Universidade Estadual do Sudoeste da Bahia
Departamento de Ciências Exatas e Tecnológicas

Testes de primalidade utilizando o Triângulo de Pascal

Aelson Dias Teles

Vitória da Conquista
2020

Aelson Dias Teles

Testes de primalidade utilizando o Triângulo de Pascal

Trabalho de Conclusão de Curso apresentado ao colegiado do curso de Licenciatura em Matemática da Universidade Estadual do Sudoeste da Bahia – Campus de Vitória da Conquista, para a obtenção do título de Licenciado em Matemática, sob orientação do Prof. Dr. Júlio César dos Reis.

Vitória da Conquista
2020

Aelson Dias Teles

Testes de primalidade utilizando o Triângulo de Pascal

Trabalho aprovado. Vitória da Conquista, 03 de Março de 2020:

Prof. Dr. Júlio César dos Reis - UESB
Orientador

Prof. Dr. André Nagamine - UESB
Convidado 1

Prof. Dr. Flaulles Boone Bergamaschi - UESB
Convidado 2

Vitória da Conquista
2020

Agradecimentos

Primeiramente agradeço a Deus pelo fôlego de vida, pela força e constantes alegrias que tem me proporcionado.

Aos meus pais, Valdemar Chaves Teles e Vildenice Dias Teles, por todos os conselhos, apoio e carinho durante essa jornada.

Aos meus familiares de modo geral, mas em especial a minha tia Vilma Ferreira Dias (*in memorian*), que sempre me motivou a seguir em frente.

Ao meu amor Renata S. Cardozo por sempre colocar um sorriso em meu rosto.

Aos meus amigos pelo companheirismo de sempre.

Ao meu orientador, Prof. Dr. Júlio César dos Reis por suas importantes contribuições, paciência e palavras motivadoras durante a idealização do trabalho.

Aos meus colegas de curso pela "camaradagem"de sempre.

Por fim, a Universidade Estadual Do Sudoeste da Bahia, todo corpo docente e funcionários.

"Que darei eu ao SENHOR, por todos os benefícios que me tem feito?"

(Sl 116.12)

Resumo

Apresentaremos neste trabalho demonstrações para o Teste de Primalidade de Mann-Shanks que utiliza como ferramenta principal o Triângulo de Pascal T_2. Em tal critério observamos o comportamento dos números binomiais presentes em certa coluna e avaliamos determinados parâmetros para constatarmos se o número da coluna é primo ou não.

Palavras-chave: Critérios de primalidade, Triângulo de Pascal, Números Binomiais, Números Primos.

Abstract

In this work we will present demonstrations for the Mann-Shanks Primalty Criterion using the Pascal Triangle T_2 as their main tool. In this criterion, we observe the behavior of binomial numbers present in a given column and evaluate certain parameters to see if the column number is cousin or not.

Keywords: Primality Criterion, Pascal Triangle, Binomial Numbers, Prime numbers.

LISTA DE TABELAS

Tabela 1 – O Triângulo de Pascal. 23
Tabela 2 – O Triângulo de Pascal T_2 24
Tabela 3 – Colunas pares do Triângulo de Pascal T_2 32
Tabela 4 – 34
Tabela 5 – 34
Tabela 6 – T_2 37
Tabela 7 – T_3 38
Tabela 8 – T_4 38

LISTA DE SÍMBOLOS

α	Letra grega Alfa
ϕ	Letra grega Fi
$\in$	Pertence

Sumário

Introdução 11

1 – Tópicos em Teoria dos números 12
- 1.1 Número Binomial 12
- 1.2 Divisibilidade 18
- 1.3 Máximo divisor comum 19
- 1.4 Inteiros primos entre si 20
- 1.5 Números Primos 21

2 – Triângulo de Pascal 23
- 2.1 O Triângulo de Pascal 23
- 2.2 O Triângulo de Pascal T_2 23

3 – O critério de primalidade de Mann-Shanks 28

4 – Construção de tabelas T_m 37

Conclusão 42

Referências 43

Introdução

Os números primos são de grande importância para Matemática por possuírem apenas dois divisores distintos e positivos, a saber o número 1 e ele mesmo. Além disso, do Teorema Fundamental da Aritmética, qualquer que seja o número natural maior que 1, este será primo ou formado pelo produto de fatores primos.

Não obstante, resultados que envolvam testes de primalidade são de crucial importância para área criptográfica, com vistas a preservar a segurança e a credibilidade dos dados de grandes empresas e bancos inclusive. Portanto, ao longo deste trabalho, demonstraremos o Critério de Primalidade de Mann-Shanks, que se trata de um método pouco conhecido, datado de 1978, que relaciona O Triângulo de Pascal T_2, suas linhas, colunas e os números binomiais dispostos.

O trabalho está dividido em quatro capítulos. No primeiro, apresentamos conceitos e resultados básicos em Teoria dos números, como por exemplo: Números binomiais, divisibilidade, máximo divisor comum, dentre outros, que se relacionam com O Critério de Primalidade de Mann-Shanks.

No segundo capítulo, apresentamos O Triângulo de Pascal popularmente conhecido e O Triângulo de Pascal T_2, que desempenha papel fundamental no Critério.

O terceiro capítulo, demonstramos Método e construímos exemplos elucidativos com a teoria formulada.

Já no quarto capítulo, apresentamos (sem demonstração) uma generalização do resultado principal do capítulo 3.

1 Tópicos em Teoria dos números

Inicialmente iremos discutir definições e exemplos de tópicos em teoria dos números que são essenciais para o desenvolvimento deste trabalho. Tais tópicos foram construídos com base em (FILHO, 1981), (CHONG; KHEE-MENG, 1992) e (KOSHY, 2008).

1.1 Número Binomial

Definição 1.1 *(Número binomial) Sejam $n > 0$ e k dois inteiros tais que $0 \leq k \leq n$ chama-se número binomial de numerador n e classe k, o inteiro indicado por $\binom{n}{k}$ tal que:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Exemplo 1.1 *Sejam $n = 5$ e $k = 3$ calcule o número binomial.*

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} \text{ (definição)}$$

$$\binom{5}{3} = \frac{5.4.3!}{3!2!} \text{ (propriedade fatorial)}$$

$$\binom{5}{3} = \frac{5.4}{2.1} \text{ (simplificando)}$$

$$\binom{5}{3} = 10$$

Exemplo 1.2 *Sejam $n = 8$ e $k = 3$ calcule o número binomial.*

$$\binom{8}{3} = \frac{8!}{3!(8-3)!} \text{ (definição)}$$

$$\binom{8}{3} = \frac{8.7.6.5.4.3!}{3!5!} \text{ (propriedade fatorial)}$$

$$\binom{8}{3} = \frac{8.7.6.5.4}{5.4.3.2.1} \text{ (simplificando e desenvolvendo)}$$

$$\binom{8}{3} = 56$$

Nota-se que:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot ... \cdot k!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot ... \cdot (k+1)}{(n-k)!}$$

