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

SABRINA DE SOUSA CRUZ

PROPRIEDADES ARITMÉTICAS DOS COEFICIENTES BINOMIAIS

FORTALEZA
2022

SABRINA DE SOUSA CRUZ

PROPRIEDADES ARITMÉTICAS DOS COEFICIENTES BINOMIAIS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestra em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto Duarte Maia.

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C964p Cruz, Sabrina de Sousa.
Propriedades aritméticas dos coeficientes binomiais / Sabrina de Sousa Cruz. – 2022.
77 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2022.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Coeficientes binomiais. 2. Propriedades aritméticas. 3. Divisibilidade. 4. Números primos. I. Título.
CDD 510

SABRINA DE SOUSA CRUZ

PROPRIEDADES ARITMÉTICAS DOS COEFICIENTES BINOMIAIS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestra em Matemática. Área de Concentração: Ensino de Matemática.

Aprovada em: 08/04/2022

BANCA EXAMINADORA

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Antonio Caminha Muniz Neto
Universidade Federal do Ceará (UFC)

Prof. Dr. Joserlan Perote da Silva
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Ao meu esposo Jones e ao meu filho Isaac, família linda que Deus me permitiu construir. De onde tudo parte, para onde tudo retorna!

AGRADECIMENTOS

Ao Pai criador que nos fez a sua imagem e semelhança e nos possibilita realizar grandes coisas aqui na Terra.

Ao meu esposo amado, Jones Cruz, companheiro de todas as horas pelo amor, o amparo, o incentivo e o exemplo de determinação. Sua mão segurando a minha me deu forças para acreditar e sempre prosseguir.

Ao meu filho Isaac, meu coração que bate fora do peito. Entendeu as minhas ausências para estudar, e me esperou a cada final de semana com amor e alegria.

À minha mãe, Nonata, que rezou por mim para que tudo desse certo, e que me ensinou que, na vida, nada era mais importante que o amor.

À minha madrinha Christiane Maia, ao Carlos, ao Inácio e a Ester por terem sido minha família em Fortaleza.

Aos meus amigos Jéssica Ximenes e Alberto Cunha, que me incentivaram a buscar o mestrado Profmat.

A todos os professores do Profmat, grandes doutores com os quais tive a honra de aprender, em especial ao meu orientador, Prof. Dr. José Alberto Duarte Maia, pelas melhores disciplinas e por este tema com o qual tanto me identifiquei.

Aos meus colegas de turma, pela união do início ao fim do curso. Não houve turma igual a nossa!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"A Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática."(GAUSS, 1966)

RESUMO

O objetivo deste estudo é reunir e levar ao conhecimento do público apreciador dos padrões em números, sejam alunos do ensino médio ou de nível superior, interessantes características dos coeficientes binomiais, bem como algumas de suas aplicações dentro da própria Matemática. De início, apresenta a definição desses números especiais como coeficientes de polinômios conhecidos, sua organização dentro do arranjo conhecido como triângulo de Pascal e as propriedades relativas a esse arranjo. Em seguida, introduz a Aritmética com os conceitos e propriedades da divisibilidade e da congruência entre os números inteiros, para então adentrar nas propriedades aritméticas dos coeficientes binomiais. Por fim, apresenta o triângulo de Pascal módulo p primo, dando ênfase ao caso $p = 2$ e discorre sobre a divisibilidade de certas expressões com binomiais por potências do número primo p.

Palavras-chave: coeficientes binomiais; propriedades aritméticas; divisibilidade; números primos.

ABSTRACT

The objective of this study is to gather and bring to the attention of the public that appreciates patterns in numbers, whether high school or college students, interesting characteristics of binomial coefficients, as well as some of their applications within Mathematics itself. At first, it presents the definition of these special numbers as coefficients of known polynomials, their organization within the arrangement known as Pascal's triangle and the properties related to this arrangement. Next, it introduces Arithmetic with the concepts and properties of divisibility and congruence between integers, and then enters into the arithmetic properties of binomial coefficients. Finally, it presents Pascal's triangle modulo p primo, emphasizing the case $p = 2$ and discusses the divisibility of certain expressions with binomials by powers of the prime number p.

Keywords: binomial coefficients; arithmetic properties; divisibility, prime numbers.

LISTA DE FIGURAS

Figura 1 – Triângulo aritmético com valores numéricos 17
Figura 2 – Triângulo de Pascal até a linha 9 49
Figura 3 – Triângulo de Pascal até a linha 9 módulo 3 50
Figura 4 – Exemplo da Relação de Stifel módulo 3 51
Figura 5 – Triângulo de Pascal módulo 2 51
Figura 6 – Estrutura do triângulo de Pascal módulo 2 52
Figura 7 – Triângulo de Sierpinski a partir do triângulo de Pascal módulo 2 53
Figura 8 – Triângulo de Pascal módulo 3, módulo 5 e módulo 7 54

SUMÁRIO

1	**INTRODUÇÃO**	11
2	**COEFICIENTES BINOMIAIS**	13
2.1	**Definição**	13
2.2	**O Triângulo Aritmético**	14
3	**DIVISIBILIDADE E CONGRUÊNCIAS**	26
3.1	**Divisibilidade**	26
3.2	**Congruências**	31
3.3	**Sistema completo de resíduos**	35
4	**PROPRIEDADES ARITMÉTICAS DOS COEFICIENTES BINOMIAIS**	38
4.1	**Congruências binomiais**	38
4.2	**Teorema de Lucas**	43
4.3	**O Triângulo Aritmético módulo p (primo)**	49
5	**CONGRUÊNCIAS BINOMIAIS POR POTÊNCIAS DE PRIMOS**	55
5.1	**O caso $p = 2$.**	55
5.2	**O caso geral**	59
6	**CONCLUSÃO**	74
	REFERÊNCIAS	76

1 INTRODUÇÃO

Desde os tokens de argila, há 10 mil anos até cálculos feitos hoje por potentes computadores, a utilização dos números para a resolução de problemas é um aspecto marcante da história da humanidade. Para além da sua utilização prática, o fascínio exercido por seus padrões fez com que, ao longo do tempo, muitos matemáticos dedicassem seus estudos ao desenvolvimento da Aritmética e mais tarde, à Teoria dos Números, que até o início do século XX, figurou como um ramo da Matemática pura, com aplicações quase que exclusivamente na própria Matemática. A era digital, porém, com a linguagem dos computadores, mudou essa realidade, trazendo à Teoria dos Números uma gama de possibilidades em termos de aplicabilidade.

Historicamente, segundo (EVES, 1996), admite-se que os primeiros passos no sentido do desenvolvimento da Teoria dos Números foram dados por Pitágoras e seus seguidores movidos pela filosofia da fraternidade. Contudo, nada há de registro formal sobre o trabalho realizado por Pitágoras e seus seguidores. A primeira menção ao estudo dos números inteiros (nesta época sendo considerados apenas os inteiros positivos) aparece, de fato, nos Elementos de Euclides (300 a.C.), mais especificamente nos livros VII, VIII e IX. Nestes, Euclides dá uma definição para número, define números primos e compostos e apresenta uma prova parcial do que hoje conhecemos como Teorema Fundamental da Aritmética. Seguem-se a Euclides, com com grandes contribuições, Diofanto de Alexandria (200 d.C), Pierre de Fermat[1], Leonhard Euler[2] e Carl Friedrich Gauss[3], este último tendo desenvolvido substancialmente a Teoria dos Números com a introdução do conceito da aritmética modular.

Sob a luz das contribuições deixadas por estes grandes personagens da história, este trabalho tem a missão de levar ao público apreciador dos números, seja composto de alunos da graduação ou de alunos do ensino médio com bom conhecimento em Matemática, interessantes aspectos aritméticos a respeito dos coeficientes binomiais. Para isto, conceituamos estes números particulares, tratando-os como coeficientes de polinômios conhecidos, e não como expressões de processos combinatórios. Neste sentido, tomamos por base a conceituação apresentada na revista Kvant(TABACHNIKOV, 1999), particularmente no parte que trata da aritmética dos coeficientes binomiais.

---

1 Fermat, Pierre de (1601 – 1665), magistrado, matemático amador e cientista francês.
2 Euler, Leonhard Paul, (1707 – 1783), matemático e físico suíço.
3 Gauss, Carl Friedrich (1777-1855), matemático, astrônomo e físico alemão.

No segundo capítulo, seguinte à introdução, apresentamos, além da definição de coeficientes binomiais, a organização desses números no triângulo aritmético, usualmente denominado triângulo de Pascal[4]. Aqui também enumeramos as principais propriedades referentes ao triângulo e propomos demonstrações acessíveis ao público a que se destina o presente texto. Já no capítulo 3, discorremos de maneira sucinta sobre divisibilidade e congruências, mostrando teoremas, proposições e exemplos, a fim de introduzir o assunto central do trabalho, constante no capítulo posterior.

No que tange às propriedades aritméticas dos coeficientes binomiais, tratam-se de aspectos referentes à divisibilidade desses números por números inteiros positivos, em especial por números primos. Este é o objeto do capítulo 4, no qual mostramos muitos exemplos de situações-problema onde o conhecimento dessas propriedades podem levam a soluções por caminhos mais curtos. Na última seção, exibimos ainda algumas curiosidades sobre o triângulo de Pascal módulo p primo, uma estrutura composta pelos restos da divisão euclidiana de cada coeficiente binomial, nas suas respectivas posições, pelo número p. Esta estrutura, independente de qual seja o primo p, guarda todas as propriedades do triângulo de Pascal inicial e apresenta padrões muito interessantes, que visualmente estão de acordo com padrões geométricos explicitados também nesta exibição.

Por fim, o capítulo 5 avança na aritmética dos coeficientes binomiais, propondo um olhar mais apurado sobre a divisibilidade de expressões com coeficientes binomiais por potências de números primos. Neste ponto, o leitor familiarizado com os conceitos apresentados até então, tem contato com notações especiais e uma Matemática mais elaborada, embora perfeitamente acessível ao público especificado no início desta introdução. Neste e nos demais capítulos, não utilizamos Matemática de nível superior, e quando as demonstrações demandaram um pouco mais de rigor, simplificamos ao máximo, com o objetivo de manter a inteligibilidade durante todo o material proposto.

