UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DÉBORA RIBEIRO VALADÃO

UM ESTUDO SOBRE A PARIDADE DA SOMA DE COEFICIENTES BINOMIAIS

PATO BRANCO
2022

DÉBORA RIBEIRO VALADÃO

UM ESTUDO SOBRE A PARIDADE DA SOMA DE COEFICIENTES BINOMIAIS

A study on the parity of the sum of binomial coefficients

Trabalho de Conclusão de Curso de graduação apresentado como requisito parcial à obtenção do título de Licenciado em Matemática do Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. André Guerino Castoldi

PATO BRANCO
2022

DÉBORA RIBEIRO VALADÃO

UM ESTUDO SOBRE A PARIDADE DA SOMA DE COEFICIENTES BINOMIAIS

Trabalho de Conclusão de Curso de graduação apresentado como requisito parcial à obtenção do título de Licenciado em Matemática do Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 14 de junho de 2022

Prof. Dr. André Guerino Castoldi
Universidade Tecnológica Federal do Paraná

Prof. Dr. Carlos Alexandre Ribeiro Martins
Universidade Tecnológica Federal do Paraná

Prof. Dr. Waldir Silva Soares Junior
Universidade Tecnológica Federal do Paraná

PATO BRANCO
2022

“Dedico este trabalho à minha família e amigos, pelos momentos de ausência."

AGRADECIMENTOS

Difícil missão a de comtemplar todos que fizeram parte da caminhada feita na Universidade. Dito isso, gostaria de agradecer a todos que de alguma forma colaboraram para que chegássemos a esse momento. Agradeço ao meu orientador Prof. Dr. André Guerino Castoldi, pela sabedoria com que me guiou nesta trajetória. Aos meus colegas de sala. Ao Departamento do Curso e professores que o compõem, pela cooperação. Gostaria de agradecer à minha família e amigos mais próximos, pois sem o apoio e amparo teria sido muito mais árduo vencer mais esse desafio e agradecer a paciência em lidar comigo em momentos difíceis. Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa. Agradeço por fim a UTFPR.

RESUMO

Os coeficientes binomiais aparecem em diversas áreas da matemática, sendo que a caracterização de uma fórmula para determinar a soma de coeficientes binomiais consecutivos em uma linha do Triângulo de Pascal ainda permanece como um problema sem solução. Existem diversas interpretações significativas da soma de coeficientes binomiais em diversas linhas de pesquisa, como na teoria de informação, na teoria de codificação, na geometria discreta e na combinatória. Este trabalho ter por objetivo analisar a paridade da soma dos coeficientes binomiais em uma linha do Triângulo de Pascal, apresentando uma revisão da contribuição de importantes matemáticos para o tema, como Blaise Pascal e François Lucas. Além disso, é apresentado uma aplicação da paridade da soma de coeficientes binomiais no estudo da paridade de RT-bolas. Para isso, foi realizada uma revisão bibliográfica dos trabalhos publicados pelos pesquisadores da área, assim reunindo os resultados já alcançados ao longo do tempo. Resultados significativos da caracterização da paridade da soma de coeficientes binomiais são apresentados, porém o problema continua em aberto, podendo ser estudado futuramente.

Palavras-chave: coeficientes binomiais; paridade; soma de coeficientes binomiais; Triângulo de Pascal; RT-bolas.

ABSTRACT

The binomial coefficients appear in many areas of mathematics, and the characterization of a formula to determine the sum of consecutive binomial coefficients in a row of Pascal's Triangle still remains a problem without a solution. There are several significant interpretations of the sum of binomial coefficients in different fields of research, as in information theory, coding theory, discrete geometry and combinatorics. This work has as goal to analyze the parity of the sum of binomial coefficients in a row of Pascal's Triangle, presenting a review of the contribution of important mathematicians, such as Blaise Pascal and François Lucas, to the theme. Furthermore, it is presented an application of the parity of binomial coefficients in the study of the parity of RT-balls. Therefore, a bibliographic review of the works published by researchers in the field was carried out, thus bringing together the results already achieved over time. Significant results of parity characterization of the sum of binomial coefficients are presented, however, the problem remains open, and it can be investigated in the future.

Keywords: binomials coefficients; parity; sum of binomial coefficients; Pascal's Triangle; RT-balls.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\|A\|$	Cardinalidade do conjunto A.
$\binom{n}{k}$	Coeficiente binomial.
$\alpha_q(k,t,m)$	Soma de coeficientes binomiais consecutivos na linha m do Triângulo de Pascal.
$\mathcal{A}^p_{n,k}$	Número de índices j tal que $b_j > a_j$ na expansão de n e k na base p.
$\nu_p\left(\binom{n}{k}\right)$	Valorização p-ádica de $\binom{n}{k}$
$(k)_2$	Representação de k como número binário.
P	Conjunto parcialmente ordenado (poset).
RT	Poset Rosenbloom-Tsfasman.
E^c	Complementar do subconjunto E.
$\langle A \rangle$	O ideal gerado por A.
$\Omega_j(i)$	Número de ideais do RT-poset $[m \times s]$ com cardinalidade i e com exatamente j elementos maximais.
$\mathbb{Z}_q$	Conjunto dos inteiros módulo q.
$\mathbb{Z}_q^n$	Conjunto de todas as n-uplas sobre $\mathbb{Z}_q$.
$d_{RT}(x,y)$	RT-distância entre x e y.
$supp(x)$	Suporte do vetor x.
$B^{RT}(x,R)$	RT-bola de centro em x e raio R.
$V_q^{RT}(m,s,R)$	Cardinalidade da RT-bola $B^{RT}(x,R)$.

SUMÁRIO

1 INTRODUÇÃO

Neste trabalho, o problema de determinar a paridade da soma dos coeficientes binomiais é estudado por meio de uma revisão bibliográfica sobre o assunto.

O matemático francês François Édouard Anatole Lucas iniciou o estudo deste, em 1878, determinando os coeficientes binomiais módulo um número primo (LUCAS, 1878). Esse resultado ficou conhecido como o Teorema de Lucas. Nascido ao norte da França na cidade de Amiens, em 1842, Lucas ingressou em uma renomada instituição de ensino francesa, a École Normale Supérieure em 1861, na qual permaneceu até 1864. Entre 1870 e 1871, Lucas serviu o exército francês na guerra contra a Prússia, mas com a derrota, ele voltou para a carreira de professor de matemática.

Lucas desenvolveu vários trabalhos em diversas áreas da matemática, em especial na Teoria dos Números (PONTES; GOBBI; SOUSA, 2018). Com os estudos da divisibilidade e fatoração, definiu a série de Lucas, a qual é uma generalização da sequência de Fibonacci. Além de uma demonstração da recíproca do Pequeno Teorema de Fermat. Na matemática recreativa, Lucas apresentou diversos trabalhos relacionados a Torre de Hanói e ao quebra-cabeça de Baguenaudier em vários volumes do chamado Recréations Mathématiques.

Outro importante matemático francês na área de combinatória foi Blaise Pascal. Nascido na cidade francesa de Clermont em 1623, foi educado em casa por seu próprio pai, o qual decidiu por não ensinar matemática ao filho até que este completasse 15 anos. Porém, movido pela curiosidade, Blaise começou a estudar geometria por conta própria aos 12 anos e após descobrir que a soma dos ângulos de um triângulo é igual a dois ângulos retos, ganhou uma cópia do livro de Euclides de seu pai. Para ajudar no trabalho do pai, Pascal inventou a primeira calculadora digital chamada de Pascaline (O'CONNOR; ROBERTSON, 1996) .

Na combinatória, Pascal apresentou um teorema para o cálculo de coeficientes binomiais, os quais podem ser representados em um arranjo conhecido como Triângulo de Pascal. O'Connor e Robertson (1996) destacam que apesar de não ser o primeiro a estudar o triângulo de Pascal, este foi o seu trabalho de mais importância na área. Além disso, seu trabalho na área foi o que levou Newton a sua descoberta do Teorema Binomial para potências que são números racionais. Os coeficientes binomiais são representados no Teorema Binomial, o qual foi mostrado por Euclides (COOLIDGE, 1949) para potência 2, sendo generalizado para potência n com estudos mais aprofundados. Devido a representação dada por Pascal dos coeficientes binomiais e ao estudo da paridade realizado por Lucas, pode-se representar a paridade como um fractal (LKUNG, 1976).

Com os trabalhos de Lucas, Kummer (1852) e outros estudiosos da área, foi possível determinar a paridade de coeficientes binomiais e assim, buscou-se determinar um modo de calcular a paridade da soma de coeficientes binomiais em determinada linha do Triângulo de Pascal. Apesar de ainda não ter sido obtida uma fórmula fechada para calcular a soma de m coeficientes consecutivos, diversos casos específicos, como o Teorema da Linhas, puderam ser estudados, sendo estes apresentados nesse trabalho.