Exemplo 1.3 *Sejam $n = 5$ e $k = 3$ calcule o número binomial.*

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot ... \cdot (k+1)}{(n-k)!}$$

$$\binom{5}{3} = \frac{5.4}{(5-3)!} \text{ (desenvolvendo)}$$

$$\binom{5}{3} = \frac{20}{2!} \text{ (simplificando)}$$

$$\binom{5}{3} = 10$$

Além disso:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot ... \cdot (n-k)!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot ... \cdot (n-k+1)}{k!}$$

Exemplo 1.4 *Sejam $n = 8$ e $k = 3$ calcule o número binomial.*

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot ... \cdot (n-k+1)}{k!}$$

$$\binom{8}{3} = \frac{8.7.6}{3!}$$

$$\binom{8}{3} = \frac{8.7.6}{3.2.1}$$

$$\binom{8}{3} = 56$$

Lema 1.1 *Sejam $p \in \mathbb{N}$ e p um número primo, então:*

$$\binom{pq}{p} = \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p!}$$

Demonstração:

$$\begin{aligned}\binom{pq}{p} &= \frac{(pq)!}{p!(pq-p)!} \\ &= \frac{(pq)\cdot(pq-1)\cdot(pq-2)\cdot\ldots\cdot(pq-p+1)\cdot(pq-p)!}{p!(pq-p)!} \\ &= \frac{(pq)\cdot(pq-1)\cdot(pq-2)\cdot\ldots\cdot(pq-p+1)}{p!}\end{aligned}$$

■

Lema 1.2 *Sejam $p \in \mathbb{N}$ e p um número primo, então:*

$$\binom{pq}{p} = \frac{q(pq-1)(pq-2)\cdots(pq-p+1)}{(p-1)!}$$

Demonstração:

Decorre do **lema** 1.1 que:

$$\binom{pq}{p} = \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p!}$$

Então:

$$\begin{aligned}\binom{pq}{p} &= \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p!} \\ &= \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p(p-1)!} \\ &= \frac{q\cdot(pq-1)\cdot(pq-2)\cdot\ldots\cdot(pq-p+1)}{(p-1)!}\end{aligned}$$

■

Definição 1.2 *Diz-se que dois números binomiais são complementares se possuírem o mesmo numerador e a soma de suas respectivas classes resultarem no numerador comum a ambos.*

Exemplo 1.5 $\binom{9}{3}$ *e* $\binom{9}{6}$ *são números binomiais complementares pois possuem o mesmo numerador e a soma de suas classes é* $3+6=9$.

Teorema 1.1 *Dois números binomiais complementares são iguais.*

Demonstração:

Sejam $\binom{n}{k}$ e $\binom{n}{h}$ dois números binomiais complementares, segue que $k+h=n$ então $k=n-h$. Assim:

$$\binom{n}{k} = \binom{n}{n-h} = \frac{n!}{(n-h)!(n-(n-h))!} = \frac{n!}{(n-h)!h!} = \binom{n}{h}$$

■

Exemplo 1.6 *Os Números binomiais* $\binom{5}{3}$ *e* $\binom{6}{1}$ *são equivalentes aos números* $\binom{5}{2}$ *e* $\binom{6}{5}$ *respectivamente.*

De fato,

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5!}{(5-3)!(5-(5-3))!} = \frac{5!}{2!(5-2)!} = \binom{5}{2} = 10$$

$$\binom{6}{5} = \frac{6!}{5!(6-5)!} = \frac{6!}{(6-5)!(6-(6-5))!} = \frac{6!}{1!(6-1)!} = \binom{6}{1} = 6$$

Definição 1.3 *Diz-se que dois números binomiais são consecutivos se possuírem o mesmo numerador e suas respectivas classes forem números consecutivos.*

Exemplo 1.7 $\binom{3}{2}$ *e* $\binom{3}{3}$ *são números binomiais consecutivos pois possuem o mesmo numerador e suas classes respectivas são os inteiros consecutivos 2 e 3.*

Teorema 1.2 *(Relação de Stifel) Dados dois números binomiais consecutivos* $\binom{n}{k-1}$ *e* $\binom{n}{k}$*, com* $1 \leq k \leq n$ *tem-se:*

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

Demonstração:

$$\begin{aligned}
\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k+1)(n-k)!} + \frac{n!}{k(k-1)!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k)!} \cdot \left[\frac{1}{(n-k+1)} + \frac{1}{k}\right] \\
&= \frac{n!}{(k-1)!(n-k)!} \cdot \frac{n+1}{k(n-k+1)} \\
&= \frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!} \\
&= \frac{(n+1)!}{k!(n-k+1)!} \\
&= \binom{n+1}{k}
\end{aligned}$$

■

Exemplo 1.8 *Dados* $\binom{5}{3}$ *e* $\binom{5}{4}$ *então:*

$$\binom{5}{3} + \binom{5}{4} = \binom{11}{4}$$

Propriedades adicionais:

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} \tag{1}$$

$$\binom{n}{k} = \frac{n}{k-1}\binom{n-1}{k} \tag{2}$$

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1} \tag{3}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{4}$$

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r} \tag{5}$$

$$\binom{n}{2} + \binom{n-1}{2} = (n-1)^2 \tag{6}$$

$$\frac{1}{n}\binom{mn}{m} = \binom{nm-1}{m-1} \tag{7}$$

$$n\binom{n}{k} = (k+1)\binom{n}{k+1} + k\binom{n}{k} \tag{8}$$

Teorema 1.3 *(Identidade de Pascal) Dados quaisquer inteiros n e k positivos, onde* $k \leq n$*, então:*

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

Demonstração:

Desenvolvendo $\binom{n-1}{k-1} + \binom{n-1}{k}$ tem-se:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\
&= \frac{k(n-1)!}{k(k-1)!(n-k)!} + \frac{(n-k)(n-1)!}{k!(n-k)(n-k-1)!} \\
&= \frac{k(n-1)!}{k!(n-k)!} + \frac{(n-k)(n-1)!}{k!(n-k)!} \\
&= \frac{(n-1)![k+(n-k)]}{k!(n-k)!} \\
&= \frac{(n-1)!n}{k!(n-k)!} \\
&= \frac{n}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

■

1.2 Divisibilidade

Definição 1.4 *Sejam a e b números inteiros, diz-se que b divide a (ou que b é um divisor de a ou, ainda, que a é um múltiplo de b) se existe um inteiro c tal que $bc = a$. Usamos a notação $b|a$ para indicar que b divide a.*

Proposição 1.1 *Quaisquer que sejam os números inteiros a,b,c,d (assumindo os divisores diferentes de zero), valem:*

(i) $a|a$.

(ii) Se $a|b$ e $b|c$, então $a|c$.

(iii) Se $a|b$ e $c|d$, então $ac|bd$.

(iv) Se $a|b$ e $a|c$, então $a|(b+c)$.

(v) Se $a|b$, então para todo $m \in \mathbb{Z}$, tem-se que $a|mb$.

(vi) Se $a|b$ e $a|c$, então para quaisquer $m, n \in \mathbb{Z}$, tem-se que $a|(mb+nc)$.