[4] Pascal, Blaise (1623-1662), matemático, filósofo e físico francês.

2 COEFICIENTES BINOMIAIS

Neste capítulo, apresentaremos uma definição de coeficientes binomiais com base no desenvolvimento do binômio de Newton [1]. O caráter combinatório desses números não será levado em consideração, porquanto não seja importante para o resultado principal deste trabalho. Analisaremos ainda a distribuição desses coeficientes no Triângulo Aritmético, dando enfase às suas propriedades mais relevantes.

2.1 Definição

Ao elevarmos o binômio $(1+x)$ a algum expoente n, onde n é um número inteiro não negativo, obtemos como resultado um polinômio de grau n, ou seja, a maior potência de x no polinômio obtido é igual a n. Por exemplo, para $0 \leq n \leq 5$, temos

$$\begin{aligned}
(1+x)^0 &= 1,\\
(1+x)^1 &= 1+x,\\
(1+x)^2 &= 1+2x+x^2,\\
(1+x)^3 &= 1+3x+3x^2+x^3,\\
(1+x)^4 &= 1+4x+6x^2+4x^3+x^4,\\
(1+x)^5 &= 1+5x+10x^2+10x^3+5x^4+x^5.
\end{aligned}$$

Em cada um dos polinômios acima, os termos são compostos de potências crescentes de x acompanhadas de coeficientes naturais. Estes coeficientes recebem uma notação especial, como enunciaremos na seguinte definição.

Definição 2.1 Sejam m e n números inteiros não negativos. Denotamos por $\binom{n}{m}$ o coeficiente de x^m no desenvolvimento de $(1+x)^n$.

Exemplo 2.2 De acordo com o definição dada, o polinômio resultante no desenvolvimento de $(1+x)^4$ pode ser expresso da seguinte forma

$$(1+x)^4 = \binom{4}{0}x^0 + \binom{4}{1}x + \binom{4}{2}x^2 + \binom{4}{3}x^3 + \binom{4}{4}x^4.$$

[1] Newton, Isaac (1642-1727), matemático e físico inglês.

E de modo geral, para $0 < k < n$ escrevemos

$$(1+x)^n = \binom{n}{0}x^0 + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{k}x^k + \ldots + \binom{n}{n}x^n. \tag{2.1}$$

De acordo com a definição 2.1, os números $\binom{n}{m}$ são inteiros não negativos, pois são os coeficientes no desenvolvimento de $(1+x)^n$. Ainda com base neste desenvolvimento, é imediato observar que $\binom{n}{0} = \binom{n}{n} = 1$, respectivamente os coeficientes do primeiro e do último termo do polinômio obtido. Além disso, se $m > n$, então $\binom{n}{m} = 0$, dado que o grau de $(1+x)^n$ é igual a n, ou seja, não aparecem termos em x^m no polinômio resultante.

Aplicando a fórmula 2.1 para $\left(1+\frac{x}{a}\right)^n$ e multiplicando ambos os membros da equação obtida por a^n, obtemos uma expressão para $(x+a)^n$, como mostramos a seguir.

$$\left(1+\frac{x}{a}\right)^n a^n = \binom{n}{0}\left(\frac{x}{a}\right)^0 a^n + \binom{n}{1}\left(\frac{x}{a}\right)a^n + \ldots + \binom{n}{k}\left(\frac{x}{a}\right)^k a^n + \ldots + \binom{n}{n}\left(\frac{x}{a}\right)^n a^n$$

Ou seja,

$$(a+x)^n = \binom{n}{0}a^n x^0 + \binom{n}{1}a^{n-1}x + \ldots + \binom{n}{k}a^{n-k}x^k + \ldots + \binom{n}{n}x^n. \tag{2.2}$$

A expressão 2.2 é chamada de binômio de Newton, e seus coeficientes são, portanto, coeficientes binomiais. O termo coeficiente binomial foi introduzido por Michael Stifel [2], que mostrou, em torno de 1550, como calcular $(1+x)^n$ a partir do desenvolvimento de $(1+x)^{n-1}$. Isaac Newton, porém, o fez diretamente e foi além, mostrando como calcular $(1+x)^r$, com r pertencente ao conjunto dos números racionais. (MORGADO *et al.*, 1991).

2.2 O Triângulo Aritmético

De posse da definição de coeficientes binomiais dada na seção anterior, podemos organizar esses números em uma tabela numérica triangular na qual o número indicativo da linha represente o expoente do Binômio de Newton e o número indicativo da coluna indique o expoente de x no desenvolvimento de $(1+x)^n$. Neste arranjo, consideramos apenas os coeficientes binomiais não nulos, ou seja, $0 \leq m \leq n$. As linhas e colunas são contadas a partir do 0, sendo numeradas, respectivamente, da esquerda para a direita e de cima para baixo, de modo que o elemento $\binom{n}{m}$ esteja situado na nª linha e na mª coluna, como podemos visualizar

[2] Stifel, Michael (1487?-1567), algebrista alemão.

abaixo.

	Coluna 0	Coluna 1	Coluna 2	Coluna 3	Coluna 4	...	Coluna n
Linha 0	$\binom{0}{0}$						
Linha 1	$\binom{1}{0}$	$\binom{1}{1}$					
Linha 2	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$				
Linha 3	$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$			
Linha 4	$\binom{4}{0}$	$\binom{4}{1}$	$\binom{4}{2}$	$\binom{4}{3}$	$\binom{4}{4}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
Linha n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	...	$\binom{n}{n}$.

Conhecido como Triângulo de Pascal ou de Tartaglia[3]- Pascal, o triângulo aritmético já era conhecido na China do século XIII, e antes disso pelos matemáticos hindus e árabes. No Ocidente, apareceu pela primeira vez no frontispício do livro *Rechnung* (1527), de Petrus Apianus [4], um século antes do nascimento de Pascal. Segundo Morgado (1991, p. 3), Nicolo Fontana Tartaglia relacionou os elementos do triângulo aritmético com as potências de $(x+y)$. Pascal publicou um tratado em 1654 mostrando como utilizá-lo para achar os coeficientes do desenvolvimento de $(a+b)^n$.

No decorrer da História da Matemática, foram estabelecidas muitas identidades por meio do triângulo aritmético, sendo estas aplicadas, por exemplo, na obtenção de raízes de equações ou no estudo das probabilidades. Enunciaremos a seguir algumas dessas identidades.

---

[3] Tartaglia, Nicolo Fontana (cerca de 1500-1557), matemático italiano.

[4] Apianus, Petrus (1495-1552), matemático e astrônomo alemão.

Teorema 2.3 (Relação de Stifel) Para todos os inteiros não negativos m e n, tem-se

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}. \tag{2.3}$$

Prova. Por definição, o número $\binom{n}{m}$ é o coeficiente de x^m no polinômio $(1+x)^n$. Para determinarmos esses coeficientes, em princípio é necessário multiplicarmos $(1+x)$ por ele mesmo n vezes. Vamos iniciar multiplicando $(1+x)$ por ele mesmo $(n-1)$ vezes. Assim, obtemos

$$(1+x)^{n-1} = 1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \ldots + \binom{n-1}{m-1}x^{m-1} + \binom{n-1}{m}x^m + \ldots + x^{n-1}.$$

Para obtermos a identidade desejada, procedemos, então, com a ultima multiplicação, ou seja, multiplicamos $(1+x)^{n-1}$ por $(1+x)$. Assim,

$$\begin{aligned}
(1+x)^n &= (1+x)\left[1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \ldots + \binom{n-1}{m-1}x^{m-1} + \binom{n-1}{m}x^m + \ldots + x^{n-1}\right] \\
&= \left[1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \ldots + \binom{n-1}{m-1}x^{m-1} + \binom{n-1}{m}x^m + \ldots + x^{n-1}\right] \\
&\quad + \left[x + \binom{n-1}{1}x^2 + \binom{n-1}{2}x^3 + \ldots + \binom{n-1}{m-1}x^m + \binom{n-1}{m}x^{m+1} + \ldots + x^n\right] \\
&= 1 + \left[\binom{n-1}{1} + 1\right]x + \left[\binom{n-1}{2} + \binom{n-1}{1}\right]x^2 + \ldots + \left[\binom{n-1}{m} + \binom{n-1}{m-1}\right]x^m + \ldots + x^n.
\end{aligned}$$

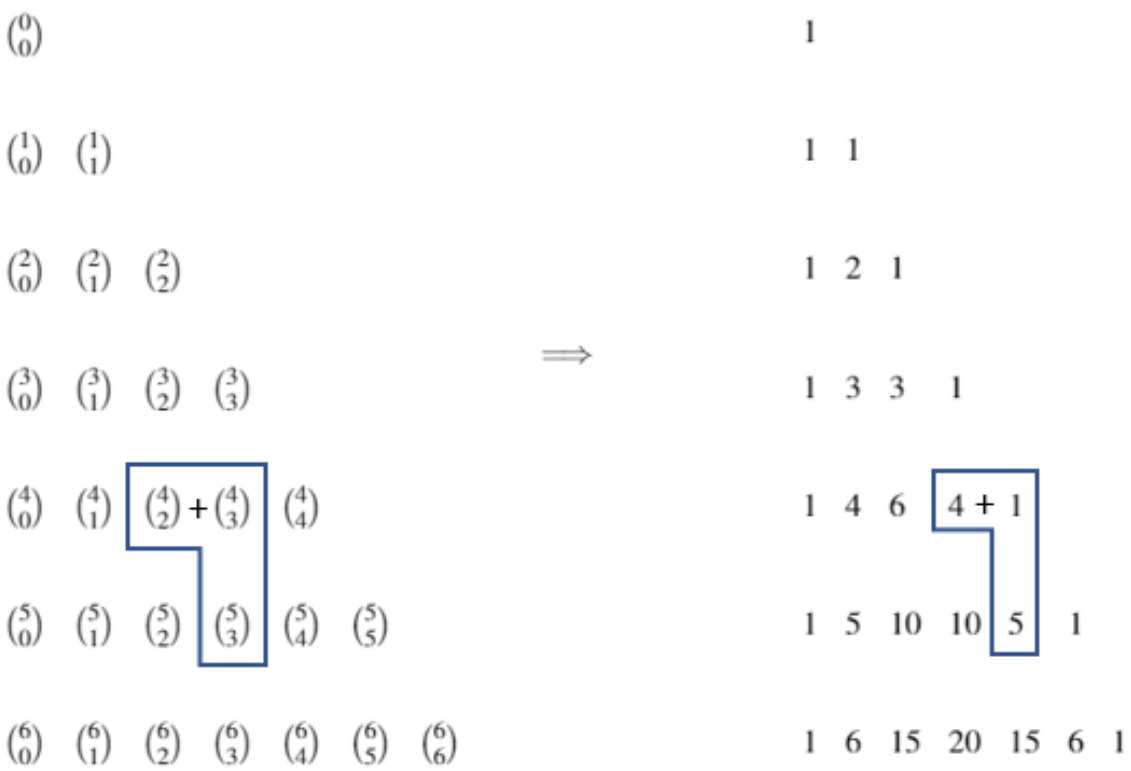
Vejamos que $\binom{n-1}{m} + \binom{n-1}{m-1}$ é o coeficiente de x^m em $(1+x)^n$, o que completa a nossa prova.

