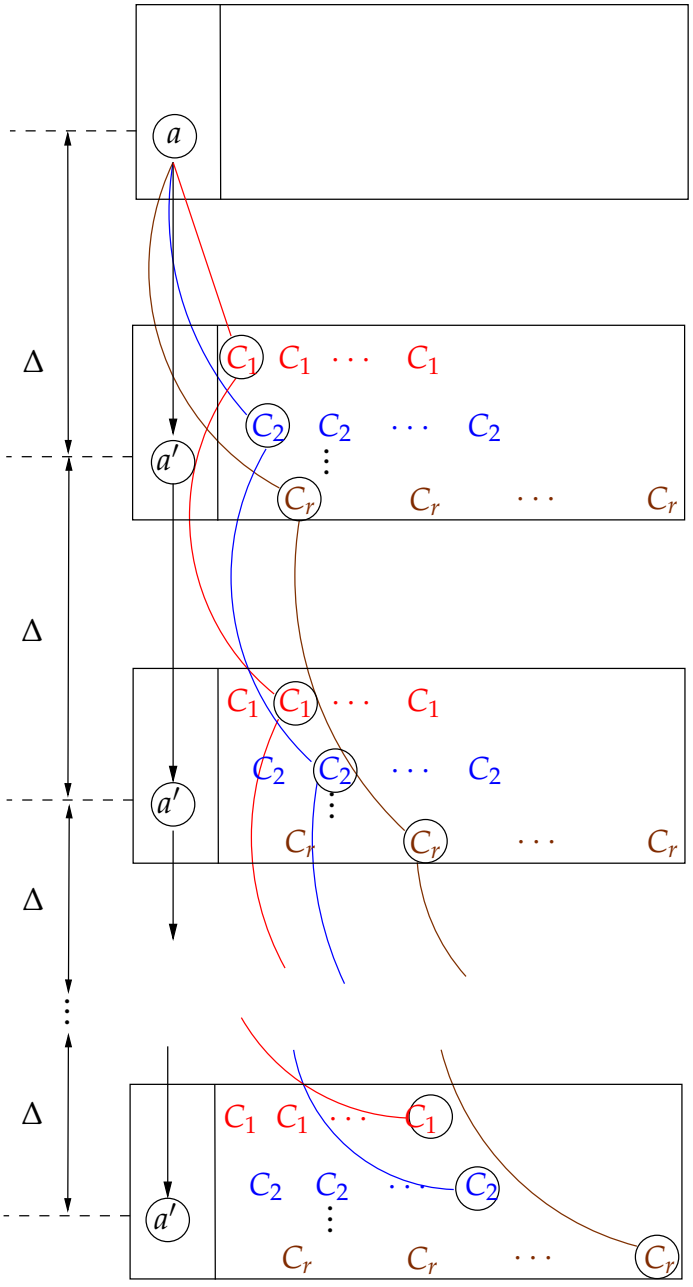

Figura 31: a primitivo das progressões aritméticas monocromáticas

que esses elementos possuem a mesma coloração sob χ, de sorte que todos os a's, da figura 31, devem ter a mesma cor e portanto

$$\varphi(a+\Delta) = \varphi(a+2\Delta) = \cdots = \varphi(a+(k-1)\Delta) = C_0.$$

Afirmamos que C_0 é distinto de todas as C_r's cores anteriores. Isto porque para todo i, com $1 \leq i \leq r$, têm-se $\varphi(a) \neq \varphi(a+\delta_i)$, logo temos $r+1$ PA's monocromáticas de

tamanho $k-1$ e todas de cores distintas partidas do mesmo primitivo a, conforme queríamos provar. □

Vamos reescrever o teorema 13 e demonstrá-lo.