A partir da paridade da soma de coeficientes binomiais determinada, pode-se utilizar a mesma para determinar a paridade das RT-bolas, as quais são utilizadas na RT-métrica para o estudo de coberturas em RT-espaços (CASTOLDI, 2012). A RT-métrica foi determinada sendo uma generalização da métrica de Hamming, feita por Rosenbloom e Tsfasman (1997). Outra forma de generalizar a métrica de Hamming foi apresentado por Brualdi, Graves e Lawrence (1995) definindo assim as métricas "posets"(conjuntos parcialmente ordenados), sendo que estas podem generalizar a RT-métrica, e são utilizadas para o estudo de códigos perfeitos.

O foco principal deste trabalho é apresentar um estudo sobre a paridade de coeficientes binomiais consecutivos em uma linha do triângulo de Pascal. Desse modo, objetiva-se com este revisar os conceitos básicos de combinatória essenciais para este trabalho, descrever o contexto histórico do problema, analisar as possíveis generalizações da paridade dos coeficientes binomiais, e apresentar uma aplicação da paridade da soma de coeficientes binomiais. Alguns resultados apresentados nesse trabalho já foram abordados no artigo de iniciação científica "A paridade da soma de coeficientes binomiais"(VALADÃO; CASTOLDI, 2021).

Este trabalho é organizado da seguinte forma:

O primeiro capítulo aborda os coeficientes binomiais, sendo primeiramente feita uma revisão de conceitos básicos da Análise Combinatória, assim como a apresentação do Triângulo de Pascal e o Teorema Binomial, os quais são importantes para a continuidade do trabalho.

Desse modo, no segundo capítulo é aprofundado o tema sobre os coeficientes binomiais módulo um número primo, apresentando o Teorema de Kummer e o Teorema de Lucas. A partir disso, é estudado a paridade da soma de coeficientes binomiais e as generalizações conhecidas da mesma.

Por último, no terceiro capítulo é apresentada uma aplicação da paridade da soma de coeficientes binomiais, a qual pode ser utilizada para determinar a paridade de uma RT-bola, considerando a métrica de Rosenbloom e Tsfasman.

1.1 Objetivos

1.1.1 Objetivo Geral

Analisar a paridade da soma dos coeficientes binomiais em uma linha do Triângulo de Pascal e suas aplicações.

1.1.2 Objetivos Específicos

- Revisar os resultados básicos de análise combinatória;
- Analisar a paridade dos coeficientes binomiais e suas generalizações.
- Aplicar os resultados sobre a paridade da soma de coeficientes binomiais na determinação da paridade de RT-bolas.

1.2 Justificativa

Sejam q, k, t e m números inteiros não negativos. A caracterização da fórmula fechada para determinar

$$\alpha_q(k,t,m) = \sum_{i=k}^{t}(q-1)^i\binom{m}{i}$$

permanece sendo um problema sem solução, sendo apenas dois casos conhecidos $\alpha_2(0,m,m) = 2^m$ e $\alpha_2(0,t,t+1) = 2^t$. Existem interpretações significativas dos números $\alpha_q(k,t,m)$ quando $k = 0$ em algumas linhas de pesquisa. Na teoria de informação, $\alpha_2(0,t,m)$ é um número de palavras de comprimento m com o peso de Hamming menor ou igual a t. Já na teoria de codificação, $\alpha_2(0,t,m)$ pode ser interpretada como a dimensão dos códigos Reed-Muller de comprimento 2^m e distância mínima 2^{m-t} (MACWILLIAMS; SLOANE, 1977). Enquanto isso, na geometria discreta, $\alpha_2(0,t,m)$ corresponde ao número máximo de regiões nas quais m hiperplanos dividem $\mathbb{R}^t$ (ORLIK; TERAO, 2013) e (SCHLÄFLI, 1901). Ademais, na combinatória, $\alpha_2(k,t,m)$ aparece como a soma de coeficientes binomiais consecutivos na linha m do Triângulo de Pascal. Percebe-se com isto, que há diversos tipos de aplicações para o tema e evidencia-se a importância de investigar o mesmo. Além disso, pode-se perceber a defasagem de estudo sobre o tema no Brasil, sendo raro encontrar um artigo ou tese sobre o mesmo em português, desse modo se faz necessário o uso de artigos em línguas estrangeiras para conseguir certo aprofundamento no tema.

2 OS COEFICIENTES BINOMIAIS

Existem dois tipos de problemas na Análise Combinatória, sendo estes demonstrar a existência de subconjuntos de elementos em um conjunto finito ou contar os subconjuntos de um conjunto finito, sendo que em ambos deve-se satisfazer condições específicas. Para que isso seja possível de ser realizado, utiliza-se algumas técnicas de contagem: princípio aditivo e multiplicativo, dupla contagem, permutação, combinação.

A fim de que as demonstrações presentes nesse trabalho sejam entendidas, faz-se necessária a revisão de alguns conceitos e fórmulas da Análise Combinatória. Para realizar as demonstrações deste capítulo, foi utilizado como base o livro Introductory Combinatorics (BRUALDI, 2004), sendo que as demonstrações retiradas de outra fonte serão devidamente referenciadas quando citadas.

Assim, neste capítulo são trabalhados os conceitos dos princípios de contagem (aditivo, multiplicativo e dupla contagem), assim como a conceituação de permutações e combinações para revisar os conceitos mais básicos de combinatória. Em seguida, apresenta-se o Triângulo de Pascal, juntamente com a fórmula de Pascal, o Teorema das Linhas e o Teorema Binomial.

2.1 Princípios de Contagem

Os princípios aditivo e multiplicativo são os princípios mais básicos de contagem e estão relacionados com as operações aritméticas de adição e multiplicação. O primeiro princípio afirma que o todo é igual a soma das suas partes.

Princípio Aditivo: Sejam A_1,...,A_n conjuntos dois a dois disjuntos, cuja cardinalidade de A_i é a_i. A união $\bigcup\limits_{i=1}^{n} A_i$ possui $\sum\limits_{i=1}^{n} a_i$ elementos.

O segundo princípio é formulado como consequência do Princípio Aditivo, já que a multiplicação de inteiros nada mais é que uma sucessão de somas.

Princípio Multiplicativo: Se A_1 é um conjunto com d_1 elementos e A_2 é um conjunto com d_2 elementos, então o conjunto $A_1 \times A_2$ dos pares ordenados (a, b), com $a \in A_1$ e $b \in A_2$, tem $d_1 \cdot d_2$ elementos.

A seguir, apresenta-se um exemplo no qual aplica-se ambos os princípios apresentados anteriormente.

Exemplo 2.1. Deseja-se contar quantos números naturais de 3 algarismos distintos são pares. Para se ter um número par, pode-se escolher o algarismo da unidade de 5 maneiras (0, 2, 4, 6 e 8). Como se quer um número de 3 algarismos, não se pode ter 0 no algarismo da centena. Dessa forma, teremos dois casos, quando 0 for escolhido para o algarismo da unidade e quando não o for. No primeiro caso, o primeiro algarismo poderá ser escolhido de 9 maneiras, e o segundo de 8 maneiras. Sendo assim, pelo Princípio Multiplicativo teremos um total de $9 \cdot 8 \cdot 1 = 72$ números.

Já no segundo caso, teremos que o último algarismo pode ser escolhido de 4 maneiras, o primeiro de 8, pois 0 não pode ser escolhido, e o segundo pode ser escolhido de 8 formas, pois não pode-se escolher os dois números escolhidos para o primeiro e terceiro algarismo. Novamente pelo Princípio Multiplicativo, tem-se $8 \cdot 8 \cdot 4 = 256$ números pares com o último número diferente de 0.

Portanto, pelo Princípio Aditivo, tem-se $72 + 256 = 328$ números pares de 3 algarismos distintos.

Outro princípio utilizado para resolver-se problemas de contagem é o Princípio da Dupla Contagem, sendo este enunciado abaixo. Esse princípio é aplicado em problemas de combinatória, sendo usado para contar de duas formas o número de elementos de um conjunto e assim demonstrar uma identidade partindo do fato que ambas as formas resultam no mesmo número.

Princípio da Dupla Contagem: Se os elementos de um conjunto são contados de duas formas diferentes, então os resultados das contagens são iguais.

Exemplo 2.2. Neste exemplo apresenta-se o conhecido lema do aperto de mãos. Suponha que um número finito de pessoas encontra-se numa festa e algumas trocam apertos de mãos. Assuma que nenhuma pessoa aperta a própria mão e que duas pessoas apertam as mãos no máximo uma vez. Então, o número de pessoas que apertam as mãos um número ímpar de vezes é par.

De fato, sejam $P_1, ..., P_n$ as pessoas. Aplicamos dupla contagem sobre o conjunto

$$A = \{(P_i, P_j)/P_i \text{ aperta a mão de } P_j, i \neq j\}.$$

Seja x_i o número de vezes que a pessoa P_i troca apertos de mãos. Seja y o número total de apertos de mãos. Por um lado, o número de elementos de A é $\sum_{i=1}^{n} x_i$, pois para cada P_i o número de escolhas de P_j é x_i. Por outro lado, cada aperto de mão nos dá dois pares (P_i, P_j) e (P_j, P_i). Assim o número total de apertos de mãos é $2y$. Portanto, $\sum_{i=1}^{n} x_i = |A| = 2y$. Agora, se a soma de n números é par, então a quantidade desses números que são ímpares é par, caso contrário a soma sempre seria ímpar.