□

A relação de Stifel é bastante útil para calcularmos diversas linhas do triângulo aritmético, utilizando as linhas anteriores. Por exemplo, para calcularmos $\binom{2}{1}$, fazemos $\binom{2}{1} = \binom{1}{0} + \binom{1}{1}$. Prosseguindo para as demais linhas, podemos obter qualquer que seja a linha desejada.

Na figura a seguir, utilizamos a relação de Stifel para determinarmos os valores numéricos dos coeficientes binomiais até a 6ª linha do triângulo aritmético.

Figura 1 – Triângulo aritmético com valores numéricos



Fonte: Elaborado pela autora.

Teorema 2.4 (Fórmula para coeficientes binomiais) Sejam m, n inteiros não negativos, então

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m}. \tag{2.4}$$

Prova. Para esta prova, usaremos indução sobre n. Para $n = 1$, a igualdade 2.4 é válida, pois

$$\binom{1}{1} = 1 = \frac{1}{1} \qquad \text{e}$$

$$\binom{1}{m} = 0 = \frac{1\cdot 0\cdots(1-m+1)}{1\cdot 2\cdots m}, \quad m > 1$$

Assumindo, então, por hipótese, que 2.4 seja válida para $n-1$, verifiquemos sua validez para todo n. Assim, se

$$\binom{n-1}{m} = \frac{(n-1)(n-2)\cdots(n-m)}{1\cdot 2\cdots m}, \qquad m = 1,2,3,\ldots$$

temos dois casos a considerar:

(i) Se $m > 1$, pela relação de Stifel,

$$\begin{aligned}
\binom{n}{m} &= \binom{n-1}{m} + \binom{n-1}{m-1} \\
&= \frac{(n-1)(n-2)\cdots(n-m+1)(n-m)}{1\cdot 2\cdots(m-1)m} + \frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\
&= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\left[\frac{n-m}{m}+1\right] \\
&= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\frac{n}{m} \\
&= \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m}.
\end{aligned}$$

(ii) Se $m = 1$, ainda pela relação de Stifel,

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1} = \binom{n-1}{1} + \binom{n-1}{0} = \frac{n-1}{1} + 1 = \frac{n}{1}.$$

Portanto, pelo princípio da indução finita, a igualdade (2.4) é válida para todo n, como queríamos provar. □

A relação de Stifel e a fórmula demonstrada acima são as propriedades mais úteis sobre coeficientes binomiais para o estudo que propomos. Vamos, porém, nos ater um pouco mais sobre outras propriedades referentes ao triângulo aritmético. Para os teoremas subsequentes, consideremos sempre $0 \leq m \leq n$, com m, n inteiros não negativos.

Teorema 2.5 (Binomiais Complementares) Para todos m, n inteiros não negativos, com $n \geq m$, é válido

$$\binom{n}{m} = \binom{n}{n-m} \tag{2.5}$$

Prova. A igualdade é óbvia para $m = n$ ou $m = n - m$. Suponhamos, então, sem perda de generalidade, $m < n - m$ (o caso $m > n - m$ é totalmente análogo). Segue da fórmula para coeficientes binomiais que

$$\begin{aligned}\binom{n}{n-m} &= \frac{n(n-1)\cdots[n-(n-m)+1]}{1\cdot 2\cdots(n-m)} \\ &= \frac{n(n-1)\cdots(m+1)}{1\cdot 2\cdots(n-m)} \\ &= \frac{n(n-1)\cdots(n-m+1)(n-m)\cdots(m+1)}{1\cdot 2\cdots m(m+1)\cdots(n-m)} \\ &= \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m} = \binom{n}{m}.\end{aligned}$$

Provamos, assim, que a identidade 2.5 é válida para todos m, n inteiros não negativos, com $0 \leq m \leq n$.

□

Teorema 2.6 (Teorema das Linhas) Sejam n, $m \in \mathbb{Z}$, com $0 \leq m \leq n$, verifica-se que

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n \tag{2.6}$$

Prova. Provaremos utilizando indução sobre n e a relação de Stifel. Para $n = 1$, temos

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

Assumindo, agora, que 2.6 seja válida para $n-1$, com $n > 1$, ou seja

$$\binom{n-1}{0} + \binom{n-1}{1} + \ldots + \binom{n-1}{n-1} = 2^{n-1},$$

verifiquemos se também é válida para n. Para isso, lembremos que, pela relação de Stifel,

$$\begin{aligned}
\binom{n}{1} &= \binom{n-1}{0} + \binom{n-1}{1};\\
\binom{n}{2} &= \binom{n-1}{1} + \binom{n-1}{2};\\
&\vdots\\
\binom{n}{n-1} &= \binom{n-1}{n-2} + \binom{n-1}{n-1}.
\end{aligned}$$

Desta forma, calculamos

$$\begin{aligned}
\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} &=\\
\binom{n}{0} + \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \ldots + \left[\binom{n-1}{n-2} + \binom{n-1}{n-1}\right] + \binom{n}{n} &=\\
\binom{n-1}{0} + \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \ldots + \left[\binom{n-1}{n-2} + \binom{n-1}{n-1}\right] + \binom{n-1}{n-1} &=\\
2 \cdot \left[\binom{n-1}{0} + \binom{n-1}{1} + \binom{n-1}{2} + \ldots + \binom{n-1}{n-1}\right] = 2 \cdot 2^{n-1} &= 2^n.
\end{aligned}$$

Portanto, pelo princípio da indução finita, a igualdade (2.6) é válida para todo $n \in \mathbb{N}$.

□

Alternativamente, podemos demonstrar o teorema das linhas considerando o fato de que

$$\binom{n}{0}x^n + \binom{n}{1}x^{n-1} + \binom{n}{2}x^{n-2} + \ldots + \binom{n}{n-1}x + \binom{n}{n} = (1+x)^n.$$

Pois fazendo $x = 1$, obtemos exatamente o resultado desejado, ou seja

$$\binom{n}{0} \cdot 1^n + \binom{n}{1} \cdot 1^{n-1} + \binom{n}{2} \cdot 1^{n-2} + \ldots + \binom{n}{n-1} \cdot 1 + \binom{n}{n} = (1+1)^n$$

$$\implies \quad \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

A explicação de que a soma dos coeficientes binomiais é 2^n, porque este é $(1+1)^n$, foi dada por Wallis[5] em 1685 e W. Jones[6] em 1706. (EDWARDS, 2019).

[5] Wallis, John (1616-1703), matemático britânico.
[6] Jones, William (1675-1749), matemático galês.

Teorema 2.7 (Teorema das Colunas) Se m e k são inteiros não negativos, então

$$\binom{m}{m}+\binom{m+1}{m}+\ldots+\binom{m+k}{m}=\binom{m+k+1}{m+1} \tag{2.7}$$

Prova. Para o que precisamos, consideremos o polinômio

$$P(x)=x(1+x)^m+x(1+x)^{m+1}+x(1+x)^{m+2}+\ldots+x(1+x)^{m+k} \tag{2.8}$$

e calculemos o coeficiente de x^{m+1} neste polinômio. Desenvolvendo cada parcela, como em 2.1, temos

$$\begin{aligned} P(x) &= x\left[\binom{m}{0}x^0+\binom{m}{1}x^1+\ldots+\binom{m}{m}x^m\right] \\ &+ x\left[\binom{m+1}{0}x^0+\binom{m+1}{1}x^1+\ldots+\binom{m+1}{m}x^m+\binom{m+1}{m+1}x^{m+1}\right] \\ &+ \ldots+x\left[\binom{m+k}{0}x^0+\ldots+\binom{m+k}{m}x^m+\ldots+\binom{m+k}{m+k}x^{m+k}\right]. \end{aligned}$$

Como podemos ver, o coeficiente de x^{m+1} em $P(x)$ equivale à soma

$$\left[\binom{m}{m}+\binom{m+1}{m}+\ldots+\binom{m+k}{m}\right]. \tag{2.9}$$

Observemos agora que o polinômio dado é a soma dos termos de uma progressão geométrica de primeiro termo $x(1+x)^m$ e razão $(1+x)$. Sendo assim, podemos calcular esta soma e escrever o polinômio da seguinte forma

$$P(x)=\frac{x(1+x)^m\left[(1+x)^{k+1}-1\right]}{(1+x)-1}=(1+x)^{m+k+1}-(1+x)^m.$$

De onde concluímos que o coeficiente de x^{m+1} em $P(x)$ é igual a

$$\binom{m+k+1}{m+1}. \tag{2.10}$$

O coeficiente de x^{m+1} em $P(x)$ é único, o que nos garante a igualdade das expressões 2.9 e 2.10, ou seja

$$\binom{m}{m}+\binom{m+1}{m}+\ldots+\binom{m+k}{m}=\binom{m+k+1}{m+1}.$$

Sendo, portanto, válido o teorema 2.7. □

Teorema 2.8 (Teorema das Diagonais) Se m e k são inteiros não negativos, então

$$\binom{n}{0}+\binom{n+1}{1}+\binom{n+2}{2}+\ldots+\binom{n+k}{k}=\binom{n+k+1}{k} \tag{2.11}$$

Prova. Faremos aqui a prova por indução sobre k. Para $k=1$, temos

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

Supondo, por hipótese de indução que

$$\binom{n}{0}+\binom{n+1}{1}+\binom{n+2}{2}+\ldots+\binom{n+k-1}{k-1}=\binom{n+k}{k-1},$$

o que falta segue da relação de Stifel. Ou seja,

$$\binom{n}{0}+\binom{n+1}{1}+\binom{n+2}{2}+\ldots+\binom{n+k-1}{k-1}+\binom{n+k}{k} =$$

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

Portanto, pelo princípio da indução finita, é válida a igualdade 2.11.