Teorema 16 (Teorema de Van der Waerden). *Dados $k, c \in \mathbb{N}$, existe $W = w(k,c) \in \mathbb{N}$, tal que para toda c-coloração $\varphi : [W] \to [c]$, existe uma k-PA monocromática, isto é, temos $a, \delta \in \mathbb{N}$, com $\delta \neq 0$, tais que*

$$\varphi(a) = \varphi(a+\delta) = \varphi(a+2\delta) = \cdots = \varphi\big(a+(k-1)\delta\big)$$

Demonstração. A prova será por indução em k, mostrando que para todo c, $w(1,c)$ existe e supondo que para todo c, $w(k-1,c)$ existe, então isso implica que também para todo c, $w(k,c)$ existe.

Caso $k = 1$, conforme já vimos, temos que $w(1,c) = 1$ e além disso sabemos que $w(2,c) = c+1$, para qualquer c.

Suponha que para todo c, $w(k-1,c)$ existe. Fixando c temos que pelo lema 8, que para todo $r \in \mathbb{N}$, com $r \leq c$ e $W_0(r) \in \mathbb{N}$, qualquer que seja a coloração $\varphi : [W_0(r)] \to [c]$, têm-se uma k-PA monocromática ou exatamente r monocromáticas $(k-1)$ PA's todas de cores distintas, além de um primitivo a, cuja cor difere de todas as r cores. Logo, se pegarmos $r = c$, então existirá um $W_0(c)$ que goza de alguma dessas duas condições, de sorte que basta analisarmos o caso em que há um número c de $(k-1)$-PA's monocromáticas de cores diferentes. O primitivo a deve necessariamente ter uma das c cores, formando assim uma k-PA monocromática com alguma dessas c monocromáticas $(k-1)$ PA's existentes, de sorte que $w(k,c) \leq W_0(r)$. Veja a figura 32, onde a cor vermelha representa a k-PA monocromática. □

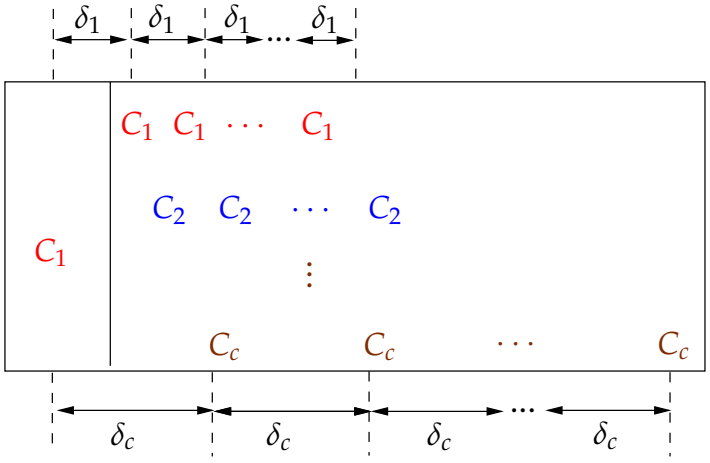

Figura 32: representando a k-PA monocromática existente.

5

CONCLUSÃO

Os trabalhos desenvolvidos principalmente no começo do século XX, foram de extrema importância para muitos avanços nos estudos de progressões aritméticas em subconjuntos dos naturais. Além do próprio Teorema de Van der Waerden, podemos destacar o Teorema de Szemerédi, que foi provado e demonstrado pelo matemático Húngaro Endre Szemerédi (Budapest-1940) em 1975, que diz que todo subconjunto dos inteiros com densidade positiva contém progressões aritméticas longas. Outro destaque também vai para outro matemático Húngaro, Paul Erdős (1913-1996) sobre progressões aritméticas. Erdős publicou uma conjectura afirmando que se A é um subconjunto dos naturais em que a soma de seus recíprocos diverge, isto é,

$$\sum_{n \in A} \frac{1}{n} = +\infty$$

então A contém progressões aritméticas de comprimento arbitrariamente longo. Inclusive Erdős oferecia uma quantia em dinheiro a quem resolve-se esse problema.

Na primeira década do século XXI, temos conforme ressaltado no capítulo 4, um teorema provado pelos matemáticos Ben Green e Terence Tao em 2004, no qual se afirma que existem progressões aritméticas de comprimentos arbitrariamente longo no conjunto dos números primos. Esse teorema é um caso particular da conjectura de Erdős, no qual o conjunto A é o conjunto dos naturais primos.