Demonstração:

(i) Basta observar que podemos escrever $a \cdot 1 = a$.

(ii) Por definição, existem inteiros d e d', tais que $ad = b$ e $bd' = c$. Substituindo o valor de b dado pela primeira igualdade, temos $c = (ad)d' = a(dd')$, logo $a|c$.

(iii) Por definição, existem inteiros f e f', tais que $af = b$ e $cf' = d$. Multiplicando ordenadamente ambas as igualdades, temos $ac(ff') = bd$, donde segue a tese.

(iv) Existem inteiros d e d', tais que $ad = b$ e $ad' = c$. Somando ordenadamente ambas as igualdades, temos: $a(d+d') = b+c$, donde $a|(b+c)$.

(v) Se $a|b$,existe um inteiro c tal que $ac = b$. Multiplicando por m, temos $a(cm) = bm$, portando, $a|mb$.

(vi) Segue diretamente de (v) e (iv)

1.3 Máximo divisor comum

Definição 1.5 *Sejam a e b inteiros não nulos. Chama-se máximo divisor comum de a e b o inteiro positivo d $(d > 0)$ que satisfaz as seguintes condições:*

(i) $d|a$ e $d|b$

(ii) se $c|a$ e se $c|b$, então $c \leq d$

Indicamos o máximo divisor comum de a e b pela notação $mdc(a, b)$.

É imediato que o $mdc(a, b) = mdc(b, a)$. Em particular:

(i) O $mdc(0, 0)$ não existe

(ii) O $mdc(a, 1) = 1$

(iii) Se $a \neq 0$, então o $mdc(a, 0) = |a|$

(iv) Se $a|b$, então o $mdc(a, b) = |a|$

Lema 1.3 *Se $b \neq 0$, então o $mdc(a, b) = mdc(a, a - b)$*

Demonstração:

Seja $mdc(a, b) = d$, por definição $d|a$ e $d|b$. Podemos então escrever $a = dc$ e $b = dh$, onde $c, h \in \mathbb{N}$. Nota-se que :

$$a - b = dc - dh = d(c - h)$$

Logo $d|(a - b)$.

Resta mostrar que d é o máximo dos divisores comuns entre a e $a - b$. De fato, considere k um dos divisores comuns entre a e b. Segue que $k|a$ e $k|b$ implicando que $k|(a - b)$. Mas d é o $mdc(a, b)$ assim $d \geq k$ o que implica $mdc(a, a - b) = d$.

■

Teorema 1.4 *Se a e b são dois inteiros não nulos, então o conjunto de todos os múltiplos do $mdc(a, b) = d$ é*

$$T = \{ax + by \ | x, y \in \mathbb{Z}\}$$

Demonstração:

Como $d|a$ e $d|b$, segue que $d|(ax + by)$, quaisquer que sejam os inteiros x e y, e por conseguinte todo elemento do conjunto T é múltiplo de d.

Por outro lado, existem inteiros x_0 e y_0 tais que

$$d = ax_0 + by_0$$

De modo que todo múltiplo kd de d é da forma:

$$kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0)$$

isto é, kd é uma combinação linear de a e b, portanto, kd é elemento do conjunto T.

1.4 Inteiros primos entre si

Definição 1.6 *Sejam a e b dois inteiros não nulos. Diz-se que a e b são primos entre si se, e somente se o $mdc(a, b) = 1$*

Teorema 1.5 *Dois inteiros a e b, não nulos, são primos entre si se, e somente se existem inteiros x e y tais que $ax + by = 1$*

Demonstração:

($\Rightarrow$) Se a e b são primos entre si, então o $mdc(a, b) = 1$ e por conseguinte existem inteiros x e y tais que:

$$ax + by = 1$$

($\Leftarrow$) Reciprocamente,se existem inteiros x e y tais que $ax+by = 1$ e se o $mdc(a, b) = d$, então $d|a$ e $d|b$. Logo $mdc = 1$, isto é, a e b são primos entre sí.

Corolário 1.1 *Se $mdc(a, b) = d$, então o $mdc(a/d, b/d) = 1$*

Demonstração:

Preliminarmente, observa-se que a/d e b/d são inteiros, pois d é um divisor comum de a e b.

Desse modo, se o $mdc(a, b) = d$, então existem inteiros x e y tais que $ax + by = d$, ou seja, dividindo ambos os membros desta igualdade por d temos:

$$(a/d)x + (b/d)y = 1$$

Logo, pelo teorema 1.5, os inteiros a/d e b/d são primos entre si, isto é o $mdc(a/d, b/d) = 1$.

Corolário 1.2 *Se $a|b$ e se $mdc(b,c)=1$, então o $mdc(a,b)=1$.*

Demonstração:

De fato,

$$a|b \Longrightarrow b = aq,\ com\ q \in \mathbb{Z}$$

$$mdc(b,c)=1 \Longrightarrow bx+cy=1,\ com\ x,y \in \mathbb{Z}$$

Portando:

$$a(qx)+cy=1 \Longrightarrow mdc(a,c)=1$$

Corolário 1.3 *Se $a|b$ e $b|c$ e se $mdc(a,b)=1$, então $ab|c$.*

Demonstração:

De fato,

$$a|c \Longrightarrow c = aq_1,\ com\ q_1 \in \mathbb{Z}$$

$$b|c \Longrightarrow c = aq_2,\ com\ q_2 \in \mathbb{Z}$$

$$mdc(a,b)=1 \Longrightarrow ax+by=1 \Longrightarrow acx+bcy=c,\ com\ x,y \in \mathbb{Z}$$

Portando:

$$c = a(bq_2)x + b(aq_1)y = ab(q_2x+q_1y) \Longrightarrow ab|c$$

1.5 Números Primos

Definição 1.7 *Diz-se que um inteiro positivo $p>1$ é um número primo se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se composto.*

Teorema 1.6 *Se um primo p não divide um inteiro a, então a e p são primos entre si.*

Demonstração:

Seja d o mdc entre a e p. Então d|a e d|p. Da relação d|p, temos que d=1 ou d=p, pois p é primo, e como a segunda igualdade é impossível, porque p não divide a, tem-se d=1, ou seja, o mdc(a,p)=1. Logo a e p são primos entre si.

■

Teorema 1.7 *Todo inteiro composto possui um divisor primo.*

Demonstração:

Seja a um inteiro composto. Consideremos o conjunto A de todos os divisores positivos de a, exceto os divisores triviais 1 e a, isto é:

$$A = \{x|a;\ 1 < x < a\}$$

Pelo princípio da boa ordenação, existe o elemento mínimo p de A que deverá ser primo. De fato, se p fosse composto admitiria pelo menos um divisor d tal que $1 < d < p$, e então d|p e p|a, o que implica d|a, ou seja, p não seria o elemento mínimo de A. Portanto, p é primo.

■

2 Triângulo de Pascal

2.1 O Triângulo de Pascal

O Triângulo de Pascal trata-se de uma tabela numérica que pode ser obtida tomando-se $\binom{n}{k}$, onde n será o número da linha e k o número da coluna, com n e k partindo da linha e coluna 0.