2.2 Permutações e Combinações

Ao estudar problemas relacionados à contagem, objetiva-se descobrir a quantidade de agrupamentos que podem ser realizados em determinada situação. Para isso pode-se utilizar de diversos métodos para resolver tais problemas. Dentre eles, são apresentados na sequência as permutações, os arranjos e as combinações.

Definição 2.1. Uma **permutação simples** de n objetos distintos é qualquer ordenação desses objetos.

Definição 2.2. Seja P_n o número de permutações de n objetos distintos. Para um inteiro não negativo n, define-se $n!$ por $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$, sendo $0! = 1$, por convenção.

Proposição 2.1. O número de permutações de n objetos distintos é $P_n = n!$.

Demonstração. Seja $(x_i, x_2, ..., x_n)$ uma ordenação de n objetos distintos. Para a escolha de x_1, existem n possibilidades. Escolhido x_1, existem $n-1$ possibilidades de escolher x_2. Em geral, escolhido x_i, existem $n-i$ possibilidades de escolher x_{i+1}. Portanto, pelo Princípio Multiplicativo, $P_n = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!$. □

Pode-se utilizar permutações simples para fazer a contagem de anagramas de uma palavra, mas apenas no caso de palavras com todas as letras distintas. Para o caso de palavras com letras que se repetem, utiliza-se permutação com repetição para fazer a contagem. Porém, existem casos em que devem-se considerar uma permutação de r elementos escolhidos dentre n elementos distintos. Denota-se por $P(n, r)$ o número de r-permutações de um conjuto com n elementos.

Proposição 2.2. Para inteiros positivos n e r, com $r \leq n$,

$$P(n, r) = n \cdot (n-1) \cdot \cdots \cdot (n-r+1).$$

Demonstração. Construindo uma r-permutação em um conjunto de n elementos, podem-se escolher o primeiro item de n formas, o segundo item de $n-1$ formas, qualquer que seja a primeira escolha. Continuando assim até o r-ésimo item, podendo escolher de $n-(r-1)$ formas, independente qual foram os primeiros $r-1$ itens. Pelo Princípio Multiplicativo, os r itens podem ser escolhidos de $n \cdot (n-1) \cdot \cdots \cdot (n-r-1)$. □

Na notação de fatorial, pode-se escrever $P(n, r)$ como

$$P(n, r) = \frac{n!}{(n-r)!},$$

o qual também é denominado por **arranjo combinatório**.

Para se calcular a quantidade parcial de possíveis sequências de um determinado conjunto utiliza-se a **combinação**, a qual é um agrupamento que não depende da posição ocupada pelos elementos na sequência.

Definição 2.3. Sejam $a_1, \ldots, a_n$ objetos distintos. Sejam n e k números naturais tais que $0 \leq k \leq n$, cada subconjunto com k elementos de $a_1, \ldots, a_n$ é chamado uma **k-combinação** dos n objetos $a_1, \ldots, a_n$. O número de k-combinações de n objetos distintos é denotado por $\binom{n}{k}$.

Segundo (BRUALDI, 2004) devido ao seu aparecimento no Teorema Binomial recebem a nomenclatura de coeficientes binomiais. A proposição seguinte estabelece o valor para $\binom{n}{k}$.

Proposição 2.3. O número de k-combinações de n objetos distintos é $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Demonstração. Utilizando dupla contagem prova-se que $n! = \binom{n}{k} \cdot (n-p)!k!$, contando de quantas formas os números de 1 até n podem ser ordenados. De fato, uma ordenação dos números de 1 até n é uma permutação simples. Pela Proposição 2.1, tem-se $n!$ ordenações dos números de 1 até n. Por outro lado, escolhe-se os k primeiros números na ordenação. Existem $\binom{n}{k}$ formas para quais os n números aparecem entre os k primeiros. Uma vez que eles foram escolhidos, existem $k!$ formas de ordená-los, seguidos por $(n-k)!$ formas de ordenar os números restantes. Pelo Princípio Multiplicativo, os números de 1 até n podem ser ordenados de $\binom{n}{k} \cdot p!(n-k)!$ formas. Desse modo, $n! = \binom{n}{k} \cdot p!(n-k)!$. □

2.3 O Triângulo de Pascal

Um importante matemático francês que estudou os coeficientes binomiais foi Blaise Pascal, o qual apresentou uma importante identidade para estes, a Fórmula de Pascal, representada pela Eq. (1).

Proposição 2.4. (Fórmula de Pascal) Para todos n e k naturais com $1 \leq k \leq n-1$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{1}$$

Demonstração. Seja S um conjunto de n elementos distintos. Distingue-se um dos elementos de S e denota-o como x. Particionando o conjunto X de k-combinações de S em duas partes, A e B. Em A coloca-se as k-combinações que não contém x. No conjunto B coloca-se todas as k-combinações que contém x. O número de elementos de X é $|X| = \binom{n}{k}$; portanto, pelo princípio aditivo,

$$\binom{n}{k} = |A| + |B|.$$

As k-combinações em A são exatamente as k-combinações do conjunto $S - \{x\}$ de $n-1$ elementos, assim, o número de elementos de A é

$$|A| = \binom{n-1}{k}.$$

Uma k-combinação em B é obtida adicionando o elemento x a uma $(k-1)$-combinação de $S - \{x\}$. Desse modo, o número de elementos de B satisfaz

$$|B| = \binom{n-1}{k-1}.$$

Combinando os fatos, tem-se que

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

$\square$

Com estas relações podemos calcular os coeficientes binomiais, formando com isso um arranjo conhecido como Triângulo de Pascal, o qual foi apresentado por Pascal no Tratado do Triângulo Aritmético (PASCAL, 1963), e pode ser observado na Figura 1.

Figura 1 – Triângulo de Pascal na forma $\binom{n}{k}$ à esquerda e com os valores de $\binom{n}{k}$ à direita.

$$\begin{array}{llllll}
\binom{0}{0} & & & & & \\
\binom{1}{0} & \binom{1}{1} & & & & \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & & \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & \\
\iddots & & \vdots & & \ddots & \\
\binom{n}{0} & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \binom{n}{4} \cdots & \binom{n}{k}
\end{array}
\qquad
\begin{array}{llllll}
1 & & & & & \\
1 & 1 & & & & \\
1 & 2 & 1 & & & \\
1 & 3 & 3 & 1 & & \\
1 & 4 & 6 & 4 & 1 & \\
1 & 5 & 10 & 10 & 5 & 1 \\
\iddots & & \vdots & & & \ddots
\end{array}$$

Fonte: Autoria própria (2021)

Cada elemento do Triângulo de Pascal, exceto aqueles iguais a 1, pode ser obtido realizando-se a soma do elemento da linha acima e mesma coluna do elemento desejado, com o elemento da coluna anterior. Existem várias relações que são obtidas ao se observar o triângulo de Pascal, com a relação de simetria $\binom{n}{k} = \binom{n}{n-k}$ para $0 \leq k \leq n$.

Outra propriedade encontrada no triângulo é conhecida como Teorema das Linhas, o qual caracteriza o resultado da soma de todos dos coeficientes binomiais presentes na linha n do Triângulo de Pascal.

Teorema 2.1. (Teorema das Linhas) Para todo inteiro $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Demonstração. Para provar este teorema utiliza-se o Princípio da Dupla Contagem para demonstrar que ambos os lados da equação contam o número total de combinações de um conjunto S de n elementos de dois modos diferentes. Primeiramente observa-se que toda combinação de S é uma k-combinação de S para algum

$k = 0, 1, 2, \ldots, n$. Como $\binom{n}{k}$ é igual ao número de k-combinações de S, segue pelo Princípio Aditivo que

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

é igual ao número de combinações de S para $k = 0, 1, 2, \ldots, n$.

Pode-se também contar o número de combinações de S separando a escolha de uma combinação em n decisões. Pada elemento de $x \in S$ há duas escolhas a se fazer: x pertence ou não a combinação. Assim, pelo Princípio Multiplicativo, existem 2^n modos de uma combinação de S ser formada. Portanto, considerando ambos os resultados, pelo Princípio da Dupla Contagem temos que

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

□

2.4 O Teorema Binomial

Uma das primeiras aparições do Teorema Binomial pode ser relacionada com Euclides, o qual, segundo Coolidge (1949), escreveu "Se uma reta for cortada aleatoriamente, o quadrado do todo é igual aos quadrados dos segmentos e duas vezes o retângulo dos segmentos"[1]. O que algebricamente pode ser representado por

$$(a + b)^2 = a^2 + b^2 + 2ab.$$

Além do uso empregado por Euclides, os coeficientes binomiais eram usados para descobrir valores aproximados de raízes, e com o passar dos anos foram representados em formas tabeladas, um exemplo disto é o Triângulo de Pascal.

Com o resultado encontrado por Euclides para o quadrado do binômio, foi possível generalizar para potência n, e assim tem-se o Teorema Binomial, o qual é demonstrado a seguir.