□

Teorema 2.9 (Soma Alternada) Se n é um número inteiro não negativo, então vale a igualdade

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\ldots=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\ldots \tag{2.12}$$

Prova. Inicialmente, vamos reescrever a igualdade 2.12 da seguinte forma:

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\binom{n}{4}-\binom{n}{5}+\cdots=0. \tag{2.13}$$

É importante observar que esta soma não é infinita. Seu último termo é $\binom{n}{n}$ precedido do sinal de mais ou de menos, de acordo com a paridade de n. Esta paridade não foi pré-estabelecida, pois queremos provar o caso geral.

Utilizando a relação de Stifel, escrevemos

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\binom{n}{4}-\binom{n}{5}+\cdots =$$

$$\binom{n-1}{0}-\left[\binom{n-1}{0}+\binom{n-1}{1}\right]+\left[\binom{n-1}{1}+\binom{n-1}{2}\right]-\ldots =$$

$$\binom{n-1}{0}-\binom{n-1}{0}-\binom{n-1}{1}+\binom{n-1}{1}+\binom{n-1}{2}-\ldots = 0$$

Concluindo, assim, a prova do teorema 2.9.

□

Assim, como no teorema das linhas, podemos demonstrar o teorema das linhas alternadas utilizando a igualdade

$$\binom{n}{0}x^n+\binom{n}{1}x^{n-1}+\binom{n}{2}x^{n-2}+\ldots+\binom{n}{n-1}x+\binom{n}{n}=(1+x)^n.$$

Neste caso, fazemos $x=-1$ e obtemos

$$\binom{n}{0}\cdot(-1)^n+\binom{n}{1}\cdot(-1)^{n-1}+\binom{n}{2}\cdot(-1)^{n-2}+\ldots+\binom{n}{n-1}\cdot(-1)+\binom{n}{n}=(1-1)^n$$

$$\Longrightarrow \quad \binom{n}{0}\cdot(-1)^n+\binom{n}{1}\cdot(-1)^{n-1}+\binom{n}{2}\cdot(-1)^{n-2}+\ldots+\binom{n}{n-1}\cdot(-1)+\binom{n}{n}=0.$$

Aqui, precisamos considerar a paridade de n. Para n par, temos

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\binom{n}{4}-\binom{n}{5}+\ldots-\binom{n}{n-1}+\binom{n}{n}=0$$

$$\Longrightarrow \quad \binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\ldots+\binom{n}{n}=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\ldots+\binom{n}{n-1}.$$

Analogamente, para n ímpar, temos

$$-\binom{n}{0}+\binom{n}{1}-\binom{n}{2}+\binom{n}{3}-\binom{n}{4}+\binom{n}{5}-\ldots+\binom{n}{n-1}-\binom{n}{n}=0$$

$$\Longrightarrow \quad \binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\ldots+\binom{n}{n-1}=\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\ldots+\binom{n}{n}$$

$$\Longrightarrow \quad \binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\ldots+\binom{n}{n}=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\ldots+\binom{n}{n-1}.$$

Mostrando, mais uma vez, que é a válida a igualdade 2.12.

Além das identidades apresentadas até agora, referentes ao triângulo aritmético, iremos mostrar mais duas identidades envolvendo os coeficientes binomiais, uma sendo consequência direta da outra.

Proposição 2.10 (Identidade de Euler-Vandermonde) Para todos os inteiros não negativos m, n e k, é verdadeira a igualdade

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k} \tag{2.14}$$

Prova. Se k é simultaneamente maior que m e n, nada temos a provar. Consideremos, neste caso, e sem perda de generalidade que $k \leq m$. Pela definição de coeficiente binomial, o número $\binom{m+n}{k}$ é o coeficiente de x^k no polinômio $(1+x)^{m+n}$. Por outro lado, este polinômio é equivalente a $(1+x)^m(1+x)^n$. Desenvolvendo cada uma dos fatores e efetuando o produto dos termos obtidos, temos

$$\begin{aligned}
(1+x)^{m+n} &= \left[\binom{m}{0}x^0 + \binom{m}{1}x^1 + \ldots + \binom{m}{k}x^k + \ldots + \binom{m}{m}x^m\right] \\
&\cdot \left[\binom{n}{0}x^0 + \binom{n}{1}x^1 + \ldots + \binom{n}{k}x^k + \ldots + \binom{n}{n}x^n\right] \\
&= \binom{m}{0}\binom{n}{0}x^0 + \binom{m}{0}\binom{n}{1}x^1 + \ldots + \binom{m}{0}\binom{n}{k}x^k \ldots + \binom{m}{0}\binom{n}{n}x^n \\
&+ \binom{m}{1}\binom{n}{0}x^1 + \binom{m}{1}\binom{n}{1}x^2 + \ldots \binom{m}{1}\binom{n}{k-1}x^k + \ldots + \binom{m}{1}\binom{n}{n}x^{n+1} \\
&+ \binom{m}{k}\binom{n}{0}x^k + \ldots + \binom{m}{m}\binom{n}{0}x^m + \binom{m}{m}\binom{n}{1}x^{m+1} + \ldots + \binom{m}{m}\binom{n}{n}x^{m+n}.
\end{aligned}$$

Com o produto acima, fica fácil perceber que o coeficiente de x^k no polinômio $(1+x)^{m+n}$ é dado pela soma

$$\binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{n}{k-1} + \ldots + \binom{m}{k}\binom{n}{0} = \sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}.$$

O que conclui a prova da Identidade de Euler para coeficientes binomiais.

□

No caso em que $m = n = k$, obtemos uma igualdade conhecida como identidade de Lagrange[7], a qual enunciaremos a seguir.

[7] Lagrange, Joseph Louis (1736-1813), matemático italiano.

Corolário 2.11 (Identidade de Lagrange) Para todo k inteiro não negativo, vale

$$\sum_{i=0}^{k}\binom{k}{i}^2=\binom{2k}{k} \tag{2.15}$$

Prova. Conclui-se imediatamente do teorema 2.5 e da proposição 2.10, pois

$$\sum_{i=0}^{k}\binom{k}{i}^2=\sum_{i=0}^{k}\binom{k}{i}\binom{k}{i}=\sum_{i=0}^{k}\binom{k}{i}\binom{k}{k-i}=\binom{2k}{k}.$$

□

Exemplo 2.12 (Brasil Preparação Cone Sul-2002) Para cada inteiro positivo n, seja $a_n=\binom{2n}{n}$, mostre que o número binomial a_n é sempre par.

Solução. Este exemplo poderia ser resolvido facilmente aplicando a identidade de Lagrange, porém, seria necessário a utilização de um resultado referente à divisibilidade de coeficientes binomiais que será apresentado somente no capítulo 4. Faremos a resolução utilizando a fórmula 2.4.

$$\begin{aligned}\binom{2n}{n} &= \frac{2n(2n-1)\cdots(2n-n+2)(2n-n+1)}{1\cdot 2\cdots(n-1)n}\\ &= \frac{2n[(2n-1)\cdots(2n-(n-1)+1)](n+1)}{1\cdot 2\cdots(n-1)n}\\ &= 2(n+1)\binom{2n-1}{n-1}.\end{aligned}$$

Logo, $\binom{2n}{n}$ é múltiplo de 2.

Aqui concluímos o capítulo 2, cujo objetivo foi apresentar a definição de números binomiais, mostrar algumas de suas propriedades dentro do triângulo aritmético ou de Pascal e algumas outras aplicações. No decorrer do trabalho, serão úteis os conceitos aqui apresentados.

3 DIVISIBILIDADE E CONGRUÊNCIAS

Neste capítulo, buscamos definir as relações de divisibilidade e congruência no conjunto dos números inteiros, fornecendo alguns exemplos e enunciando as propriedades fundamentais para o entendimento do que segue nos capítulos posteriores. A consistência dos conceitos apresentados assegura-se na pesquisa bibliográfica em clássicos da Teoria dos Números como (LANDAU, 2002) e (ALENCAR FILHO, 1981) e grandes autores contemporâneos como (HEFEZ, 2013) e (CAMINHA, 2012), os quais indicamos para um estudo aprofundado sobre o assunto.

3.1 Divisibilidade

Definição 3.1 Dados a e b números inteiros, dizemos que $a \mid b$, se existir $c \in \mathbb{Z}$, tal que $b = ac$. Se $a \mid b$, diz-se também que a é um divisor ou fator de b, que b é múltiplo de a, ou que b é divisível por a. Se a não divide b, então escrevemos $a \nmid b$.

Exemplo 3.2 Pela definição dada acima, podemos escrever

(a) $2 \mid 6$, pois $6 = 2 \cdot 3$.

(b) $3 \nmid 5$, pois não existe $c \in \mathbb{Z}$ tal que $3 \cdot b = 5$.

(c) $-5 \mid 20$, pois $20 = (-5)(-4)$.

Enunciaremos a seguir algumas propriedades acerca da relação de divisibilidade entre dois inteiros.