Tabela 1 – O Triângulo de Pascal.

•	0	1	2	3	4	...	k
0	$\binom{0}{0}$						
1	$\binom{1}{0}$	$\binom{1}{1}$					
2	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$				
3	$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$			
4	$\binom{4}{0}$	$\binom{4}{1}$	$\binom{4}{2}$	$\binom{4}{3}$	$\binom{4}{4}$		
...							
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	...	$\binom{n}{k}$

Fonte - Própria

Nota-se que dada uma determinada linha do Triângulo de Pascal, os números binomiais tem variação de: $\binom{n}{0} \leq \binom{n}{r} \leq \binom{n}{k}$, isto é, n é fixo enquanto as colunas k variam de 0 até n.

2.2 O Triângulo de Pascal T_2

O Triângulo de Pascal T_2 pode ser obtido, realizando um deslocamento de duas casas partindo da linha 1 e sempre do primeiro elemento da linha anterior do triângulo original. Conforme a Tabela 2 indica.

Lema 2.1 *Na construção do Triângulo deslocado, partindo de uma linha fixa l, a variação da coluna c será dada por*

$$2l \leq c \leq 3l$$

(consequência imediata do deslocamento).

Tabela 2 – O Triângulo de Pascal T_2

•	0	1	2	3	4	5	6	7	8	9	...	c
0	$\binom{0}{0}$											
1			$\binom{1}{0}$	$\binom{1}{1}$								
2					$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$					
3							$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$		
...												
l											...	$\binom{l}{k_\alpha}$

Fonte - Própria

Exemplo 2.1 *Dada a linha $l = 3$, temos:*

$$6 \leq c \leq 9$$

Exemplo 2.2 *Dada a linha $l = 7$, temos:*

$$14 \leq c \leq 21$$

Por outro lado, no Triângulo original os números binomiais presentes na linha variam até o termo $\binom{l}{l}$. Considerando as modificações realizadas temos $c \leq 3l$, tomando $c = 3l$ e subtraindo $2l$ de ambos os lados da equação obtemos $c - 2l = l$.

Lema 2.2 *Seja $k_\alpha = c - 2l$, então os elementos da linha l varia até o termo $\binom{l}{k_\alpha}$ isto é:*

$$\binom{l}{0} \leq \binom{l}{r} \leq \binom{l}{k_\alpha}, \quad 0 \leq k_\alpha \leq l$$

Exemplo 2.3 *Seja $l = 8$ segue que:*

$$k_\alpha = c - 2l \Rightarrow k_\alpha = c - 16$$

$$0 \leq k_\alpha \leq l \Rightarrow 0 \leq k_\alpha \leq 8 \Rightarrow 0 \leq c - 16 \leq 8 \Rightarrow 16 \leq c \leq 24$$

Então:

$$k_0 = 16 - 16 = 0$$

$$k_1 = 17 - 16 = 1$$

$$k_2 = 18 - 16 = 2$$

$$k_3 = 19 - 16 = 3$$

$$k_4 = 20 - 16 = 4$$

$$k_5 = 21 - 16 = 5$$

$$k_6 = 22 - 16 = 6$$

$$k_7 = 23 - 16 = 7$$

$$k_8 = 24 - 16 = 8$$

Portanto os elementos da linha 8 do Triângulo T_2 são:

$$\binom{8}{0};\ \binom{8}{1};\ \binom{8}{2};\ \binom{8}{3};\ \binom{8}{4};\ \binom{8}{5};\ \binom{8}{6};\ \binom{8}{7};\ \binom{8}{8}$$

Exemplo 2.4 *Seja $l = 5$ segue que:*

$$k_\alpha = c - 2l \Rightarrow k_\alpha = c - 10$$

$$0 \leq k_\alpha \leq l \Rightarrow 0 \leq k_\alpha \leq 5 \Rightarrow 0 \leq c - 10 \leq 5 \Rightarrow 10 \leq c \leq 15$$

Então:

$$k_0 = 10 - 10 = 0$$

$$k_1 = 11 - 10 = 1$$

$$k_2 = 12 - 10 = 2$$

$$k_3 = 13 - 10 = 3$$

$$k_4 = 14 - 10 = 4$$

$$k_5 = 15 - 10 = 5$$

Portanto os elementos da linha 5 do Triângulo T_2 são:

$$\binom{5}{0};\ \binom{5}{1};\ \binom{5}{2};\ \binom{5}{3};\ \binom{5}{4};\ \binom{5}{5}$$

Como consequência da desigualdade $2l \leq c \leq 3l$ obtemos:

$$\frac{k_\alpha + 2l}{3} \leq l \leq \frac{k_\alpha + 2l}{2}$$

Proposição 2.1 *Tomando colunas múltiplas de 6, isto é $c = 6a$, $a \in \mathbb{N}^*$ nota-se que as linhas estão compreendidas entre $2a \leq l \leq 3a$.*

De fato,

$$\frac{k_\alpha + 2l}{3} \leq l \leq \frac{k_\alpha + 2l}{2}$$

Logo,

$$\frac{k_\alpha + 2l}{3} \leq l \leq \frac{k_\alpha + 2l}{2} \Leftrightarrow \frac{(c-2l) + 2l}{3} \leq l \leq \frac{(c-2l) + 2l}{2} \Leftrightarrow$$

$$\frac{c}{3} \leq l \leq \frac{c}{2} \Leftrightarrow \frac{6a}{3} \leq l \leq \frac{6a}{2} \Leftrightarrow 2a \leq l \leq 3a$$

■

Exemplo 2.5 *Considere $a = 3$, desse modo $c = 18$, além disso, a linha l varia de $6 \leq l \leq 9$.*

Segue que $\binom{l}{k_\alpha}$, $6 \leq l \leq 9$, indicará os números binomiais presentes na coluna múltipla de 6.

Proposição 2.2 *Para as colunas da forma* $c_p = 6a + 1$ *temos que* $\frac{c_p}{3} < l \leq \frac{c_p}{2}$.

De fato,

$$2l \leq c_p < 3l \Rightarrow 2l \leq c_p \Rightarrow l \leq \frac{c_p}{2} \; e \; c_p < 3l \Rightarrow \frac{c_p}{3} < l$$

Assim,

$$\frac{c_p}{3} < l \leq \frac{c_p}{2} \qquad (*)$$

■

Exemplos:

a) $c_p = 7 \Rightarrow 2 < l \leq 3$

b) $c_p = 13 \Rightarrow 4 < l \leq 6$

c) $c_p = 19 \Rightarrow 6 < l \leq 9$

d) $c_p = 25 \Rightarrow 8 < l \leq 12$

Em $(*)$ considere a parte inteira das divisões de c_p por 2 e 3.

3 O critério de primalidade de Mann-Shanks

No artigo (MANN; SHANKS, 1972) temos determinado critério para verificar se um número inteiro é primo. No presente trabalho dividiremos tal resultado em dois teoremas iniciais que juntos computam a prova necessária e suficiente do método. Como se segue:

Teorema 3.1 *Se o número da coluna do Triângulo de Pascal T_2 é primo, então os coeficientes são divisíveis pelo número da linha correspondente.*

A demonstração de tal teorema será realizada por intermédio de uma sequência lógica de resultados munidos de exemplos convenientemente elucidativos.