Teorema 2.2. (Teorema Binomial) Seja n um inteiro positivo. Então, para todos x e y,

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Demonstração. Escreva $(x + y)^n$ como o produto $(x + y)(x + y) \cdots (x + y)$ de n fatores cada um igual a $(x + y)$. Expande-se este produto completamente, usando a lei distributiva, e agrupa-se os termos iguais. Já que, para cada fator $(x + y)$, pode-se escolher ou x ou y na multiplicação de $(x + y)^n$, o que resulta em 2^n termos e cada um pode ser arranjado na forma $x^{n-k}y^k$ para algum $k = 0, 1, \ldots, n$. Obtém-se o termo

[1] If a straight line be cut at random, the square on the whole is equal to the squares on the segments and twice the rectangle of the segments.

$x^{n-k}y^k$ escolhendo y em k dos n fatores e x nos $n-k$ fatores remanescentes. Portanto, o número de vezes que o termo $x^{n-k}y^k$ ocorre no produto expandido é igual ao número $\binom{n}{k}$ de k-combinações do conjunto de n fatores. Dessa forma,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.$$

$\square$

3 OS COEFICIENTES BINOMIAIS MÓDULO UM NÚMERO PRIMO

Neste capítulo, aprofunda-se o estudo dos coeficientes binomiais investigando-os módulo um número primo. Para isso, apresenta-se os teoremas fundamentais sobre o assunto, como o Teorema de Kummer e o Teorema de Lucas, sendo este último apresentado também para o caso de números binários. Para finalizar, apresentam-se alguns resultados sobre a paridade da soma de números binomiais.

3.1 O Teorema de Kummer

Nascido em Berlim, Ernst Eduard Kummer foi um matemático alemão que atuou em diversas vertentes da matemática tais como Teoria do Números, Teoria dos Ideais e a série hipergeométrica de Gauss (O'CONNOR; ROBERTSON, 1997). Ao pesquisar sobre os coeficientes binomiais, chegou ao resultado apresentado no Teorema 3.1 sobre a valorização p-ádica de coeficientes binomiais, o qual podemos ver em Mevstrovic (2014).

Definição 3.1. A valorização p-ádica de um inteiro n é o expoente da maior potência do número primo p que divide n, denotado por $\nu_p(n)$.

Em outras palavras, $\nu_p(n)$ é o expoente do número primo p que aparece na fatoração em números primos de n.

Dado um primo p, considere as expansões de n e k na base p, assim

$$\begin{aligned} n = &\quad a_0 + a_1 p + \cdots + a_l p^l \\ k = &\quad b_0 + b_1 p + \cdots + b_l p^l, \end{aligned}$$

onde $0 \leq a_i \leq p-1$ e $0 \leq b_i \leq p-1$ para $0 \leq i \leq l$. Define-se

$$\mathcal{A}^p_{n,k} = \{j \in \{0, 1, \ldots, l\} \ : \ b_j > a_j\}.$$

O Teorema de Kummer é enunciado abaixo e uma demonstração por ser vista em Kummer (1852).

Teorema 3.1. (Teorema de Kummer) Para um número primo p,

$$\nu_p\left(\binom{n}{k}\right) = |\mathcal{A}^p_{n,k}|.$$

Exemplo 3.1. Seja $p = 3$, então

$$\nu_p\left(\binom{20}{8}\right) = 1.$$

De fato, considerando $n = 20$ e $k = 8$, pode-se escrever tais números da forma,

$$\begin{aligned} n = &\quad 2 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 \\ k = &\quad 2 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2, \end{aligned}$$

Comparando os coeficientes de n e k, percebe-se que apenas em 3^1 o coeficiente de k é maior que o de n. Portanto, o número de elementos em $\mathcal{A}^p_{n,k}$ é 1.

Uma consequência do Teorema de Kummer é uma condição necessária sobre n para que o coeficiente binomial $\binom{n}{k}$ seja divisível por p para todo $0 < k < n$. Uma versão mais completa do resultado seguinte foi demonstrada por Fine (1947).

Corolário 3.1. Seja p um número primo. Se n é uma potência de p, então o coeficiente binomial $\binom{n}{k}$ é divisível por p para todo $0 < k < n$.

Demonstração. Deve-se demonstrar que $\nu_p\left(\binom{n}{k}\right) \geq 1$ para todo $0 < k < n$. De fato, se n é uma potência de p, existe $m \in \mathbb{N}$ tal que $n = p^m$. Assim, a expansão de n na base p é $n = 1 \cdot p^m$. Sendo $0 < k < n$, tem-se que a expansão de k na base p é

$$k = b_0 + b_1 p + \cdots + b_l p^l$$

com $l < m$, já que $k < n$. Desde que $k > 0$, temos que existe $i \in \{0, 1, \cdots, l\}$ tal que $b_i > 0$. Pelo Teorema 3.1, conclui-se que $\nu_p\left(\binom{n}{k}\right) \geq 1$ para todo $k = 1, \cdots, n-1$. $\square$

3.2 O Teorema de Lucas

Outro importante matemático na área de combinatória foi o francês François Édouard Anatole Lucas, o qual provou um teorema interessante que caracteriza a paridade dos coeficientes binomiais $\binom{n}{k}$ fazendo o uso da representação binária de n e k. Lucas determinou um método para encontrar os coeficientes binomiais módulo p (LUCAS, 1878), chegando na Eq. (2), com o resultado apresentado a seguir. Uma demonstração para este teorema é dada utilizando indução e baseada no Teorema Binomial da expansão de $(1 + x)^n$ (MEŠTROVIĆ, 2014).

Teorema 3.2. (Teorema de Lucas) Seja p um número primo. Sejam $n = n_s p^s + \cdots + n_1 p + n_0$ e $k = k_s p^s + \cdots + k_1 p + k_0$ as representações de n e k na base p, respectivamente. Então,

$$\binom{n}{k} \equiv \binom{n_s}{k_s} \cdots \binom{n_1}{k_1} \binom{n_0}{k_0} (\mathrm{mod}\ p) = \prod_{i=0}^{s} \binom{n_i}{k_i} (\mathrm{mod}\ p). \tag{2}$$

Demonstração. Pelo Corolário 3.1, tem-se que o coeficiente binomial $\binom{p}{k}$ é divisível por um primo p para todo $k = 1, 2, \ldots, p-1$, pelo Teorema Binomial 2.2 segue que

$$(1 + x)^p = \sum_{i=0}^{p} \binom{p}{k} x^i \equiv 1 + x^p (\mathrm{mod}\ p).$$

Por uma argumentação utilizando indução em k, a seguinte congruência é válida

$$(1+x)^{p^k} \equiv 1 + x^{p^k} (\text{mod } p),$$

onde k é um inteiro não negativo. De fato, para $k = 1$, o Teorema Binomial 2.2 nos diz que

$$(1+x)^p = \sum_{i=0}^{p} \binom{p}{i} x^i.$$

Pelo Teorema 3.1 temos que cada coeficiente binomial $\binom{p}{i}$ é divisível por p para todo $i = 1, \cdots, p-1$. Assim,

$$(1+x)^p \equiv 1 + x^p (\text{mod } p), \tag{3}$$

provando a congruência para $k = 1$. Suponha, por hipótese de indução que $(1+X)^{p^k} \equiv 1 + X^{p^k}(\text{ mod } p)$. Deve-se provar que a congruência vale para $k+1$. Pela hipótese de indução, tem-se

$$(1+x)^{p^{k+1}} = [(1+x)^{pk}]^p \equiv (1 + x^{p^k})^p (\text{mod } p).$$

Agora, pela Eq. (3) tem-se

$$(1+x)^{p^{k+1}} \equiv 1 + (x^{p^k})^p (\text{mod } p).$$

Portanto, $(1+x)^{p^k} \equiv 1 + x^{p^k} (\text{ mod } p)$ é válida.

Escrevendo-se n e k na base p, tal que $n = \sum_{i=1}^{s} n_i$ e $k = \sum_{i=1}^{s} k_i$ para alguns inteiros não negativos $s, n_0, ..., n_s, k_0, ..., k_s$, com $0 \leq n_i, k_i \leq p-1$ para todos $i = 0, 1, ..., s$. Então

$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} x^k &= (1+x)^n \\ &= \prod_{i=0}^{s} ((1+x)^{p^i})^{n_i} \\ &\equiv \prod_{i=0}^{s} (1 + x^{p^i})^{n_i} (\text{mod } p) \end{aligned}$$

pela congruência provada anteriormente. Fazendo a expansão de $(1 + x^{p^i})^{n_i}$ e a substituindo no produtório, tem-se

$$\sum_{k=0}^{n} \binom{n}{k} x^k \equiv \prod_{i=0}^{s} \left(\sum_{k_i=0}^{n_i} \binom{n_i}{k_i} x^{k_i p^i} \right) (\text{mod } p)$$

.