Esses resultados mencionados nos parágrafos anteriores são exemplos da evolução decorrente principalmente dos trabalhos desenvolvidos no começo do século XX, que contribuiram para a criação e desenvolvimento de várias áreas de pesquisa na matemática, tais como a Combinatória Extremal, Combinatória Aditiva e a Teoria Ergódica, por exemplo. O próprio Teorema de Van der Waerden, que foi demonstrado em 1927 como um resultado essencialmente da Teoria dos Números e da Combinatória, em 1977, o matemático israelense Hillel Furstenberg, redemonstrou o Teorema de Szeme-

rédi recorrendo a métodos e resultados da Teoria Ergódica. De sorte que, ao longo das últimas décadas começaram a surgir algumas relações entre a Teoria dos Números, a Combinatória e os Sistemas Dinâmicos Topológicos. O próprio trabalho de Green e Tao utilizam-se de técnicas e argumentos da Teoria Ergódica em um enunciado de natureza aritmética e combinatória.

Dos trabalhos mais recentes sobre progressões aritméticas, deixamos indicado ao leitor um artigo publicado em 2017 (veja [6]), pelos matemáticos Jordan Stuart Ellberg e Dion Gijswijt, que diz respeito a subconjuntos de tamanho arbitrariamente grande em grupos abelianos sem progressões aritméticas de três termos.

Gostaria de fazer uma provocação ao leitor, especialmente aos professores do Ensino Médio, a terem uma visão pluralista da Análise Combinatória. Área que não se restringe apenas em técnicas de contagem como arranjos, permutações e combinações, algo frequentemente ensinado e encontrado nos materiais didáticos. Tomamos como exemplos o príncipio da casa dos pombos, conteúdo do qual não se faz presente, em grande maioria, dos currículos escolares, bem como noções sobre a Teoria dos Grafos. Poderíamos questionar se exemplos como o da reunião com n pessoas (exemplo 2, página 10), da festa com 17 pessoas (exemplo 10, página 30), das posições dos cavalos pretos e brancos (visto no capítulo 3, página 25), entre outros, podem despertar nos alunos, a curiosidade e o racíocinio em resolver problemas de matemática que não requerem uso de uma fórmula, algoritmo para sua solução.

Para finalizar gostaria de ressaltar que tanto a Teoria dos Números como a Combinatória, assim como as demais áreas da Matemática, não podem ser consideradas como finalizadas, e sim como áreas que devem ser permanentemente completadas.

A

APÊNDICE A

A.1 ORDEM LEXOGRÁFICA

Definição 9 (boa-ordem). *$(A, \preceq)$ é boa ordem, se é uma ordem total e todo subconjunto não vazio de A tem mínimo. A notação $a \prec b$ abrevia $a \preceq b$ e $a \neq b$.*

A propriedade útil da boa-ordem é que ela permite provas por indução, como nos naturais.

Teorema 17. *Seja $(A, \preceq)$ uma boa ordem e B um subconjunto de A tal que:*

$$\forall s \in A(\forall t \in A(t \prec s \Rightarrow t \in B) \Rightarrow s \in B) \tag{A.1}$$

então $B = A$.

Demonstração. A prova é por contradição. Sejam A,B e $\preceq$ como no enunciado do teorema. Assuma que $B \subsetneq A$, considere

$$A \setminus B = \{a \in A; a \notin B\} \neq \emptyset \tag{A.2}$$

e tome m o menor elemento da $A \setminus B$, com respeito a ordem $\preceq$, o qual existe em virtude da boa ordenação.

De m ser o menor elemento de A que não pertence a B, temos

$$\forall t \in A(t \prec m \Rightarrow t \in B) \tag{A.3}$$

daí por A.1, temos que $m \in B$, o que é uma contradição. □

A.1.1 *Indução em* $\mathbb{N}\times\mathbb{N}$

O conjunto $\mathbb{N} \times \mathbb{N}$ com a ordem lexicográfica $\preceq$,

$$(x, y) \preccurlyeq (a, b) \text{ se } \begin{cases} x < a & \text{ou} \\ x = a & \text{e } y \leq b \end{cases}$$

sendo $\leq$ a relação usual em $\mathbb{N}$, é boa ordem.