De início, nota-se que as colunas 2 e 3 são primárias. Considere as seguintes colunas:

$$6a; 6a+1; 6a+2; 6a+3; 6a+4; 6a+5 = 6a-1$$

Estamos à procura de colunas cujo resto da divisão pelos números 2 ou 3 seja diferente de 0.

Observe as seguintes congruências módulo 2 e 3:

$$6a \equiv 0(mod2)$$
$$6a \equiv 0(mod3)$$
$$6a+1 \equiv 1(mod2)$$
$$6a+1 \equiv 1(mod3)$$
$$6a+2 \equiv 0(mod2)$$
$$6a+2 \equiv 2(mod3)$$
$$6a+3 \equiv 3(mod2)$$
$$6a+3 \equiv 0(mod3)$$
$$6a+4 \equiv 0(mod2)$$
$$6a+4 \equiv 4(mod3)$$
$$6a+5 \equiv 5(mod3)$$
$$6a+5 \equiv 5(mod3)$$

Com base em tais congruências, verificamos que as únicas colunas que não são múltiplas de 2 ou 3,simultaneamente, são colunas $c_p = 6a + 1$ e $c_p = 6a + 5 = 6a - 1$; $\mathbb{N}^*$. Dessa maneira, podemos nos restringir ao estudo de tais colunas.

Denotamos ϕ os coeficientes binomiais da coluna $c_p = 6a + 1$, onde:

$$\phi = \binom{l_p}{k_p},\ l_p = 2a + u \ e\ k_p = 3u - 1 \ onde\ 1 \leq u \leq a.$$

Agora, com base nas construções anteriores , vejamos alguns exemplos elucidativos:

Exemplo 3.1 *Tome $a = 2$, então $c_p = 13$, donde*

$$l_p = 4 + u \ e\ k_p = 3u - 1;\ 1 \leq u \leq 2$$

Isto é, os coeficientes da coluna $c_p = 13$ são:

$$\binom{5}{2} \ e \ \binom{6}{5}$$

*Pela **definição** 1.2 , esses números binomiais são respectivamente complementares aos inteiros $\binom{5}{3}$ e $\binom{6}{1}$. Segue do **teorema** 1.1 que:*

$$\binom{5}{2} = \binom{5}{3} \ e \ \binom{6}{5} = \binom{6}{1}$$

E portanto os coeficientes binomiais da coluna $c_p = 13$ são:

$$\binom{5}{2} \ e \ \binom{6}{5}$$

Exemplo 3.2 *Tome $a = 4$, então $c_p = 25$, donde*

$$l_p = 8 + u \ e\ k_p = 3u - 1;\ 1 \leq u \leq 4$$

Isto é, os coeficientes da coluna $c_p = 13$ são:

$$\binom{9}{2}, \ \binom{10}{5}, \ \binom{11}{8} \ e \ \binom{12}{11}$$

*Pela **definição** 1.2, esses números binomiais são respectivamente complementares aos inteiros $\binom{9}{7}$, $\binom{10}{5}$, $\binom{11}{3}$ e $\binom{12}{1}$. E o raciocínio segue análogo ao exemplo anterior.*

Retomando a demonstração do Teorema, no caso em que os coeficientes ϕ pertencentes a coluna c_p forem divisíveis pelas suas respectivas linhas l_p nada temos que provar.

Pela propriedade adicional (1) de números binomiais:

$$\binom{l_p-1}{k_p-1} l_p = \phi k_p,\ 1 \leq u \leq a$$

Veja o seguinte exemplo elucidativo:

Exemplo 3.3 *Tome $a = 3$, então:*

$$l_p = 6 + u \ e \ k_p = 3u - 1,\ 1 \leq u \leq a$$

E obtemos os seguintes pares ordenados da forma (l_p, k_p):

$$\{(7,2)(8,5)(9,8)\}$$

Computando os pares ordenados temos:

a) $(7,2) \Rightarrow \binom{7-1}{2-1} \cdot 7 = \binom{7}{2} \cdot 2 \Rightarrow \binom{6}{1} \cdot 7 = \binom{7}{2} \cdot 2 \Rightarrow 6 \cdot 7 = 21 \cdot 2 \Rightarrow 42 = 42$

b) $(8,5) \Rightarrow \binom{8-1}{5-1} \cdot 8 = \binom{8}{5} \cdot 5 \Rightarrow \binom{7}{4} \cdot 5 = \binom{8}{5} \cdot 5 \Rightarrow 35 \cdot 8 = 56 \cdot 5 \Rightarrow 280 = 280$

c) $(9,8) \Rightarrow \binom{9-1}{8-1} \cdot 9 = \binom{9}{8} \cdot 8 \Rightarrow \binom{8}{7} \cdot 9 = \binom{9}{8} \cdot 8 \Rightarrow 8 \cdot 9 = 9 \cdot 8 \Rightarrow 72 = 72$

Agora, prosseguindo a demonstração, suponha, por absurdo, que ϕ não é divisível pela respectiva linha l_p, considere a seguinte igualdade:

$$\binom{l_p-1}{k_p-1} l_p = \phi k_p,$$

Se $mdc(l_p, k_p) = 1$ dividindo ambos os membros da equação por l_p temos:

$$\binom{l_p-1}{k_p-1} = \frac{\phi \cdot k_p}{l_p}$$

Como $\binom{l_p-1}{k_p-1} \in \mathbb{Z}^*$, então $\frac{\phi \cdot k_p}{l_p} \in \mathbb{Z}^*$, mas $mdc(l_p, k_p) = 1$ logo l_p divide ϕ.

Suponha agora que $mdc(l_p, k_p) > 1$, então $mdc(3l_p, k_p) > 1$.

Como $l_p = 2a + u$ e $k_p = 3u - 1$ segue que $mdc(3(2a + u), 3u - 1) = mdc(6a + 3u, 3u - 1)$.

Por definição $c_p = 6a + 1$ o que implica $6a = c_p - 1$.

Assim $mdc((c_p - 1) + 3u, 3u - 1) = mdc(c_p + (3u - 1), 3u - 1) = mdc(3u - 1, c_p + (3u - 1))$.

Pelo **lema** 1.3: $mdc(a, b) = mdc(a, a - b)$.

Tome $a = 3u - 1$ e $b = (c_p + 3u - 1)$, logo:

$$mdc(3u-1, c_p+(3u-1)) = mdc(3u-1, (3u-1)-(c_p+(3u-1)) = mdc(3u-1, -(c_p)) = mdc(c_p, 3u-1)$$

Então $mdc(c_p, k_p) > 1$. O que configura um absurdo pois c_p é primo, logo cada coeficiente é divisível pelo número da linha correspondente.

Se $c_p = 6a - 1$, tome :

$$\phi = \binom{l_p}{k_p},\ l_p = 2a + u \ e \ k_p = 3u + 1 \ onde \ 1 \leq u \leq a - 1.$$

E o raciocínio é semelhante.