Intercalando o somatório com o produtório tem-se:

$$\sum_{k=0}^{n} \binom{n}{k} x^k \equiv \sum_{k=0}^{n} \left(\prod_{i=0}^{s} \binom{n_i}{k_i} \right) x^k (\text{mod } p).$$

Comparando os coeficientes de x^k à esquerda com os coeficientes à direita da congruência acima, obtém-se a Eq. (2). $\square$

No caso binário (módulo 2), tem-se como consequência do Teorema de Lucas a paridade de coeficientes binomiais (YOSHIKO, 2005). Antes de enunciá-la, são necessárias algumas notações.

Definição 3.2. Seja k um inteiro natural. Denota-se $(k)_2$ a representação de k na base 2, ou seja, a sua representação como um número binário.

Além disso, a paridade de um número inteiro pode se definida como a soma dos bits na representação binária módulo dois.

Exemplo 3.2. Se $k = 13 = 1.2^3 + 1.2^2 + 0.2^1 + 1$, então $(k)_2 = 1101$. A paridade de 13 então é $3 \pmod 2) = 1$, ou seja, 13 é ímpar.

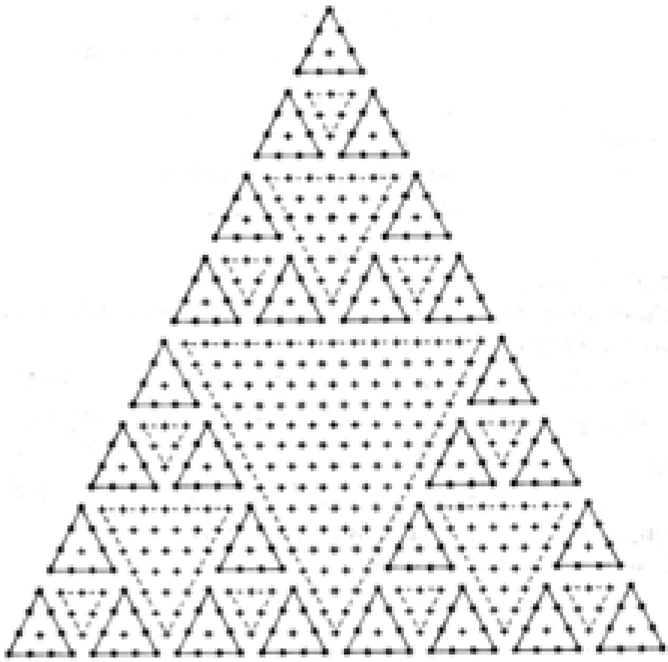
Definição 3.3. Dados dois números naturais k e n, diz-se que $(k)_2 \subseteq (n)_2$ se ao serem comparados os dígitos correspondentes de $(k)_2$ e $(n)_2$, começando pelo bit mais à direita, cada bit de $(k)_2$ é menor ou igual ao correspondente em $(n)_2$.

Assim, a paridade dos coeficientes binomiais é caracterizada pelo seguinte resultado.

Corolário 3.2. (Teorema de Lucas - caso binário): Sejam n e k dois inteiros, $0 \leq k \leq n$. Então $\binom{n}{k}$ é ímpar, se e somente se $(k)_2 \subseteq (n)_2$.

Com o resultado anterior, é possível observar que a paridade dos coeficientes binomiais se comporta como um fractal. Representando cada coeficiente binomial par por uma cruz "$+$" e cada coeficiente binomial ímpar por um asterisco "$*$", e substituindo no Triângulo de Pascal, obtém-se a seguinte representação fractal, apresentada por Kung (1976) e ilustrada na Figura 2.

Figura 2 – Representação fractal da paridade dos coeficientes binomiais no Triângulo de Pascal.



Fonte: Kung, S. (1976, p. 54)

Estabelecidos os resultados sobre a paridade dos coeficientes binomiais, questiona-se se é possível que todos os coeficientes binomiais em uma linha do Triângulo de Pascal tenham a mesma paridade. Observando a Figura 2, tem-se que essa característica acontece em alguns casos.

No caso binário, pelo Corolário 3.1 tem-se que os coeficientes $\binom{n}{k}$, $0 < k < n$, tem a mesma paridade quando n é uma potência de 2. E nesse caso, tais coeficientes são todos pares. No caso em que $n = 2^m - 1$, pelo teorema anterior e a Fórmula de Pascal (Proposição 2.4) tem-se que todos os coeficientes binomiais $\binom{n}{k}$ são ímpares.

3.3 A paridade da soma de números binomiais

Uma forma de generalizar a paridade dos coeficientes binomiais é investigar a paridade da soma de coeficientes binomiais consecutivos em uma linha do Triângulo de Pascal, ou seja, investigar a paridade dos números:

$$\alpha_q(k,t,m) = \sum_{i=k}^{t} (q-1)^i \binom{m}{i}, \tag{4}$$

onde q, k, t, m são números inteiros não negativos tais que $k \leq t \leq m$. Se $k = t$ e $q = 2$, então a Eq. (4) é o coeficiente binomial $\binom{m}{k}$.

O primeiro resultado aborda algumas consequências da Fórmula de Pascal, do Teorema das Linhas e do Teorema de Lucas na determinação da paridade de $\alpha_2(k,t,m)$

em algumas classes de parâmetros (k, t, m).

Proposição 3.1. (a) Para $m > 0$, o número $\alpha_2(0, m, m)$ é par;

(b) Para $0 < k < m$, $\alpha_2(k-1, k, m)$ é ímpar se, e somente se $(k)_2 \subseteq (m+1)_2$;

(c) Se m é ímpar da forma $m = 2t+1$, então $\alpha_2(0, t+1, m)$ é par.

(d) Se m é ímpar da forma $m = 2t+1$, então $\alpha_2(1, t+1, m)$ é ímpar.

Demonstração. (a) Pela Eq. (4), tem-se

$$\alpha_2(0,m,m) = \sum_{i=0}^{m}(2-1)^i\binom{m}{i} = \sum_{i=0}^{m}\binom{m}{i} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{m}.$$

Pelo Teorema das Linhas 2.1 resulta em 2^m, ou seja, $\alpha_2(0, m, m)$ é par.

(b) Pela Eq. (4), tem-se

$$\alpha_2(k-1,k,m) = \sum_{i=k-1}^{k}\binom{m}{s} = \binom{m}{k-1} + \binom{m}{k}.$$

Pela Fórmula de Pascal 2.4,

$$\alpha_2(k-1,k,m) = \binom{m+1}{k}.$$

Pelo Corolário 3.2, $\binom{m+1}{k}$ é ímpar se, e somente se $(k)_2 \subseteq (m+1)_2$.

(c) Sabe-se, pelo Teorema das Linhas 2.1, que

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{t} + \binom{m}{t+1} + \cdots + \binom{m}{m} = 2^m.$$

Como $m = 2t+1$, ou seja, m é ímpar, os coeficientes na linha m são simétricos, de forma que a soma de $\binom{m}{0}$ até $\binom{m}{t}$ é igual a soma de $\binom{m}{t+1}$ até $\binom{m}{m}$. Desse modo

$$2\left[\binom{m}{0} + \cdots + \binom{m}{t}\right] = 2^m.$$

Portanto, $\alpha_2(0, t+1, m)$ é par.

(d) Pelo item (c), sabe-se que $\alpha_2(0, t+1, m)$ é par. Sabendo que a expansão $\alpha_2(1, t+1, m)$ é a mesma que $\alpha_2(0, t+1, m)$ apenas sem o elemento $\binom{m}{0} = 1$, assim pode-se afirmar que $\alpha_2(1, t+1, m)$ é ímpar. □

O seguinte resultado, juntamente com o item (a) da Proposição 3.1 caracteriza a paridade de $\alpha_2(0, t, m)$. Esse resultado foi demonstrado em (CASTOLDI; CARMELO; SILVA, 2019, Proposição 2) utilizando o Teorema Binomial, sendo apresentada a seguir.

Teorema 3.3. (a) Se q é ímpar, então $\alpha_q(0, t, m) \equiv 1 \pmod 2$.

(b) Se q é par, então

$$\alpha_q(0,t,m) \equiv \begin{cases} 1(\bmod 2) & \text{se } t = 0, \\ 0(\bmod 2) & \text{se } t = m, \\ \binom{m-1}{t}(\bmod 2) & \text{se } 0 < t < m. \end{cases}$$

Demonstração. (a) Como q é ímpar, a potência $(q-1)^i$ é par para qualquer inteiro positivo i. Portanto $\alpha_q(0,t,m) \equiv 1 \pmod 2$.