Para mais detalhes da ordem lexicográfica e suas aplicações recomendamos ao leitor [13].

B

APÊNDICE B

B.1 GRUPO

Um grupo $(G, *)$ é um conjunto G (não vazio) munido de uma operação $*$, tal que:

1. $(x * y) * z = x * (y * z), \forall x, y, z \in G$ (associativa);
2. $\exists e \in G; x * e = e * x = x, \forall x \in G$ (elemento neutro);
3. $\forall x \in G, \exists y \in G; x * y = y * x = e$ (elemento inverso).

Os elementos neutro e inverso são únicos. Da associatividade, o elemento

$$x^n = \underbrace{x \cdot x \cdots x}_{n}$$

fica bem definido. Se $n < 0$, tomamos $x^n = \left(x^{-1}\right)^{-n}$ e, para $n = 0$, $x^0 = 1$, $\forall x \in G$. Assim $x^n \cdot x^m = x^{n+m}, \forall m, n \in \mathbb{Z}$ e $\forall x \in G$.

Considere $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, onde $\overline{j} = \{j + kp; k \in \mathbb{Z}\}$ e $j \in \{1, 2, \ldots, p-1\}$. Temos que $(\mathbb{Z}_p^*, \cdot)$, onde a operação "$\cdot$" é a multiplicação $\pmod p$, é grupo, já que todo elemento de $\mathbb{Z}_p^*$ é invertível, possui elemento neutro e a multiplicação $\pmod p$ é associativa.

Seja G um grupo e $g \in G$. Definimos o conjunto gerado por g, denotado por $\langle g \rangle$, como sendo o conjunto de todas as potências inteiras de g, ou seja,

$$\langle g \rangle = \{g^n; n \in \mathbb{Z}\}.$$

Para a prova desses resultados e demais informações sobre a teoria de grupos, recomendamos a leitura de [5] e [8].

C

APÊNDICE C

Teorema 18 (**Teorema Fundamental da Arimética**)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Apresentamos nesse Apêndice apenas a prova da unicidade do Teorema enunciado acima, sem usar o Teorema de Bézout, que se encontra disponível em [14] e [1]. Para a prova completa do Teorema Fundamental da Aritmética, recomendemos ao leitor [8].

Demonstração. Suponha que $s > 1$ seja o menor inteiro positivo que é o produto de números primos e feito de dois modos distintos. Caso s seja primo, evidentemente que sua decomposição é ele próprio, assim deve haver pelo menos dois primos em cada decomposição de s.

$$s = p_1 \cdot p_2 \cdots p_m$$

$$= q_1 \cdot q_2 \cdots q_n$$

Se qualquer $p_i = q_j$, então $\frac{s}{p_i} = \frac{s}{q_j}$ seria um inteiro positivo menor do que s, que é maior que 1 e também teria duas decomposições distintas. Mas isso é uma contradição, pois supomos que s era tal menor inteiro positivo. Portanto, devemos ter $p_i \neq q_j$, $\forall i, j$.

Sem perda de generalidade, tomemos $p_1 < q_1$ (se esse não for o caso, basta mudar as designações de p e q). Considere $t = (q_1 - p_1) \cdot (q_2 \cdots q_n)$, portanto temos $1 < q_2 \leq t < s$. Daí, t deve ter uma única decomposição em primos. Por rearranjo, temos

$$\begin{aligned} t = & \quad q_1(q_2 \cdots q_n) - p_1(q_2 \cdots q_n) \\ = & \quad\quad s - p_1(q_2 \cdots q_n) \\ = & \quad p_1 p_2 \cdots p_m - p_1(q_2 \cdots q_m) \\ = & \quad p_1[(p_2 \cdots p_m) - (q_2 \cdots q_n)] \end{aligned}$$

Afirmamos que $u = (p_2 \cdots p_m) - (q_2 \cdots q_n)$ é positivo. De fato, pois caso fosse negativo ou zero, então seu produto com p_1 também seria, todavia seu produto vale t que é positivo. Logo u é igual a 1 ou é decomposto em fatores primos. Em ambos os casos, $t = p_1 u$ produz uma decomposição de t, daí p_1 aparece na decomposição em fatores primos de t.