Proposição 3.3 Sejam $a, b, c, d \in \mathbb{Z}$ tem-se:

(a) $a \mid 0, \quad 1 \mid a \quad$ e $\quad a \mid a.$

(b) $0 \mid a, \quad$ se, e somente se, $\quad a = 0.$

(c) se $\quad a \mid b \quad$ e $\quad c \mid d, \quad$ então $\quad ac \mid bd.$

(d) se $\quad a \mid b \quad$ e $\quad b \mid c\,, \quad$ então $\quad a \mid c.$

(e) se $\quad a \mid b \quad$ e $\quad b \mid a, \quad$ com $\quad a, b \neq 0, \quad$ então $\quad a = \pm b.$

(f) se $\quad a \mid b \quad$ com $\quad b \neq 0, \quad$ então $\quad |a| \leq |b|.$

(g) se $\quad a \mid (b \pm c), \quad$ então $\quad a \mid b \Longleftrightarrow a \mid c.$

(h) se $\quad a \mid b \quad$ e $\quad a \mid c, \quad$ então $\quad a \mid (bx + cy), \quad \forall\, x, y \in \mathbb{Z}.$

Prova.

(a) Com efeito,

$$0 = a \cdot 0, \quad a = 1 \cdot a \quad \text{e} \quad a = a \cdot 1.$$

(b) Supondo que $0 \mid a$, pela definição 3.1 existe $c \in \mathbb{Z}$ tal que $0 \cdot c = a$, de onde concluímos que $a = 0$.

A recíproca é também válida, pois $0 \mid 0$, como mostramos no item anterior.

(c) Como $a \mid b$ e $c \mid d$, existem inteiros k_1 e k_2 de modo que $b = a \cdot k_1$ e $d = c \cdot k_2$, então

$$b \cdot d = a \cdot k_1 \cdot c \cdot k_2 = (ac)(k_1 k_2) \qquad \Longrightarrow \qquad ac \mid bd.$$

(d) Se $a \mid b$ e $b \mid c$, existem q_1 e $q_2 \in \mathbb{Z}$ tais que $b = a \cdot q_1$ e $c = b \cdot q_2$. Daí concluímos que

$$c = a \cdot q_1 \cdot q_2 = a \cdot (q_1 q_2) \qquad \Longrightarrow \qquad a \mid c.$$

(e) De fato, $a \mid b$ e $b \mid a$ implica na existência de inteiros t_1 e t_2 de modo que $b = a \cdot t_1$ e $a = b \cdot t_2$. Como $a, b \neq 0$, podemos escrever

$$b = t_1 \cdot t_2 \cdot b \qquad \Longrightarrow \qquad t_1 \cdot t_2 = 1.$$

Como $t_1, t_2 \in \mathbb{Z}$, temos

$$t_1 = t_2 = \pm 1 \qquad \Longrightarrow \qquad a = \pm b.$$

(f) Se $a \mid b$, existe $c \in \mathbb{Z}$ de modo que $b = a \cdot c$. Tomando esta igualdade em módulo, e sabendo que o módulo do produto é igual ao produto dos módulos, temos

$$|b| = |a \cdot c| = |a| \cdot |c|.$$

A condição $b \neq 0$ garante que $|c| \geq 1$, e então

$$|b| = |a| \cdot |c| \geq |a| \qquad \Longrightarrow \qquad |a| \leq |b|.$$

(g) Supondo que $a \mid (b + c)$, então existe $f \in \mathbb{Z}$ tal que $b + c = fa$. Da mesma forma, se $a \mid b$, existe $g \in \mathbb{Z}$ tal que $b = ga$. Assim temos

$$b + c = fa \quad \Longrightarrow \quad ga + c = fa \quad \Longrightarrow \quad c = (f - g)a \quad \Longrightarrow \quad a \mid c.$$

Se $a \mid (b-c)$ e $a \mid b$, pelo que provamos anteriormente, $a \mid -c$, o que implica $a \mid c$.
A prova da implicação contrária se faz de modo totalmente análogo.

(h) Sejam $b = a \cdot d_1$ e $c = a \cdot d_2$, com $d_1, d_2 \in \mathbb{Z}$. Notemos que d_1 e d_2 existem, pois $a \mid b$ e $a \mid c$. Então, quaisquer que sejam os inteiros x e y, podemos escrever

$$(bx+cy) = (ad_1x + ad_2y) = a(d_1x + d_2y) \qquad \Longrightarrow \qquad a \mid (bx+cy).$$

□

Ainda sobre o item (h) da proposição 3.3, temos a seguinte e óbvia generalização
Se $a \mid b_k$, com $k = 1,2,3,\ldots,n$, então

$$a \mid (b_1x_1 + b_2x_2 + b_3x_3 + \cdot + b_nx_n),$$

quaisquer que sejam $x_1, x_2, x_3, \ldots, x_n \in \mathbb{Z}$.

Proposição 3.4 Dados a, b inteiros e k natural, então
(a) $(a-b) \mid (a^k - b^k)$.
(b) se k for ímpar, $(a+b) \mid (a^k + b^k)$.

Prova.
(a) Para provarmos este item, mostraremos que é válida a igualdade

$$(a^k - b^k) = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}).$$

De fato, desenvolvendo o produto do lado esquerdo da igualdade, como veremos a seguir, obtemos o resultado desejado.

$$\begin{gathered}(a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}) = \\ = a[(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1})] \\ -b[(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1})] \\ = (a^k + a^{k-1}b + a^{k-2}b^2 + \ldots + a^2b^{k-2} + ab^{k-1}) \\ -(a^{k-1}b + a^{k-2}b^2 + a^{k-3}b^3 + \ldots + ab^{k-1} + b^k) = (a^k - b^k).\end{gathered}$$

Como $k \in \mathbb{N}$, $(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1})$ é inteiro, o que nos garante que

$$(a-b) \mid (a^k - b^k).$$

(b) Aqui, mostraremos a validez da igualdade

$$(a^k + b^k) = (a+b)(a^{k-1} - a^{k-2}b + a^{k-3}b^2 - \ldots - ab^{k-2} + b^{k-1}),$$

efetuando o produto do segundo membro e observando que a alternância dos sinais dentro do parêntese se adéqua ao fato de k ser ímpar.

$$\begin{aligned}
&(a+b)(a^{k-1} - a^{k-2}b + a^{k-3}b^2 - \ldots - ab^{k-2} + b^{k-1}) = \\
&= a[(a^{k-1} - a^{k-2}b + a^{k-3}b^2 - \ldots - ab^{k-2} + b^{k-1})] \\
&+b[(a^{k-1} - a^{k-2}b + a^{k-3}b^2 - \ldots - ab^{k-2} + b^{k-1})] \\
&= (a^k - a^{k-1}b + a^{k-2}b^2 - \ldots - a^2b^{k-2} + ab^{k-1}) \\
&+(a^{k-1}b - a^{k-2}b^2 + a^{k-3}b^3 - \ldots - ab^{k-1} + b^k) = (a^k + b^k).
\end{aligned}$$

O que mostra que $(a+b) \mid (a^k + b^k)$, com k ímpar, e conclui a prova desta proposição.

□

Mesmo quando um número inteiro a não é divisível por um número inteiro $b \neq 0$, é possível efetuar a divisão de a por b, havendo, neste caso, um resto não nulo. Este resultado foi proposto por Euclides nos seu Elementos, há 300 anos antes de Cristo, e é hoje um dos resultados mais importantes da Teoria dos Números.

Teorema 3.5 (Divisão Euclidiana) Se a e b são números inteiros, com $b \neq 0$, então existem e são únicos os números inteiros q e r tais que

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

Prova. Consideremos o conjunto $X = \{a - bt / t \in \mathbb{Z}\} \cap \mathbb{N}$. O conjunto X é não vazio, pois tomando $t_0 = -b|a|$ segue que

$$a - bt_0 = a - b(-b|a|) = a + b^2|a| \geq a + |a| \geq 0 \quad \Longrightarrow \quad a - bt_0 \in X.$$

Como $a - bt \geq 0$, o princípio da boa ordenação garante que X possui elemento mínimo. Seja $r \in X$ o tal elemento mínimo. Assim, existe um único $q \in \mathbb{Z}$ tal que $r = a - bq$ isto é, $a = bq + r$, com $0 \leq r$. Para mostrar que $r \leq |b|$, basta notar que para $t_1 = q + \frac{|b|}{b}$, temos

$$r_1 := a - bt_1 = a - b\left(q + \frac{|b|}{b}\right) = r - |b|.$$

Desta forma, $r_1 < r$ e da minimalidade de r segue que $r_1 \in X$, o que implica $r_1 < 0$, ou seja $r < |b|$.

Por fim, para qualquer elemento $s = a - bt \in X$, com $s \neq r$, temos $s > r$, de onde segue que

$$s - r = |s - r| = |b(q - t)| = |b||q - t| \quad \Longrightarrow \quad s = r + |b||q - t| \quad \Longrightarrow \quad s \geq |b|.$$

Logo, o elemento mínimo de X é caracterizado pelas condições $r = a - bq$ e $0 \leq r < |b|$. Fica, portanto estabelecida a unicidade de r e, a fortiori, a de q.

□

Os inteiros q e r assim determinados são, respectivamente, o quociente e o resto da divisão de a por b.

Não dedicaremos neste trabalho um capítulo ou seção específica para tratar das propriedades do *mdc* e dos números primos, para o que recomendamos as referências já citadas no início deste capítulo. Porém, antes de finalizar esta seção, citaremos um teorema importante sobre divisibilidade envolvendo números primos, o Lema de Euclides. este resultado no será útil no capítulo que trata da divisibilidade de coeficientes binomiais.

Para tal, lembremos que um número inteiro positivo é dito primo quando seus únicos divisores positivos são 1 e ele próprio e que o *mdc* de um conjunto de números inteiros não nulos é o maior divisor comum entre eles.

Na demonstração a seguir, faremos uso do teorema de Bézout [1], cuja demonstração nos absteremos de desenvolver e sugerimos a referência (CAMINHA, 2012), páginas 14 e 15.

Proposição 3.6 (Lema de Euclides). Sejam a, b, $p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Prova. Se $p \mid ab$, então existe $q \in \mathbb{Z}$ tal que $pq = ab$. Caso $p \mid a$, nada temos a mostrar. Usemos, então, como hipótese que $p \nmid a$. Neste caso, como p é primo, $mdc\,(a, p) = 1$, e pelo teorema de Bézout, existem m e n, inteiros tais que

$$ma + np = 1. \tag{3.1}$$

Multiplicando por b ambos os membros da igualdade 3.1, temos

$$mab + npb = b \quad \Longrightarrow \quad mpq + npb = b \quad \Longrightarrow \quad p(mq + nb) = b \quad \Longrightarrow \quad p \mid b.$$

[1] Bézout, Etienne (1730 - 1783), matemático francês.