(b) Suponha que q é par. O caso $t = 0$ é trivial, já que $\alpha_q(0,0,m) = 1$. Uma aplicação do Teorema Binomial 2.2 com $x = q-1$ e $y = 1$ produz $\alpha_q(0,m,m) = q^m$, o qual valida o caso $t = m$. Resta analisar o caso onde $0 < t < m$. Usando a Fórmula de Pascal 2.4 para $1 \leq i \leq m-1$, tem-se que

$$\begin{aligned} \alpha_q(0,t,m) &= \sum_{i=0}^{t}(q-1)^i\binom{m}{i} \\ &= (q-1)^0\binom{m}{0} + \sum_{i=1}^{t}(q-1)^i\binom{m}{i} \\ &= (q-1)^0\binom{m}{0} + \sum_{i=1}^{t}(q-1)^i\left[\binom{m-1}{i-1} + \binom{m-1}{i}\right] \\ &= (q-1)^0\binom{m}{0} + \sum_{i=1}^{t}(q-1)^i\binom{m-1}{i-1} + \sum_{i=1}^{t}(q-1)^i\binom{m-1}{i}. \end{aligned}$$

Consegue-se adicionar os termos $(q-1)^0\binom{m}{0}$ e $\displaystyle\sum_{i=1}^{t}(q-1)^i\binom{m-1}{i}$, assim

$$\alpha_q(0,t,m) = (q-1)\sum_{i=1}^{t}(q-1)^{i-1}\binom{m-1}{i-1} + \sum_{i=0}^{t}(q-1)^i\binom{m-1}{i}.$$

Mudando-se o índice da primeira somatória, obtém-se com

$$\alpha_q(0,t,m) = (q-1)\sum_{i=0}^{t-1}(q-1)^i\binom{m-1}{i} + \sum_{i=0}^{t}(q-1)^i\binom{m-1}{i}$$

Assim, pela Eq. (4) tem-se a seguinte relação de recorrência

$$\begin{aligned} \alpha_q(0,t,m) &= (q-1)\alpha_q(0,t-1,m-1) + \alpha_q(0,t,m-1) \\ &= q\alpha_q(0,t-1,m-1) - \alpha_q(0,t-1,m-1) + \alpha_q(0,t,m-1). \end{aligned}$$

Como $\alpha_q(0,t-1,m-1)$ e $\alpha_q(0,t,m-1)$ tem parcelas em comum, pode-se reescrever a equação acima da seguinte forma:

$$\begin{aligned} \alpha_q(0,t,m) &= q\alpha_q(0,t-1,m-1) + (q-1)^t\binom{m-1}{t} \\ &= q\left[1 + \sum_{i=1}^{t-1}(q-1)^i\binom{m-1}{i}\right] + (q-1)^t\binom{m-1}{t}. \end{aligned}$$

Como q é par, a afirmação é válida. □

Os seguintes resultados tratam dos casos em que m é uma potência de 2 e uma potência de 2 menos um e são consequência do Teorema 3.2 particularizado para esses casos.

Teorema 3.4. Seja m uma potência de 2.

(a) Se $t < m$, então $\alpha_2(0, t, m)$ é ímpar.

(b) Se $k > 0$ e $t < m$, então $\alpha_2(k, t, m)$ é par.

(c) Se $k > 0$, então $\alpha_2(k, m, m)$ é ímpar.

Demonstração.

(a) Sabendo que $m = 2^l$ para $l \in \mathbb{N}$, e sendo $t < m$, tem-se que pela Eq. (4)

$$\alpha_2(k, t, m) = \sum_{i=0}^{t} \binom{m}{i} = \binom{m}{0} + \binom{m}{1} + ... + \binom{m}{t}.$$

Sabendo que $\binom{m}{0} = 1$ e que todos os outros coeficientes binomiais em linhas pares são iguais a um número par, tem-se que $\alpha_2(0, t, m) = 1+2n$, para todo $n < m$, concluindo-se que $\alpha_2(0, t, m)$ é ímpar.

(b) Sabendo que $m = 2^l$ para $l \in \mathbb{N}$, e sendo $k > 0$ e $t < m$, tem-se pela Eq. (4)

$$\alpha_2(k, t, m) = \sum_{i=k}^{t} \binom{m}{i} = \binom{m}{k} + ... + \binom{m}{t}.$$

De forma análoga a apresentada no item (a), tem-se que como m é uma potência de 2, todos os coeficientes binomiais diferentes de $\binom{m}{0}$ e $\binom{m}{m}$ serão números pares, e como sabe-se que $k > 0$ e $t < m$, ou seja, $\binom{m}{0}$ e $\binom{m}{n}$ não estão presentes na soma, tem-se a soma dos n números pares, o que resulta em $\alpha_2(k, t, m)$ sendo um número par.

(c) Sabendo que $m = 2^l$ para $l \in \mathbb{N}$, e sendo $k > 0$, tem-se pela Eq. (4)

$$\alpha_2(k, m, m) = \sum_{i=k}^{t} \binom{m}{i} = \binom{m}{k} + ... + \binom{m}{m}.$$

Sabe-se pelas propriedades dos coeficientes binomiais que $\binom{m}{m} = 1$, e que a soma dos coeficientes nos quais $i \neq 0$ e m resulta em um número par. Tem-se então que $\alpha_2(k, m, m) = 2n + 1$, para todo $n < m$, ou seja, $\alpha_2(s, m, m)$ é ímpar. $\square$

Teorema 3.5. Seja $n = 2^n - 1$. Então, $\alpha_2(k, t, m)$ é par se, e somente se o número de parcelas na soma $\alpha_2(k, t, m)$ é par.

Demonstração. Tendo que $m = 2^n - 1$, pelo Teorema 3.1 e pelo Triângulo de Pascal, tem-se que os coeficientes são ímpares. Assim, sabendo que o número de parcelas na soma $\alpha_2(k, t, m)$ é par, é perceptível que $\alpha_2(k, t, m)$ será par, uma vez que qualquer número ímpar ao ser somado com outro número ímpar, resultará em um algarismo par.

Tem-se, pelo Teorema 3.1 e pelo Triângulo de Pascal, que se $m = 2^n - 1$, então todos os coeficientes deste serão ímpares. Desse modo, para que se tenha $\alpha_2(k, t, m)$ par, deve-se ter a soma de dois em dois coeficientes. Ou seja, deve-se ter um número par de parcelas na soma $\alpha_2(k, t, m)$. $\square$

Sintetizando os resultados anteriores, a paridade de $\alpha_2(k, t, m)$ foi determinada quando essa soma tem duas parcelas, $m = 2t + 1$ e $k = 0$, $0 < t < m$ e $k = 0$, m é uma potência de 2 e por fim $m = 2^n - 1$.

4 UMA APLICAÇÃO DA PARIDADE DA SOMA DE COEFICIENTES BINOMIAIS

Neste capítulo é apresentada uma aplicação da paridade da soma de coeficientes binomiais. Com esse objetivo, apresenta-se o conceito de conjuntos parcialmente (poset) ordenados e suas propriedades, além da sua representação gráfica. Apresenta-se a definição da métrica de Rosenbloom-Tsfasman (RT-métrica) e suas propriedades, o que conduz para o RT-espaço e uma RT-bola, sobre a qual se analisa a paridade e determina-se a relação existente desta com a paridade dos coeficientes binomiais. As principais referências deste capítulo são Brualdi, Graves e Lawrence (1995), Castoldi (2012) e Castoldi, Carmelo e Silva (2019).

4.1 Conjuntos Parcialmente Ordenados

Nesta seção, é revisado os principais conceitos envolvendo conjuntos parcialmente ordenados (posets). Em particular, uma classe de conjunto parcialmente ordenado conhecida como RT-poset é apresentada.

Definição 4.1. Um conjunto parcialmente ordenado (abreviadamente um poset) é um par ordenado $P = (X, \preceq)$ formado por um conjunto X e uma relação binária $\preceq$ contida em $X \times X$ (chamada de ordem parcial em X) satisfazendo as propriedades :
(i) A relação $\preceq$ é reflexiva, isto é, para todo $a \in X$ tem-se $a \preceq a$;
(ii) A relação $\preceq$ é antissimétrica, isto é, para quaisquer $a, b \in X$ se $a \preceq b$ e $b \preceq a$ então $a = b$;
(iii) A relação $\preceq$ é transitiva, isto é, para quaisquer $a, b, c \in X$ se $a \preceq b$ e $b \preceq c$ então $a \preceq c$.

Dados $a, b \in X$, se $a \preceq b$ ou $b \preceq a$ é dito que a e b são *comparáveis*, caso contrário é dito que eles são *incomparáveis*.

Definição 4.2. Um poset é uma cadeia quando quaisquer dois elementos são comparáveis. Um poset é uma anticadeia quando quaisquer dois elementos distintos não são comparáveis.

Exemplo 4.1. (i) O par $(\mathbb{N}, \leq)$ é um poset, onde $\leq$ denota a ordem usual em $\mathbb{N}$. Mais precisamente, o poset $(\mathbb{N}, \leq)$ é uma cadeia.
(ii) Seja E um conjunto e $\mathcal{P}(E) = \{Y : Y \subseteq E\}$ o conjunto formado por todos os subconjuntos de E. O par $(\mathcal{P}(E), \subseteq)$ é um poset. Se $|E| \geq 2$, o poset $(\mathcal{P}(E), \subseteq)$ não é uma cadeia nem uma anticadeia.

Neste trabalho, o conjunto X é considerado sempre finito. Representa-se graficamente posets finitos através dos diagramas de Hasse, cuja descrição é apresentada a seguir. Dado um poset finito $P = (X, \preceq)$, os elementos de X são representados por pontos e as comparações entre dois elementos distintos $a, b \in X$ são representadas por segmentos de reta ligando estes pontos, onde se convenciona que um elemento a está abaixo de b se, e somente se, $a \preceq b$ e não existe c distinto de a e b tal que $a \preceq c \preceq b$.