■

Exemplo 3.4 $\binom{5}{3} e \binom{6}{1}$ *são os números binomiais presentes na coluna prima 13, e estão localizados nas linhas* 5 *e* 6 *respectivamente.*

Do teorema anterior devemos ter que 5 *divide* $\binom{5}{3}$ *e* 6 *divide* $\binom{6}{1}$

De fato,

$\binom{5}{3} = 10$ *e* $5|10$

$\binom{6}{1} = 6$ *e* $6|6$

Exemplo 3.5 $\binom{8}{7}, \binom{9}{5}, \binom{10}{3}$ *e* $\binom{11}{1}$ *são os números binomiais presentes na coluna prima 23, e estão localizados nas linhas* 8,9,10 *e* 11 *respectivamente.*

Do teorema anterior devemos ter que $\binom{8}{7}, \binom{9}{5}, \binom{10}{3}$ *e* $\binom{11}{1}$ *são divisíveis por* 8,9,10 *e* 11.

De fato,

$\binom{8}{7} = 8$ *e* $8|8$

$$\binom{9}{5} = 126 \ e \ 9|126$$

$$\binom{10}{3} = 120 \ e \ 10|120$$

$$\binom{11}{1} = 11 \ e \ 11|11$$

A segunda parte do Teorema possui o seguinte enunciado:

Teorema 3.2 *Se os coeficientes do Triângulo de Pascal T_2 são divisíveis pelo número da linha correspondente, então o número da coluna é primo.*

Considerando a contra-positiva do teorema temos:

"Se o número da coluna não é primo então algum coeficiente do Triângulo de Pascal T_2 não é divisível pelo número da linha correspondente."

Observe a seguinte tabela:

Tabela 3 – Colunas pares do Triângulo de Pascal T_2

	0	...	4	...	6	...	8	...	10	...	12	...
0	$\binom{0}{0}$											
...												
2			$\binom{2}{0}$									
3					$\binom{3}{0}$							
4							$\binom{4}{0}$					
5									$\binom{5}{0}$			
6											$\binom{6}{0}$	
...												...

Fonte - Própria

Considerando a coluna $c = 6$ o número binomial $\binom{3}{0}$ não é divisível pela sua respectiva linha.

De fato,

$$\binom{3}{0} = 1, \ e \ 3 \ não \ divide \ 1.$$

Dessa maneira, se cada coluna for da forma $c = 2q; q = 0, 3, 4, ..$ possuirá um coeficiente:

$$\binom{l}{0} = 1;\ l \in \mathbb{N}.$$

E o mesmo não será divisível pela sua respectiva linha. Assim vamos nos restringir a composições ímpares c. Segue que c possui um fator primo p e podemos escrever:

$$c = p(2q + 1); q \geq 1.$$

Tomando $R = pq$ o coeficiente na linha R-ésima e na coluna C-ésima será:

$$\binom{pq}{p}$$

Vejamos alguns exemplos:

Exemplo 3.6 *Tome $c = 15$, então $R = 6$, pois $15 = 3(2 \cdot 2 + 1)$ e o coeficiente será:*

$$\binom{6}{3} = 20$$

É evidente que 20 não é divisível pela sua respectiva linha.

Exemplo 3.7 *Tome $c = 21$, então $R = 9$, pois $21 = 3(2 \cdot 3 + 1)$ e o coeficiente será:*

$$\binom{9}{3} = 84$$

É evidente que 84 não é divisível pela sua respectiva linha.

Agora, retomando a demonstração, considere o **lema:** 1.1 sabemos que

$$\binom{pq}{p} = \frac{q(pq-1)(pq-2)\cdots(pq-p+1)}{(p-1)!}$$

Suponha que a maior potência de p que divide q é p^s. Então p^{s+1} não divide o coeficiente e assim pq não o divide. Portanto, mostramos que se o número da coluna não é primo então algum coeficiente do Triângulo de Pascal T_2 não é divisível pelo número (pq).

■

Ressaltamos que a notação padrão do artigo (MANN; SHANKS, 1972), foi reescrita, com vistas a facilitar a compreensão da demonstração.

Temos no artigo (HONSBERGER, 1976) uma prova levemente diferente da apresentada anteriormente. Como se segue:

Tabela 4

•	0	1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12	**13**	14	15	16	**17**
0	1																	
1			①	①														
2					1	②	1											
3							1	③	③	1								
4									1	④	6	④	1					
5											1	⑤	⑩	⑩	⑤	1		
6													1	⑥	15	20	15	⑥
7															1	7	㉑	㉟
8																	1	⑧

Fonte - Própria

A Tabela anterior mostra que o resultado é válido para $k = 1, 2, 3$ (de fato, até $k = 17$). Para $k = 2m$, um número par maior que 2, temos $m > 1$ e também que a primeira entrada da linha m ocorre na coluna k. Mas tal entrada corresponde ao número 1 e não será circulado pois, para $m > 1$, m não divide 1. Como os números pares superiores a 2 são compostos, a hipótese é válida para k pares.

Suponha, então, que k seja ímpar. Mostraremos que, se k é um número primo p, todas as entradas na coluna k são circuladas, isto é, k é composto, pelo menos um número na coluna k não é contornado. Observe que as linhas, n, que atribuem entradas na coluna k, são aqueles para os quais

$$2n \leq k \leq 3n,$$

isto é,

$$\frac{k}{3} \leq n \leq \frac{k}{2}$$

Analisando a linha n verificamos que a entrada atribuída por ela à coluna k é $\binom{n}{k-2n}$, conforme a tabela a seguir:

Tabela 5

$L\backslash C$	- - -	$2n$	$2n+1$	$2n+2$	- - -	k	- - -	$3n$	- - -
- - -	- - -	- - -	- - -	- - -		- - -	- - -	- - -	- - -
n	- - -	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	- - -	$\binom{n}{k-2n}$	- - -	$\binom{n}{n}$	- - -
- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -

Fonte - (HONSBERGER, 1976)

(i)Se $k = p$, um primo maior que 3, as entradas na coluna k são $\binom{n}{p-2n}$ onde,

$$\frac{p}{3} \leq n \leq \frac{p}{2}$$

Como p é maior que 3, temos $1 < n < p$, implicando que n e p são números relativamente primos. Isso significa que n e $p - 2n$ também são relativamente primos.

Segue que para cada uma das entradas $\binom{n}{P-2n}$ dessa coluna, temos

$$\begin{aligned}\binom{n}{p-2n} &= \frac{n!}{(p-2n)!(3n-p)!} \\ &= \frac{n}{p-2n} \cdot \frac{(n-1)!}{(p-2n-1)!(3n-p)!} \\ &= \frac{n}{p-2n}\binom{n-1}{p-2n-1}\end{aligned}$$

E assim,

$$(p-2n)\binom{n}{p-2n} = n\binom{n-1}{p-2n-1}$$

Consequentemente, n está no lado direito da equação. Mas, como n e $p - 2n$ são relativamente primos, concluímos que n divide $\binom{n}{p-2n}$, e, portanto, a entrada é circulada.