Como queríamos mostrar.

□

3.2 Congruências

Uma das descobertas mais importantes de Gauss foi a aritmética modular, apresentada em seu livro *Disquisitiones Arithmeticae* (1801), e usada nessa importante obra como base para ideias mais profundas. Nesse livro, Gauss conduziu a teoria dos números para o centro do palco matemático (STEWART, 2014), trazendo ideias inovadoras como o tema desta seção e sistematizando as descobertas de seus predecessores.

Definição 3.7 Sejam a, b e m números inteiros, com $m > 1$, dizemos que a é congruente a b módulo m e escrevemos $a \equiv b \pmod{m}$, se a e b deixam o mesmo resto na divisão euclidiana por m, ou ainda se $m \mid (a-b)$. Caso a e b deixem restos diferentes na divisão euclidiana por m, ou seja, $m \nmid (a-b)$, então a não é congruente a b módulo m e escrevemos $a \not\equiv b \pmod{m}$.

Exemplo 3.8 De acordo com a definição 3.6, podemos escrever:

(a) $8 \equiv 5 \pmod{3}$, pois $3 \mid (8-5)$.

(b) $12 \equiv -2 \pmod{7}$, pois $7 \mid (12-(-2))$.

(c) $-4 \not\equiv 16 \pmod{6}$, pois $6 \nmid (-4-16)$.

Decorre, ainda, da definição de congruência que, se r é o resto na divisão euclidiana do número inteiro a pelo número natural m, então $a \equiv r \pmod{m}$, pois $m \mid (a-r)$. Desta forma, a é congruente módulo m a algum dos $\{0,1,2,\ldots,m-2,m-1\}$, que são os restos possíveis na divisão de a por m.

Exemplo 3.9 Se $n \in \mathbb{Z}$, então $n^2 \equiv 0 \pmod{4}$ ou $n^2 \equiv 1 \pmod{4}$.

Solução. Se n é par, então n é da forma $2k$ para algum $k \in \mathbb{Z}$. Assim,

$$n^2 = 4k^2 \quad \Longrightarrow \quad 4 \mid n^2 \quad \Longrightarrow \quad n^2 \equiv 0 \pmod{4}.$$

Se n é ímpar, então n é da forma $2k+1$ para algum $k \in \mathbb{Z}$. Desta forma,

$$n^2 = 4(k^2+k)+1 \quad \Longrightarrow \quad 4 \mid (n^2-1) \quad \Longrightarrow \quad n^2 \equiv 1 \pmod{4}.$$

Portanto, $\forall n \in \mathbb{Z}$, os únicos restos possíveis na divisão euclidiana de n^2 por 4 são 0 e 1.

Exemplo 3.10 Se $n \in \mathbb{Z}$ não é múltiplo de 3, então $n^2 \equiv 1\,(mod\,3)$.

Solução. Se n não é múltiplo de 3, então n é da forma $3k+1$ ou $3k+2$, para algum k inteiro. Elevando n ao quadrado, temos

$$n^2 = (3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1 \quad \Longrightarrow \quad n^2 \equiv 1\,(mod\,3)$$

Ou ainda,

$$n^2 = (3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1 \quad \Longrightarrow \quad n^2 \equiv 1\,(mod\,3).$$

Desta forma, se n não é múltiplo de 3, n^2 deixa resto 1 na divisão por 3, como desejávamos mostrar.

Vejamos a seguir algumas propriedades básicas acerca das congruências.

Proposição 3.11 Dados os números inteiros a, b, c e m, com $m > 1$, tem-se:

(a) (Reflexividade) $a \equiv a$ (mod m).

(b) (Simetria) Se $a \equiv b$ (mod m), então $b \equiv a$ (mod m).

(c) (Transitividade) Se $a \equiv b$ (mod m) e $b \equiv c$ (mod m), então $a \equiv c$ (mod m).

Prova.

(a) Basta vermos que

$$m \mid 0 \qquad \Longrightarrow \qquad m \mid (a-a) \qquad \Longrightarrow \qquad a \equiv a \text{ (mod m)}.$$

(b) Pela definição 3.6, se $a \equiv b$ (mod m), então $m \mid (b-a)$. Desta forma, valem as equivalências

$$m \mid (b-a) \quad \Longrightarrow \quad m \mid -(b-a) = (a-b) \quad \Longrightarrow \quad b \equiv a \text{ (mod m)}.$$

(c) Se $a \equiv b$ (mod m) e $b \equiv c$ (mod m), então $m \mid (b-a)$ e $m \mid (c-b)$. Utilizando o caso particular $x = y = 1$ da proposição 3.3 (g), escrevemos

$$m \mid (b-a) \quad \text{e} \quad m \mid (c-b) \quad \Longrightarrow \quad m \mid (b-a)+(c-b) = (c-a) \quad \Longrightarrow \quad a \equiv c \text{ (mod m)}.$$

Valem, portando, a reflexividade, a simetria e a transitividade na congruência entre dois inteiros.

□

Com a prova da proposição 3.11, concluímos que a congruência é uma relação de equivalência em $\mathbb{Z}$.

Proposição 3.12 Sejam m e n inteiros positivos e sejam a, b, c, d, inteiros quaisquer. São válidas as seguintes asserções:

(a) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+c \equiv b+d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

(b) Se $a \equiv b \pmod{m}$, então $a+c \equiv b+c \pmod{m}$ e $ac \equiv bc \pmod{m}$.

(c) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.

(d) Se $ac \equiv bc \pmod{m}$ e se o $mdc(c,m) = d$, então $a \equiv b \pmod{\frac{m}{d}}$. Em particular, se $mdc(c,m) = 1$, então $a \equiv b \pmod{m}$.

Prova.

(a) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m \mid (b-a)$ e $m \mid (d-c)$. Assim, pela propriedade 3.3 (g), podemos escrever

$$m \mid (b-a)+(d-c) \quad \Longrightarrow \quad m \mid (b+d)-(a+c) \quad \Longrightarrow \quad a+c \equiv b+d \,(\text{mod } m).$$

Ainda pela proposição 3.3 (g), fazendo $x = c$ e $y = b$, obtemos

$$m \mid (b-a)c+(d-c)b = bc-ac+bd-bc = bd-ac \quad \Longrightarrow \quad ac \equiv bd \,(\text{mod m}).$$

(b) Da mesma forma que no item anterior, se $a \equiv b \pmod{m}$, então

$$m \mid (b-a) = (b-a)+c-c = (b+c)-(a+c) \quad \Longrightarrow \quad a+c \equiv b+c \,(\text{mod } m).$$

Como $m \mid (b-a)$, podemos também escrever

$$m \mid (b-a)c = bc-ac \quad \Longrightarrow \quad ac \equiv bc \,(\text{mod } m).$$

(c) Vimos na proposição 3.4 (a) que $(a-b) \mid (a^k-b^k)$, $\forall\, k \in \mathbb{N}$, e obviamente, $(b-a) \mid (b^k-a^k)$, $\forall\, k \in \mathbb{N}$. Fazendo $k = n$, utilizando a transitividade da relação de divisibilidade provada na proposição 3.3 (d) e o fato de que $a \equiv b \pmod{m}$, temos

$$m \mid (b-a) \quad \text{e} \quad (b-a) \mid (b^n-a^n) \quad \Longrightarrow \quad m \mid (b^n-a^n) \quad \Longrightarrow \quad a^n \equiv b^n \,(\text{mod m}).$$

(d) Se $ac \equiv bc \pmod{m}$, então

$$m \mid bc-ac \quad \Longrightarrow \quad m \mid c(b-a).$$

Como $d = mdc(c,m)$, existem inteiros positivos c' e m' tais que

$$c = c'd \quad \text{e} \quad m = m'd \quad \text{com} \quad mdc(c',m') = 1.$$

Substituímos as relações acima em $m \mid c(b-a)$ e concluímos que

$$m'd \mid c'd(b-a) \quad \Longrightarrow \quad m' \mid c'(b-a).$$

O fato de c' e m' serem primos entre si conclui a nossa prova, ou seja

$$m' \nmid c' \quad \Longrightarrow \quad m' \mid (b-a) \quad \Longrightarrow \quad a \equiv b (\text{mod m'}) \quad \Longrightarrow \quad a \equiv b \left(mod \frac{m}{d}\right).$$

Em particular, se $d = mdc(c,m) = 1$, então $\frac{m}{d} = m$ e temos $a \equiv b \pmod{m}$.

□

Exemplo 3.13 Vamos encontrar o resto da divisão de 3^{1000} por 101.

Solução. Desejamos encontrar um número natural x tal que $3^{1000} \equiv x\,(mod 101)$. Começaremos com potências de 3 menores e utilizaremos sucessivas vezes a proposição 3.10, itens (a) e (c) a fim de chegar a 3^{1000}. Ou seja,

$$3^4 \equiv -20 (\text{mod } 101) \quad \Longrightarrow \quad (3^4)^2 \equiv (-20)^2 (\text{mod } 101) \quad \Longrightarrow \quad 3^8 \equiv -4 (\text{mod } 101);$$
$$3^4 \equiv -20 (\text{mod } 101) \quad \Longrightarrow \quad (3^4)^5 \equiv (-20)^5 (\text{mod } 101) \quad \Longrightarrow \quad 3^{20} \equiv -17 (\text{mod } 101);$$
$$3^{20} \equiv -17 (\text{mod } 101) \quad \Longrightarrow \quad (3^{20})^4 \equiv (-17)^4 (\text{mod } 101) \quad \Longrightarrow \quad 3^{80} \equiv -6 (\text{mod } 101);$$
$$3^{100} \equiv 102 (\text{mod } 101) \quad \Longrightarrow \quad 3^{100} \equiv 1 (\text{mod } 101) \quad \Longrightarrow \quad 3^{1000} \equiv 1 (\text{mod } 101).$$

Portanto, o resto da divisão de 3^{1000} por 101 é igual a 1.