Os posets cadeia e anticadeia de comprimento 4 são representados através de diagramas de Hasse na Figura 3.

Figura 3 – Diagrama de Hasse dos posets cadeia e anticadeia de comprimento 4, respectivamente.

Fonte: Castoldi, A. G. (2012, p. 23)

A partir de agora P denota um poset arbitrário. O complemento de um subconjunto E de P é denotado por E^c.

Definição 4.3. (a) Um subconjunto I de P é um ideal de P se satisfaz: dado $b \in I$ e $a \preceq b$, então $a \in I$.

(b) O ideal gerado por um subconjunto A de P, denotado por $\langle A \rangle$, é o ideal de menor cardinalidade que contém A.

(c) Um elemento $a \in I$ é maximal em I se $a \preceq b$ implica que $b = a$.

(d) Um elemento $a \in I$ é minimal em I se $b \preceq a$ implica que $b = a$.

A seguir, apresenta-se o RT-poset e algumas propriedades relacionadas a este poset.

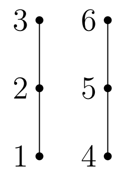
Definição 4.4. Sejam m e s inteiros positivos e $\Omega[m,s]$ um conjunto com ms elementos, particionado em m blocos B_i de cardinalidade s, onde para $i = 0, \ldots, m-1$, $B_i = \{b_{is}, \ldots, b_{(i+1)s-1}\}$ e cada bloco tem a relação de ordem total $b_{is} \preceq b_{is+1} \preceq \cdots \preceq b_{(i+1)s-1}$ (ou seja, cada bloco é uma cadeia de comprimento s).

O conjunto $\Omega[m,s]$ tem a estrutura de um conjunto parcialmente ordenado (poset): é a união de m cadeias disjuntas com s elementos cada. Este poset é chamado de *Rosembloom-Tsfasman poset* $\Omega[m,s]$, e abreviadamente por RT-poset $\Omega[m,s]$. Quando $\Omega[m,s] = [m \times s] = \{1, \ldots, ms\}$ denota-se o RT-poset $\Omega[m,s]$ simplesmente por RT-poset $[m \times s]$.

Denote por $\Omega_j(i)$ o número de ideais do RT-poset $[m \times s]$ com cardinalidade i e com exatamente j elementos maximais.

Exemplo 4.2. O RT-poset $[2 \times 3]$ é representado na Figura 4 (CASTOLDI, 2012).

Figura 4 – RT-poset $[2 \times 3]$



Fonte: Adaptado de Castoldi, A. (2012, p. 26)

Por simples inspeção, os ideais de cardinalidade 4 do RT-poset $[2 \times 3]$ são $\{1,2,3,4\}$, $\{1,2,4,5\}$ e $\{1,4,5,6\}$. A Tabela 1 apresenta todos os parâmetros $\Omega_j(i)$ do RT-poset $[2 \times 3]$.

$j \backslash i$	1	2	3	4	5	6
1	2	2	2	0	0	0
2	0	1	2	3	2	1

Tabela 1 – Parâmetros $\Omega_j(i)$

Sob certas condições sobre i e j, pode-se determinar explicitamente os valores de $\Omega_j(i)$. Uma demonstração para este resultado pode ser encontrada em (CASTOLDI; CARMELO; SILVA, 2019, Proposição 1).

Proposição 4.1. Se $j \leq i \leq s$, então $\Omega_j(i) = \binom{m}{j}\binom{i-1}{j-1}$.

Para $i = j$, como uma consequência da proposição anterior tem-se que $\Omega_i(i) = \binom{m}{i}$.

4.2 A métrica de Rosenbloom-Tsfasman

A RT-métrica é apresentada como uma métrica poset de acordo com Brualdi (1995).

Seja $\mathbb{Z}_q$ o conjunto dos inteiros módulo q. As n posições coordenadas de um elemento em $\mathbb{Z}_q^n = \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$ estão em bijeção com os elementos do conjunto $[n] = \{1, \ldots, n\}$. Um elemento $z = (z_1, \ldots, z_n) \in \mathbb{Z}_q^n$ pode ser simplesmente representado por $z = (z_1 \ldots z_n)$. O suporte de um elemento z é o conjunto $supp(z) = \{i : z_i \neq 0\}$.

Dados $x, y \in \mathbb{Z}_q^{ms}$ e o RT-poset $[m \times s]$, a RT-distância entre x e y é definida por

$$d_{RT}(x, y) = |\langle supp(x - y) \rangle|,$$

ou seja, a RT-distância entre x e y é o número de elementoos no ideal gerado pelo suporte do elemento $x - y$.

O conjunto $\mathbb{Z}_q^{ms}$ munido com a RT-distância é o Espaço de Rosenbloom-Tsfasman, ou simplesmente, o RT-espaço.

Exemplo 4.3. Considere o RT-poset $[2 \times 3]$ apresentado no Exemplo 4.2. Dados $x = (010100)$ e $y = (100110)$ em $\mathbb{Z}_2^6$, a RT-distância entre x e y é

$$d_{RT}(x, y) = |\langle supp(110010)\rangle| = |\langle\{1, 2, 5\}\rangle| = |\{1, 2, 4, 5\}| = 4.$$

A proposição seguinte, afirma que a RT-distância é uma métrica e foi demonstrada em (BRUALDI; GRAVES; LAWRENCE, 1995, Lema 1.1).

Proposição 4.2. Dados x, y, z no RT-espaço $\mathbb{Z}_q^{ms}$, as seguintes propriedades são verdadeiras:
(a) $d_{RT}(x, y) \geq 0$ e $d_{RT}(x, y) = 0$ se, e somente se, $x = y$.
(b) $d_{RT}(x, y) = d_{RT}(y, x)$.
(c) $d_{RT}(x, y) \leq d_{RT}(x, z) + d_{RT}(z, y)$.

Demonstração. Claramente vale o item (a). Da igualdade $supp(x - y) = supp(y - x)$,

$$d_{RT}(x, y) = | < supp(x - y) > | = | < supp(y - x) > | = d_{RT}(y, x),$$

donde concluí-se o item (b). Também, é conhecido que $supp(x + y) \subseteq supp(x) \cup supp(y)$. Como a união de dois ideais é ideal, obtemos

$$\begin{aligned} d_{RT}(x, y) &= | < supp(x - y) > | \\ &= | < supp(x - z + z - y) > | \\ &\leq | < supp(x - z) \cup supp(z - y) > | \\ &= | < supp(x - z) > \cup < supp(z - y) > | \\ &\leq | < supp(x - z) > | + | < supp(z - y) > | \\ &= d_{RT}(x, z) + d_{RT}(z, y). \end{aligned}$$

Assim, o item (c) está provado. □

Uma RT-bola com centro em x de raio R, denotada por $B^{RT}(x, R) = \{y \in \mathbb{Z}_q^{ms} : d_{RT}(x, y) \leq R\}$, tem sua cardinalidade dada pela fórmula

$$V_q^{RT}(m, s, R) = 1 + \sum_{i=1}^{R} \sum_{j=1}^{\min\{m,i\}} q^{i-j}(q - 1)^j \Omega_j(i). \tag{5}$$

Uma consequência direta pode ser obtida da Proposição 4.1, da seguinte forma.

Corolário 4.1. Dado um espaço RT-espaço $\mathbb{Z}_q^{ms}$, para qualquer m e $R \leq s$,

$$V_q^{RT}(m, s, R) = 1 + \sum_{i=1}^{R} \sum_{j=1}^{\min\{m,i\}} q^{i-j}(q - 1)^j \binom{m}{j}\binom{i-1}{j-1}.$$

4.3 Uma Análise da Paridade das RT-bolas

Nesta seção, critérios são estabelecidos para determinar a paridade das RT-bolas. Em particular, mostra-se que existe uma relação entre a paridade da soma dos coeficientes binomiais e a paridade das RT-bolas.

O cálculo de $V_q^{RT}(m,s,R)$ exige o conhecimento de todos os parâmetros $\Omega_j(i)$, de acordo com a Eq. (5). Nessa seção, investiga-se a paridade de $V_q^{RT}(m,s,R)$. O processo se inicia com uma conexão entre a paridade de $V_q^{RT}(m,s,R)$ e uma soma parcial adequada induzida por alguns parâmetros, os quais reduzem consideravelmente os cálculos.

Dado um RT-poset $[m \times s]$ e um inteiro positivo $t \leq m$, pode-se atribuir a sequência de parâmetros $\Omega_1(1), \ldots, \Omega_t(t)$ a soma parcial

$$\beta_q(t,m) = 1 + \sum_{i=1}^{t} (q-1)^i \Omega_i(i). \tag{6}$$

O próximo resultado estabelece uma conexão entre a paridade de $V_q^{RT}(m,s,R)$ e a paridade de $\beta_q(t,m)$ para um t adequado.

Teorema 4.1. Para inteiros positivos $q \geq 2$, $m \geq 2$, s, R, seja $t = \min\{m, R\}$. Os números $V_q^{RT}(m,s,R)$ e $\beta_q(t,m)$ possuem a mesma paridade.