(ii) Finalmente, suponha que k seja um número composto ímpar. Como tal, é o produto de dois ou mais números primos ímpares. Denote por p um divisor primo ímpar de k. Assim:

$$k = p(2r + 1)$$

(P divide k um número ímpar de vezes). Como k é composto, devemos ter $r \geq 1$. Consequentemente, temos $p \leq pr$ e

$$2pr < k = 2pr + p \leq 3pr$$

Assim, a linha $n = pr$ contribui para a coluna k, e sua entrada é

$$\binom{n}{p-2n} = \binom{pr}{p}$$

Mostraremos que $n = pr$ não divide esse número, implicando que a coluna k tem um número não circulado.

Do **lema:** 1.2 sabemos que

$$\binom{pq}{p} = \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p!}$$

Realizando a divisão de $\binom{pq}{p}$ por pq tem-se

$$\begin{aligned} \frac{1}{pq}\cdot\binom{pq}{p} &= \frac{1}{pq}\cdot\frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p!} \\ &= \frac{(pq-1)(pq-2)\cdots(pq-p+1)}{1\cdot 2\cdot 3...\cdot p} \end{aligned}$$

Nenhum fator $(pq-i)$ no numerador é divisível pelo número primo p pois $1 \leq i \leq p-1$. Desse modo, a fração não se reduz a um número inteiro e, por consequência pq não divide $\binom{pq}{p}$. Portanto, se os coeficientes do Triângulo de Pascal com colunas deslocadas 2 a são divisíveis pelo número da linha correspondente, então o número da coluna é primo.

■

4 Construção de tabelas T_m

O objetivo de tal capitulo é apresentar uma generalização do resultado principal dos capítulos anteriores. Veremos que existe um teste de primalidade para as tabelas Tm. Faremos primeiramente a construção das tabelas Tm e por fim apresentaremos (sem demonstração) o teste de primalidade geral para Tm.

Definição 4.1 *Para qualquer $m > 0$, T_m é a tabela cujas linhas são indexadas por n = 0,1,2,..., e colunas por k = 0, 1, 2, ... e cujas entradas são obtidas da seguinte maneira:*

(a) T_0 é a tabela formada por zeros;

(b) T_1 é a tabela cujas linhas são compostas de 1 seguido por zeros;

(c) T_m; $m \geq 2$, é a tabela cuja linha n = 0 é formada por 1 seguido por zeros, cuja linha n = 1 é composta de m números 1 seguido por zeros e qualquer uma das entradas nas linhas subsequentes é a soma das m entradas logo acima e à esquerda na linha anterior.

Exemplo 4.1 *Construção da tabela T_2:*

Tabela 6 – T_2

l/c	0	1	2	3	4	5	6	...
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
...								...

Fonte - Própria

Exemplo 4.2 *Construção da tabela T_3:*

Exemplo 4.3 *Construção da tabela T_4:*

Definição 4.2 *A interseção da linha l e coluna c na tabela T_m é denotada por $C_m(l, c)$.*

Exemplo 4.4 *(a) $C_2(0, 0) = 1$*

Tabela 7 – T_3

l/c	0	1	2	3	4	5	6	...
0	1							
1	1	1	1					
2	1	2	3	2	1			
3	1	3	6	7	6	3	1	
4	1	4	10	16	19	16	10	...
5	1	5	15	30	45	51	45	...
6	1	6	21	50	90	126	141	...
...								...

Fonte - Própria

Tabela 8 – T_4

l/c	0	1	2	3	4	5	6	...
0	1							
1	1	1	1	1				
2	1	2	3	4	3	2	1	
3	1	3	6	10	12	12	10	
4	1	4	10	20	31	40	44	...
5	1	5	15	35	65	101	135	...
6	1	6	21	56	120	216	336	...
...								...

Fonte - Própria

Exemplo 4.5 *(b)* $C_2(0,5) = 0$

Exemplo 4.6 *(c)* $C_2(6,4) = 15$

Exemplo 4.7 *(d)* $C_3(6,4) = 90$

Exemplo 4.8 *(e)* $C_4(6,4) = 120$

Observemos que T_2 é o triângulo de Pascal então:

$$C_2(l,c) = \binom{l}{c}$$

Além disso, existem $(m-1)n+1$ entradas diferentes de zero na linha l e esses são os coeficientes da expansão:

$$(1 + x + x^2 + ... + x^{l-1})^l = \sum_{c=0}^{(m-1)l} C_m(l, c)x^c$$

Exemplo 4.9 *Considere a expansão:* $(1 + x)^2$ *então:*

$$(1 + x)^2 = \sum_{c=0}^{l=2} C_2(2, c)x^c$$

$$\sum_{c=0}^{l=2} C_2(2, c)x^c = C_2(2, 0)x^0 + C_2(2, 1)x^1 + C_2(2, 2)x^2$$

Portanto,

$$(1 + x)^2 = 1 \cdot x^0 + 2 \cdot x^1 + 1 \cdot x^2$$

Exemplo 4.10 *Considere a expansão:* $(1 + x)^3$ *então:*

$$(1 + x)^3 = \sum_{c=0}^{l=3} C_2(3, c)x^c$$

$$\sum_{c=0}^{l=3} C_2(3, c)x^c = C_2(3, 0)x^0 + C_2(3, 1)x^1 + C_2(3, 2)x^2 + C_2(3, 3)x^3$$

Portanto,

$$(1 + x)^3 = 1 \cdot x^0 + 3 \cdot x^1 + 3 \cdot x^2 + 1 \cdot x^3$$

Definição 4.3 *O número* $\dfrac{l!}{l_1!l_2! \cdot ... \cdot l_m!}$*, denotado por* $\binom{l}{l_1, l_2, ..., l_m}$ *é denominado coeficiente multinomial.*

Teorema 4.1 *(Teorema multinomial) Para todo* $x_1, x_2, ..., x_m$ *e para* l *inteiro positivo vale a seguinte igualdade:*

$$(1 + x_1 + x_2 + ... + x_m)^l = \sum \binom{l}{l_1, l_2, ..., l_m} x_1^{l_1} \cdot x_2^{l_2} \cdot ... \cdot x_m^{l_m}$$

onde a soma se estende sobre todas as combinações possíveis de inteiros não negativos $l_1, l_2, ..., l_m$ *tais que* $l_1 + l_2 + ... + l_m = l$

Teorema 4.2 *Se* $C_m(l, c)$ *é a interseção entre a linha* l *e a coluna* c *em* T_m*;* $m \geq 3$*, então para todo* $l \geq 0$ *e* $0 \leq c \leq l(m - 1)$*, vale:*

$$C_m(l, c) = \sum_{l_1, l_2, ..., l_m} \binom{l}{l_1, l_2, ..., l_m}$$

onde a soma se estende sobre todas as combinações possíveis de inteiros não negativos $l_1, l_2, ..., l_m$ *tais que* $l_1 + l_2 + ... + l_m = l$ *e* $0l_1 + 1l_2 + ... + (m - 1)l_m = c$.