A solução deste exemplo é óbvia se utilizarmos o Pequeno Teorema de Fermat[2], segundo o qual

$$a^{p-1} \equiv 1\,(mod\, p)$$

com p primo, a inteiro e $mdc(a,p) = 1$, já que 101 é um número primo, e $mdc\,(3,101) = 1$. Bastaria observarmos que

$$3^{1000} = (3^{101-1})^{10} \equiv 1^{10} \equiv 1\,(mod\, 101).$$

No entanto, optamos por mostrar a possibilidade de resolvê-lo utilizando apenas os resultados provados nesta seção. Não apresentaremos aqui a demostração deste importante teorema, bem como de outros resultados importantes da Teoria dos Números a fim de nos limitarmos aos conhecimentos estritamente necessários à compreensão do capítulo que segue.

---

[2] Pierre de Fermat, magistrado, matemático e cientista francês (1601-1665)

3.3 Sistema completo de resíduos

Nesta seção, mostraremos um último aspecto da relação de congruência entre dois inteiros, o conjunto chamado sistema completo de resíduos.

Definição 3.14 Seja m um número inteiro, com $m > 1$. O conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de m números inteiros é dito um *sistema completo de resíduos (restos)* módulo m se um inteiro qualquer a é congruente módulo m a somente um elemento de S. Isto equivale também a dizer que os elementos de S são dois a dois incongruentes módulo m.

Por exemplo, o conjunto $\{-1, 0, 1\}$ é um sistema completo de resíduos módulo 3. De fato, se a é um número inteiro, em relação à divisão euclidiana de a por 3, temos

$$a = 3q \qquad \text{ou} \qquad a = 3q' + 1 \qquad \text{ou} \qquad a = 3q'' + 2.$$

Pela definição de congruência, podemos escrever

$$\begin{aligned} a &= 3q \quad \Longrightarrow \quad 3 \mid (a-0) \quad \Longrightarrow \quad a \equiv 0 \,(mod\ 3) \\ a &= 3q' + 1 \quad \Longrightarrow \quad 3 \mid (a-1) \quad \Longrightarrow \quad a \equiv 1 \,(mod\ 3) \\ a &= 3q'' + 2 \quad \Longrightarrow \quad 3 \mid (a+1) \quad \Longrightarrow \quad a \equiv -1 \,(mod\ 3). \end{aligned}$$

Daí vemos claramente que o conjunto $\{0, 1, 2\}$ é também um sistema completo de resíduos módulo 3.

Proposição 3.15 O conjunto $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.

Prova. Sejam a, q, m, r números inteiros, com $0 \leq r < m$. Se $a = mq + r$, ou seja, se q e r são, respectivamente, o quociente e o resto da divisão euclidiana de a por m, então

$$mq = a - r \quad \Longrightarrow \quad m \mid (a-r) \quad \Longrightarrow \quad a \equiv r \,(mod\, m).$$

Como $0 \leq r < m$, então os possíveis valores para r são $0, 1, 2, \ldots, m-1$, que são exatamente os elementos de S. Portanto, um inteiro a qualquer será congruente módulo m a somente um dos elementos de S. Desta forma, pela definição 3.12, o conjunto $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.

□

Pela transitividade da relação de congruência, se um conjunto $\{r_1, r_2, \ldots, r_m\}$ de m inteiros é um sistema completo de resíduos módulo m, então cada elemento desse conjunto é congruentes a somente um dos inteiros $0, 1, 2, \ldots, m-1$.

Proposição 3.16 O conjunto $R = \left\{r \in \mathbb{Z}; -\frac{m}{2} \leq r < \frac{m}{2}\right\}$ é um sistema completo de resíduos módulo m.

Prova. Sejam r_i, $r_j \in R$, tais que $r_i < r_j$. Temos $0 < r_j - r_i < m$ e assim, $r_i \not\equiv r_j \,(mod\, m)$, ou seja, os elementos de R são dois a dois incongruentes módulo m. Devemos mostrar, então, que R tem m elementos. Vejamos que o extremo $\frac{m}{2} \notin R$, mas o extremo $-\frac{m}{2}$ pode ou não pertencer de acordo com a paridade de m.
Se m é par, $-\frac{m}{2} \in R$. Notemos que $\frac{m}{2}$ também é inteiro. Então, o número de elementos de R é dado por

$$\frac{m}{2} - \left(-\frac{m}{2}\right) = \frac{2m}{2} = m.$$

Se m é ímpar, $-\frac{m}{2} \notin R$, então nenhum dos dois extremos pertence a R. Neste caso, o menor valor de r é o inteiro imediatamente à direta de $-\frac{m}{2}$, que é $\frac{-m+1}{2}$. É conveniente também escrevermos o maior valor de r, que é $\frac{m-1}{2}$, para que o nosso resultado seja um número inteiro. Assim, o número de elementos de R é dado por.

$$\frac{m-1}{2} - \left(\frac{-m+1}{2}\right) + 1 = \frac{2m-2}{2} + 1 = m - 1 + 1 = m.$$

Em ambos os casos, R tem m elementos. Portanto, é um sistema completo de resíduos módulo m.

□

O conjunto que acabamos de analisar tem m inteiros consecutivos. Conjuntos com m inteiros consecutivos são sempre sistemas completos de resíduos módulo m. A proposição a seguir nos ajudará a compreender esse fato.

Proposição 3.17 Sejam a, c, m inteiros, com $m > 1$ e $mdc\,(c, m) = 1$. Se o conjunto $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m, então o conjunto $\{a + cr_1, a + cr_2, \ldots, a + cr_m\}$ é também um sistema completo de resíduos módulo m.

Prova. Dados $i, j \in \{1, 2, \ldots, m\}$, de acordo com a proposição 3.11, itens b e d, é verdade que

$$a + cr_i \equiv a + cr_j \,(mod\, m) \quad \Longrightarrow \quad cr_i \equiv cr_j \,(mod\, m) \quad \Longrightarrow \quad r_i \equiv r_j \,(mod\, m).$$

Como $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m,

$$r_i \equiv r_j \,(mod\, m) \quad \Longrightarrow \quad i = j.$$

Assim, dois elementos distintos do conjunto $\{a + cr_1, a + cr_2, \ldots, a + cr_m\}$ são incongruentes módulo m, o que significa que tal conjunto é um sistema completo de resíduos módulo m.

□

Com o resultado acima demonstrado, fica fácil perceber que um conjunto de m inteiros consecutivos é um sistema completo de resíduos módulo m, pois pode sempre ser escrito na forma

$$\{a, a+1, \ldots, a+m-1\},$$

configurando-se assim como um caso particular da proposição 3.15, para $c = 1$ e $\{r_1, r_2, \ldots, r_m\} = \{0, 1, \ldots, m-1\}$.

Existem muitas propriedades e aplicações sobre as relações de divisibilidade e congruência entre dois inteiros, as quais não comentaremos neste capítulo. No entanto, é suficiente o exposto para que possamos adentrar o capítulo central deste trabalho com entendimento e domínio das notações que serão utilizadas. No mais, abriremos parênteses ao logo do texto a fim de que se mostrem perfeitamente claras as ideias aqui apresentadas.

4 PROPRIEDADES ARITMÉTICAS DOS COEFICIENTES BINOMIAIS

O objetivo principal deste capítulo é mostrar aspectos da divisibilidade de coeficientes binomiais por números primos. Alguns dos resultados aqui apresentados já são conhecidos e estão contidos nas obras referenciadas ao longo deste trabalho. Buscamos, porém demostrá-los alternativamente, e de maneira simples ao entendimento, de modo que alunos do ensino médio com um razoável nível de conhecimentos possam compreendê-los. Por fim, discorreremos sobre a aritmética no triângulo de Pascal módulo p primo, uma aplicação muito interessante de todos os teoremas, lemas e corolários aqui expostos.

4.1 Congruências binomiais

Já sabemos que número primo é o inteiro positivo cujos únicos divisores positivos são 1 e ele mesmo. Sabemos também que o *mdc* entre dois inteiros é o maior divisor comum entre eles. Recordemos então que, números primos entre si, coprimos ou relativamente primos são aqueles que só têm como fator comum o número 1. Desta forma, se m e n são números inteiros primos entre si, temos $mdc\,(m,n) = 1$.

Teorema 4.1 Sejam m e n números inteiros relativamente primos, então $\binom{n}{m}$ é divisível por n.

Prova. No capítulo 2, teorema 2.4 (Fórmula para coeficientes binomiais), vimos que

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m}.$$

Assim, temos

$$\begin{aligned}
\binom{n}{m} &= \frac{n}{m}\cdot\frac{(n-1)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\
\Longrightarrow \quad \binom{n}{m} &= \frac{n}{m}\cdot\frac{(n-1)\cdots[(n-1)-(m-1)+1]}{1\cdot 2\cdots(m-1)} \\
\Longrightarrow \quad \binom{n}{m} &= \frac{n}{m}\cdot\binom{n-1}{m-1}.
\end{aligned}$$

Sabemos, pela definição de coeficientes binomiais, que $\binom{n-1}{m-1}$ é um número inteiro, digamos $\binom{n-1}{m-1} = k$. Então, escrevemos

$$\binom{n}{m} = \frac{n}{m}\cdot k \quad \Longrightarrow \quad \frac{m}{n}\cdot\binom{n}{m} = k.$$

Desta forma, n divide o produto $m \cdot \binom{n}{m}$, pois $k \in \mathbb{Z}$. Como n não tem fator comum com m, concluímos que n divide $\binom{n}{m}$, sendo válido o teorema 4.1.

□

Vejamos, por exemplo, que

$$\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126,$$

que é divisível por 9 e os números 9 e 4 são primos entre si. No lema a seguir, veremos um caso mais específico sobre essa relação de divisibilidade.

Corolário 4.2 Se p é um número primo e r um número inteiro, com $0 < r < p$, então $\binom{p}{r}$ é divisível por p.

Prova. Como p é primo e r é um número inteiro positivo menor que p, então r e p são relativamente primos. Segue imediatamente do teorema 4.1 a prova deste corolário.