Demonstração. Para facilitar, separa-se a demonstração em dois casos:
Caso 1: Se $m < R$. Neste caso $t = m$. A Eq. (5) pode ser reescrita como

$$\begin{aligned} V_q^{RT}(m,s,R) &= 1 + \sum_{i=1}^{m}\sum_{j=1}^{i} q^{i-j}(q-1)^j \Omega_j(i) + \sum_{i=m+1}^{R}\sum_{j=1}^{m} q^{i-j}(q-1)^j \Omega_j(i) \\ &= \beta_q(m,m) + \sum_{i=2}^{m}\sum_{j=1}^{i-1} q^{i-j}(q-1)^j \Omega_j(i) + \sum_{i=m+1}^{R}\sum_{j=1}^{m} q^{i-j}(q-1)^j \Omega_j(i). \end{aligned}$$

Se q é par, então q^{i-j} é par; caso q seja ímpar, então $(q-1)^j$ é par. Portanto as duas últimas parcelas da soma anterior são pares. Portanto, a paridade de $V_q^{RT}(m,s,R)$ é igual a paridade de $\beta_q(m,m)$.
Caso 2: Se $m \geq R$. Neste caso $t = R$. A Eq. (5) pode ser reescrita como

$$V_q^{RT}(m,s,R) = \beta_q(R,m) + \sum_{i=2}^{R}\sum_{j=1}^{i-1} q^{i-j}(q-1)^j \Omega_j(i).$$

Novamente, como $q^{i-j}(q-1)^j$ é sempre par quando $i > j \geq 1$, a segunda parcela da soma apresentada é par, e o resultado é válido. $\square$

A seguinte afirmação reflete a impotância dessa ligação.

Corolário 4.2. Se q é ímpar, então $\beta_q(t,m)$ é ímpar para qualquer $t \leq m$. Em particular, $V_q^{RT}(m,s,R)$ é ímpar.

Demonstração. Como q é ímpar, a potência $(q-1)^i$ é par para qualquer inteiro positivo i. Portanto $\beta_q(t,m)$ é ímpar. Aplicando o Teorema 4.1 conclui-se a afirmação. $\square$

Calcular a paridade de $\beta_q(t,m)$ para um q par, exige uma análise mais precisa do que no Corolário 4.2 (para q ímpar). Note que $\Omega_i(i) = \binom{m}{i}$ é válido para qualquer $i \leq s$ como é apresentado no final da Seção 4.1. Dessa forma, a soma parcial na Eq. (6) corresponde a

$$\alpha_q(0,t,m) = \sum_{i=0}^{t} (q-1)^i \binom{m}{i},$$

ou seja, $\beta_q(t,m) = \alpha_q(0,t,m)$.

Encontrar uma fórmula fechada para $\alpha_2(0,t,m)$ generalizada continua sendo um problema em aberto. Por ser um caso complicado, apenas dois casos são conhecidos, sendo estes $\alpha_2(0,m,m) = 2^m$ e $\alpha_2(0,t,2t+1) = 2^{2t}$. Apesar disso, a paridade de $\alpha_q(0,t,m)$ pode ser descrita completamente como mostrado no Teorema 3.3.

Finalmente, a paridade das RT-bolas é apresentada quando o raio R satisfaz algumas condições em relação aos parâmetros m e s.

Corolário 4.3. Seja q um número inteiro positivo e par.

(a) Se $m \leq R \leq s$, então $V_q^{RT}(m,s,R)$ é par.

(b) Se $R \leq s < m$, então $V_q^{RT}(m,s,R)$ é ímpar se, e somente se $\binom{m-1}{R}$ é ímpar . Particularmente, $V_2^{RT}(m,s,s)$ é ímpar se, e somente se $\binom{m-1}{s}$ é ímpar.

Demonstração. (a) Como q é par, Teorema 3.3 assegura $\alpha_q(0,m,m) \equiv 0 (\mathrm{mod}\ 2)$. Desse modo, Teorema 4.1 afirma que $V_q^{RT}(m,s,R)$ é par.

(b) Segue pelo Teorema 4.1 e pelo Teorema 3.3. $\square$

5 CONCLUSÃO

Por intermédio da pesquisa realizada, percebe-se o esforço de matemáticos renomados em pesquisas na área de análise combinatória e a importância desse estudo. Os coeficientes binomiais, assim como o Teorema Binomial, desenvolveram papéis importantes para o progresso em diversas áreas da matemática. Apesar disso, fica evidente a grande defasagem em trabalhos nacionais que abordem o tema, além do fato da grande dificuldade para encontrar-se uma fómula fechada para $\alpha_q(k,t,m)$ e para sua paridade. Pode-se perceber também uma aplicação para a paridade da soma de coeficientes binomiais, sendo esta importante para a teoria combinatória dos códigos.

O problema de determinar a paridade da soma de coeficientes binomiais consecutivos em uma linha de Triângulo de Pascal não foi resolvido completamente neste trabalho, porém resultados significativos sobre o tema foram apresentados. Uma possível continuidade deste trabalho é explorar a paridade de $\alpha_q(k,t,m)$ para outras classes de parâmetros (k,t,m), uma fórmula fechada para $\alpha_q(k,t,m)$, ou outras formas de generalizar a paridade dos coeficientes binomiais.

REFERÊNCIAS

BRUALDI, R. A. **Introductory Combinatorics**. 4. ed. [S.l.]: Pearson Education, 2004.

BRUALDI, R. A.; GRAVES, J. S.; LAWRENCE, K. M. Codes with a poset metric. **Discrete Mathematics**, Elsevier, v. 147, n. 1-3, p. 57–72, 1995.

CASTOLDI, A. G. **Coberturas em Espaços de Rosenbloom-Tsfasman**. 90 p. Dissertação (Mestrado em Matemática) — Universidade Estadual de Maringá, Maringá, 2012.

CASTOLDI, A. G.; CARMELO, E. L.; SILVA, R. da. Partial sums of binomials, intersecting numbers, and the excess bound in rosenbloom–tsfasman space. **Computational and Applied Mathematics**, Springer, v. 38, n. 2, p. 1–15, 2019.

COOLIDGE, J. L. The story of the binomial theorem. **The American Mathematical Monthly**, Taylor & Francis, v. 56, n. 3, p. 147–157, 1949.

FINE, N. J. Binomial coefficients modulo a prime. **The American Mathematical Monthly**, JSTOR, v. 54, n. 10, p. 589–592, 1947.

KUMMER, E. E. Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen. Walter de Gruyter, Berlin/New York Berlin, New York, 1852.

LKUNG, S. Parity triangles of pascal's triangle. Citeseer, 1976.

LUCAS, É. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. **Bulletin de la Société mathématique de France**, v. 6, p. 49–54, 1878.

MACWILLIAMS, F. J.; SLOANE, N. J. A. **The theory of error correcting codes**. [S.l.]: Elsevier, 1977. v. 16.

MEŠTROVIĆ, R. Lucas' theorem: its generalizations, extensions and applications (1878–2014). **arXiv preprint arXiv:1409.3820**, 2014.

O'CONNOR, J. J.; ROBERTSON, E. F. **Blaise Pascal**. 1996. Disponível em: https://mathshistory.st-andrews.ac.uk/Biographies/Pascal/. Acesso em: 19 de novembro de 2021.

O'CONNOR, J. J.; ROBERTSON, E. F. **Ernst Eduard Kummer**. 1997. Disponível em: https://mathshistory.st-andrews.ac.uk/Biographies/Kummer/. Acesso em: 22de maio de 2022.

ORLIK, P.; TERAO, H. **Arrangements of hyperplanes**. [S.l.]: Springer Science & Business Media, 2013. v. 300.

PASCAL, B. **Traité du triangle arithmétique**. [S.l.]: Éditions du Seuil, 1963.

PONTES, F. L. G. de; GOBBI, C. R.; SOUSA, E. K. V. de. As contribuições de édouard lucas para a teoria dos números. **Boletim Cearense de Educação e História da Matemática**, v. 5, n. 14, p. 243–252, 2018.

ROSENBLOOM, M. Y.; TSFASMAN, M. A. Codes for the m-metric. **Problemy Peredachi Informatsii**, Russian Academy of Sciences, v. 33, n. 1, p. 55–63, 1997.

SCHLÄFLI, L. **Theorie der vielfachen Kontinuität**. [S.l.]: Zürcher & Furrer, 1901. v. 38.

VALADÃO, D. R.; CASTOLDI, A. G. A paridade da soma de coeficientes binomiais. **XXVI Seminário de Iniciação Científica e Tecnológica**, Guarapuava, Brasil, 2021. Disponível em: https://eventos.utfpr.edu.br//sicite/sicite2021/paper/viewFile/8903/4324. Acesso em: 27 de maio de 2022.

YOSHIKO. **Brincando com Lucas e Pascal**. 2005. Disponível em: https://www.ime.usp.br/~yw/lic-mat-not-2005/mac110/eps/ep1.pdf. Acesso em: 05 de abril de 2022.