Se $q_1 - p_1 = 1$, então a decomposição de t seria $t = q_2 \cdots q_n$, o que implica $p_1 = q_i$ para algum $j = 2, 3, \ldots, n$. Assim $q_1 - p_1 \neq 1$, então podemos escrever $q_1 - p_1 = r_1 \cdots r_h$, onde cada r_l é primo, com $l = 1, \ldots, h$. Assim t pode ser escrito como

$$(r_1 \cdots r_k) \cdot (q_2 \cdots q_n).$$

Como p_1 aparece na decomposição de t e não é nenhum dos $q_2, \ldots, q_n$, então ele deve ser algum dos $r_1, r_2, \ldots, r_h$. Isso significa que p_1 é um fator de $(q_1 - p_1)$, então existe um inteiro positivo k, tal que $p_1 k = (q_1 - p_1)$, daí

$$p_1 k = (q_1 - p_1) \Rightarrow p_1(k+1) = q_1$$

mas isso acarreta que q_1 possui uma decomposição em fatores primos, então q_1 não é primo. Essa contradição mostra que s não possui duas decomposições em fatores primos distintos. □

BIBLIOGRAFIA

[1] Ahmet G Agargün e Colin R Fletcher, *The fundamental theorem of arithmetic dissected*, The Mathematical Gazette **81** (1997), nº 490, 53–57.

[2] Augusto César de Oliveira Morgado, João Bosco Pitombeira de Carvalho, Paulo Cezar Pinto Carvalho e Pedro Fernandez, *Análise combinatória e probabilidade*, Sociedade Brasileira de Matemática, Rio de Janeiro (1991).

[3] José Plínio de Oliveira Santos, *Introdução à teoria dos números*, Instituto de Matemática Pura e Aplicada, 1998.

[4] José Plínio de Oliveira Santos, Margarida Pinheiro Mello e Idani Theresinha Calzolari Murari, *Introdução à análise combinatória*, Ed. Ciencia Moderna, 2007.

[5] Hygino H Domingues e Gelson Iezzi, *Álgebra moderna*, Atual Editora (1982).

[6] Jordan S Ellenberg e Dion Gijswijt, *On large subsets of F_q^n with no three-term arithmetic progression*, Annals of Mathematics (2017), 339–343.

[7] William Gasarch, Clyde Kruskal e Andy Parrish, *Purely combinatorial proofs of van der Waerden-type theorems*, Draft book (2010).

[8] Abramo Hefez, *Aritmética*, Rio de Janeiro: Sociedade Brasileira de Matemática (2014), 42.

[9] Paul R Herwig, Marijn JH Heule, P Martijn van Lambalgen e Hans van Maaren, *A new method to construct lower bounds for van der Waerden numbers*, the electronic journal of combinatorics **14** (2007), nº 1, 6.

[10] Summer Lynne Kisner, *Schur's Theorem and Related Topics in Ramsey Theory*, (2013).

[11] Allan Weslley Padua, *O Teorema de van der Waerden.*, Trabalho de Conclusão de Curso, Universidade Federal de Itajubá - MG (2016).

[12] Stanisław P Radziszowski et al., *Small ramsey numbers*, Electron. J. Combin **1** (1994), nº 7.

[13] Kenneth H Rosen, *Matemática discreta e suas aplicações*, Grupo A Educação, 2009.

[14] Wikipedia contributors, *Fundamental theorem of arithmetic — Wikipedia, The Free Encyclopedia*, 2019, https://en.wikipedia.org/w/index.php?title=Fundamental_theorem_of_arithmetic&oldid=894336481, [Online; acesso em 22-05-2019].