Teorema 4.3

$$C_m(l,c) = \sum_{j=0}^{l} \binom{l}{c} C_{m-1}(j, c-j)$$

O leitor interessado pode consultar (BOLLINGER, 1986), para as demonstrações dos teoremas 4.2 e 4.3. Nota-se também que tais resultados decorrem do teorema 4.1.

Exemplo 4.11 *Encontre o termo* $C_3(3,3)$.
Solução:

$$\begin{aligned} C_3(3,3) &= \sum_{j=0}^{l=3} \binom{3}{c} C_2(j, 3-j) \\ &= \binom{3}{0} C_2(0,3) + \binom{3}{1} C_2(1,2) + \binom{3}{2} C_2(2,1) + \binom{3}{3} C_2(3,0) \\ &= \binom{3}{0} \cdot 0 + \binom{3}{1} \cdot 0 + \binom{3}{2} \cdot 2 + \binom{3}{3} \cdot 1 \\ &= 0 + 0 + 3 \cdot 2 + 1 \cdot 1 \\ &= 7 \end{aligned}$$

Exemplo 4.12 *Encontre o termo* $C_3(5,5)$.
Solução:

$$\begin{aligned} C_3(5,5) &= \sum_{j=0}^{l=5} \binom{5}{c} C_2(j, 5-j) \\ &= \binom{5}{0} C_2(0,5) + \binom{5}{1} C_2(1,4) + \binom{5}{2} C_2(2,3) + \binom{5}{3} C_2(3,2) + \binom{5}{4} C_2(4,1) + \binom{5}{5} C_2(5,0) \\ &= \binom{5}{0} \cdot 0 + \binom{5}{1} \cdot 0 + \binom{5}{2} \cdot 0 + \binom{5}{3} \cdot 3 + \binom{5}{4} \cdot 4 + \binom{5}{5} \cdot 1 \\ &= 0 + 0 + 0 + 10 \cdot 3 + 5 \cdot 4 + 1 \cdot 1 \\ &= 51 \end{aligned}$$

Exemplo 4.13 *Encontre o termo* $C_4(6,5)$.
Solução:

$$\begin{aligned} C_4(6,5) &= \sum_{j=0}^{l=6} \binom{6}{c} C_2(j, 5-j) \\ &= \binom{6}{0} C_3(0,5) + \binom{6}{1} C_3(1,4) + \binom{6}{2} C_3(2,3) + \binom{6}{3} C_3(3,2) + \binom{6}{4} C_3(4,1) + \binom{6}{5} C_3(5,0) \\ &= \binom{6}{0} \cdot 0 + \binom{6}{1} \cdot 0 + \binom{6}{2} \cdot 2 + \binom{6}{3} \cdot 6 + \binom{6}{4} \cdot 4 + \binom{6}{5} \cdot 1 + 0 \\ &= 0 + 0 + 15 \cdot 2 + 20 \cdot 6 + 15 \cdot 4 + 6 \cdot 1 + 0 \\ &= 216 \end{aligned}$$

* *Veja que* $C_3(6,-1)$ *não existe em* T_3, *logo tomamos como sendo 0.*

Enunciaremos o Teorema geral para o Teste de Primalidade em tabelas T_m que pode ser visto de modo mais aprofundado em (EGER, 2014) .

Definição 4.4 *Os coeficientes binomiais estendidos* $\binom{n}{k}_{(f(s))s\in\mathbb{N}}$, *onde* $\mathbb{N} = \{0, 1, 2, ...\}$ *são definidos da seguinte forma:*

$$\binom{n}{k}_{(f(s))s\in\mathbb{N}} = [x^n](\sum_{s\in\mathbb{N}} f(s)x^s)^k$$

Onde $f : \mathbb{N} \longrightarrow \mathbb{N}$ *é uma função de ponderação e* $[x^n]p(x)$ *denota o coeficiente de* x^n *na série polinomial ou de potência* $p(x)$.

Teorema 4.4 *Considere os coeficientes* $\binom{n}{k}_{(f(s))s\in\mathbb{N}}$. *Seja* $f(0) = f(1) = 1$. *Então, um número inteiro* $n > 1$ *é primo se e somente se* m *divide* $\binom{m}{n-2m}_{(f(s))s\in\mathbb{N}}$ *para todo inteiros* m *com* $0 \leq 2m \leq n$.

Conclusão

Neste trabalho estudamos O Triângulo de Pascal T_2, bem como a variação da coluna em relação a uma linha l dada, isto é, partindo de uma linha fixa l, a variação de certa coluna c será: $2l \leq c \leq l$. Observar tal comportamento se faz relevante para prova do Critério de Primalidade de Mann-Shanks.

Não obstante, analisamos a variação dos termos binomiais presentes em certa linha l, ou seja, os termos $\binom{l}{r}$, que estão limitados por $\binom{l}{0}$ e $\binom{l}{k_\alpha}$; $0 \leq k_\alpha \leq l$.

Ressaltamos que a demonstração do Critério de Primalidade de Mann-Shanks foi realizada de modo a facilitar a compressão do leitor. Assim, dividimos a prova necessária e suficiente do Método em dois teoremas. Além disso, durante toda demonstração, utilizamos exemplos elucidativos com base nos processos lógicos seguidos.

O trabalho possibilitou ainda, a construção de uma notação única baseada em (MANN; SHANKS, 1972).Onde, $c_p = 6a + 1$ e $c_p = 6a - 1$ são as colunas analisadas, ϕ são os coeficientes presentes na coluna c_p.Utilizamos também (HONSBERGER, 1976) para outra possibilidade de demonstração levemente diferente.

Em resumo, mostramos que tal Critério é válido para O Triangulo de Pascal T_2, mas, de modo geral, é válido para Tn como verificamos no quarto capítulo. O leitor interessado pode consultar (EGER, 2014) para sua demonstração.

Referências

BOLLINGER, R. C. A note on pascal-t triangles, multinomial coefficients, and pascal pyramids. *relation*, Citeseer, v. 1000, p. 1, 1986. Citado na página 40.

CHONG, C. C.; KHEE-MENG, K. *Principles and techniques in combinatorics*. [S.l.]: World Scientific, 1992. Citado na página 12.

EGER, S. A proof of the mann-shanks primality criterion conjecture for extended binomial coefficients. *Integers*, v. 14, p. A60, 2014. Citado 2 vezes nas páginas 41 e 42.

FILHO, E. de A. *Teoria elementar dos números*. [S.l.]: Nobel, 1981. Citado na página 12.

HONSBERGER, R. Mathematical gems ii: The dolciani mathematical expositions. *Mathematical Association of America*, n. 2, p. 12, 1976. Citado 2 vezes nas páginas 34 e 42.

KOSHY, T. *Catalan numbers with applications*. [S.l.]: Oxford University Press, 2008. Citado na página 12.

MANN, H. B.; SHANKS, D. A necessary and sufficient condition for primality, and its source. *Journal of Combinatorial Theory, Series A*, Elsevier, v. 13, n. 1, p. 131–134, 1972. Citado 3 vezes nas páginas 28, 33 e 42.