□

De fato, no cálculo de $\binom{11}{8}$, por exemplo, podemos observar que nenhum dos fatores do denominador divide 11, pois são todos menores e primos com 11. O resultado é, portanto, múltiplo de 11.

$$\binom{11}{8} = \frac{11 \cdot 10 \cdots 4}{1 \cdot 2 \cdots 8} = 165.$$

O resultado apresentado a seguir embora não enuncie uma congruência binomial, utiliza-se das congruências mostradas anteriormente em sua demonstração e será importante para a prova de alguns teoremas posteriores.

Lema 4.3 O polinômio $(1+x)^p - (1+x^p)$ tem todos os seus coeficientes divisíveis por p (primo).

Prova. Desenvolvendo o binômio $(1+x)^p$ na expressão dada acima, encontramos

$$\begin{aligned}(1+x)^p-(1+x^p) &= \binom{p}{0}x^0+\binom{p}{1}x^1+\binom{p}{2}x^2\cdots+\binom{p}{p-1}x^{p-1}+\binom{p}{p}x^p-1-x^p\\ &= 1+\binom{p}{1}x+\binom{p}{2}x^2+\cdots+\binom{p}{p-1}x^{p-1}+x^p-1-x^p\\ &= \binom{p}{1}x+\binom{p}{2}x^2+\cdots+\binom{p}{p-1}x^{p-1}.\end{aligned}$$

Como $0<1,2,\ldots,p-1<p$, pelo corolário 4.2, os números $\binom{p}{1},\binom{p}{2},\ldots,\binom{p}{p-1}$ são todos divisíveis por p, ou seja, todos os coeficientes do polinômio $(1+x)^p-(1+x^p)$ são divisíveis por p.

□

A seguir, apresentaremos a prova do teorema mais importante desta seção. Desde o início do trabalho tratamos os números binomiais como coeficientes de polinômios conhecidos. Então, apresentaremos o detalhamento de uma prova constante na revista (TABACHNIKOV, 1999), que se utiliza além de um polinômio particular, dos conceitos de divisibilidade vistos na capítulo 3, e dos lemas e teoremas provados no capítulo em curso.

Teorema 4.4 Seja p um número primo e sejam m, n números inteiros não negativos. Se $m=kp+s$ e $n=lp+t$, onde k,l,s,t são inteiros com $0\leq s<p$ e $0\leq t<p$. Então,

$$\binom{n}{m}\equiv\binom{l}{k}\cdot\binom{t}{s}(mod\,p). \tag{4.1}$$

Prova. Para o nosso objetivo, olharemos com atenção algumas particularidades do polinômio

$$P(x)=(1+x)^{lp+t}-(1+x)^t(1+x^p)^l.$$

Afirmamos que este polinômio tem todos os seus coeficientes divisíveis por p. De fato, utilizando propriedades simples das potenciações e a proposição 3.4 (a), podemos escrever

$$\begin{aligned}P(x) &= (1+x)^t(1+x)^{pl}-(1+x)^t(1+x^p)^l\\ &= (1+x)^t[(1+x)^{pl}-(1+x^p)^l]\\ &= (1+x)^t[((1+x)^p)^l-((1+x^p)^l]\\ &= (1+x)^t[(1+x)^p-(1+x^p)]\cdot[(1+x)^{p(l-1)}+\cdots+(1+x^p)^{l-1}].\end{aligned}$$

Ou seja, decompomos $P(x)$ em três fatores, dos quais o segundo é um polinômio de coeficientes divisíveis por p (lema 4.3). Desta forma, podemos garantir que todos os coeficientes em $P(x)$ são divisíveis por p. Basta recordarmos que

$$(1+x)^p-(1+x^p)=\binom{p}{1}x+\binom{p}{2}x^2+\cdots+\binom{p}{p-1}x^{p-1}.$$

Onde $\binom{p}{1},\binom{p}{2},\ldots,\binom{p}{p-1}$ são todos divisíveis por p. Assim, podemos escrever

$$(1+x)^p-(1+x^p)=p\cdot F(x)$$

e fazendo

$$H(x)=(1+x)^t\cdot[(1+x)^{p(l-1)}+\cdots+(1+x^p)^{l-1}],$$

temos que $P(x)$ é um produto de polinômios cujos coeficientes são todos múltiplos de p, pois

$$P(x)=p\cdot F(x)\cdot H(x),$$

o que valida nossa afirmação.

A definição 2.1 nos diz que $\binom{n}{m}=\binom{lp+t}{kp+s}$ é o coeficiente de x^{kp+s} em $(1+x)^{lp+t}$, que é parte do polinômio $P(x)$. Vamos, então, observar o que acontece ao efetuarmos o produto $(1+x)^t(1+x^p)^l$, que é a outra parte. Façamos

$$\begin{aligned}
(1+x)^t(1+x^p)^l &= \left[1+\binom{t}{1}x+\binom{t}{2}x^2+\cdots+x^t\right]\cdot\left[1+\binom{l}{1}x^p+\binom{l}{2}x^{2p}+\cdots+x^{lp}\right]\\
&= 1+\binom{t}{1}x+\binom{t}{2}x^2+\cdots+x^t+\\
&+ \binom{l}{1}x^p+\binom{l}{1}\binom{t}{1}x^{p+1}+\binom{l}{1}\binom{t}{2}x^{p+2}+\cdots+\binom{l}{1}x^{p+t}+\\
&+ \binom{l}{2}x^{2p}+\binom{l}{2}\binom{t}{1}x^{2p+1}+\binom{l}{2}\binom{t}{2}x^{2p+2}+\cdots+\binom{l}{2}x^{2p+t}+\\
&+ \cdots\quad+x^{lp}+\binom{t}{1}x^{lp+1}+\binom{t}{2}x^{lp+2}+\cdots+x^{lp+t}.
\end{aligned}$$

Uma vez que $t<p$, cada um dos $1,\ldots,t,p,\ldots,p+t,2p,\ldots,2p+t,\ldots,lp,\ldots,lp+t$ são diferentes entre si, ou seja, cada potência de x é única. Desta forma, o coeficiente de x^{kp+s}

nesse produto é $\binom{l}{k}\binom{t}{s}$, como podemos ver no desenvolvimento acima. Em particular, se $s > t$, este coeficiente é nulo.

Pelo exposto, o coeficiente de x^{kp+s} em $P(x) = (1+x)^{lp+t} - (1+x)^t(1+x^p)^l$ é igual $\binom{lp+t}{kp+s} - \binom{l}{k}\binom{t}{s}$. E como cada coeficiente em $P(x)$ é divisível por p, temos

$$p \mid \left[\binom{lp+t}{kp+s} - \binom{l}{k}\binom{t}{s}\right] \quad \Longrightarrow \quad \binom{lp+t}{kp+s} \equiv \binom{l}{k}\binom{t}{s} \,(mod\, p).$$

□

Exemplo 4.5 Mostrar que $\binom{1134}{32}$ deixa resto 0 na divisão por 3.

Solução. Com certeza calcular $\binom{1134}{32}$ e depois efetuar a divisão por 3 não é o melhor caminho, pois os cálculos seriam muito extensos. Vamos, então utilizar o teorema 4.4. Dividindo 1134 e 32 por 3, temos

$$1134 = 378 \cdot 3 + 0 \qquad \text{e} \qquad 32 = 10 \cdot 3 + 2$$

Assim

$$\binom{1134}{32} \equiv \binom{378}{10}\binom{0}{2} (mod\ 3) \quad \Longrightarrow \quad \binom{1134}{32} \equiv 0\,(mod\ 3),$$

pois $\binom{0}{2}$ é igual a zero por definição. Portanto, $\binom{1134}{32}$ deixa resto 0 na divisão por 3.

No exemplo a seguir, faremos uso da notação $\lfloor x \rfloor$, que representa o piso ou parte inteira de $x \in \mathbb{R}$. Definimos $\lfloor x \rfloor$ como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k+1$.

Exemplo 4.6 Dados n, um número inteiro não negativo e p, um número primo, com $n \geq p$, mostrar que

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \,(mod\, p).$$

Solução. Como p é um número primo, e $n \geq p$, é suficiente efetuarmos a divisão de n por p e

aplicarmos o teorema 4.4. Ou seja,

$$\begin{aligned} \binom{n}{p} &= \binom{p\cdot t+r}{p\cdot 1+0} \equiv \binom{t}{1}\binom{r}{0} (mod\, p) \\ \Longrightarrow \quad \binom{n}{p} &\equiv t\,(mod\, p) \\ \Longrightarrow \quad \binom{n}{p} &\equiv \left\lfloor \frac{n}{p} \right\rfloor (mod\, p), \end{aligned}$$

pois t é a parte inteira da divisão de n por p.

Em alguns casos, é necessário aplicarmos o teorema 4.4 diversas vezes até encontrarmos o resto da divisão de um coeficiente binomial por um número p primo. Para resolvermos com mais agilidade esses e outros tipos de problemas, podemos utilizar o Teorema de Lucas[1], enunciado na seção a seguir.

4.2 Teorema de Lucas

Édouard Lucas foi um matemático francês que deu importantes contribuições no campo da Teoria dos Números e da Matemática recreativa. Apresentou resultados sobre testes de primalidade, desenvolveu as sequências de Lucas, que se relacionam, dentre outras, com a sequência de Fibonacci, e é o criador do conhecido jogo Torre de Hanói. Nesta seção, trataremos do Teorema de Lucas, que aborda a divisibilidade de um coeficiente binomial por um número primo. Para fazermos tal análise de divisibilidade, escreveremos sempre o numerador e o denominador do coeficiente binomial na base p, para o que se faz necessário recordar, ou conhecer, a seguinte definição:

Definição 4.7 Seja m um número inteiro e p um número primo, definimos como $m = m_0 + m_1 p + m_2 p^2 + \ldots + m_k p^k$ a escrita p-ádica ou expansão p-ádica do número m, onde cada m_i é tal que $0 \leq m_i \leq p-1$. Dizemos também que, desta forma, m está escrito na base p e os m_i são os seus $k+1$ algarismos.

A escrita p-ádica de um número inteiro é única, o que não será provado neste texto. Recomendamos, para isto, a leitura da referência (HEFEZ, 2013).

[1] Lucas, François Édouard Anatole (1842-1891), matemático francês.

Teorema 4.8 (Teorema de Lucas) Seja p um número primo e sejam $n = n_0 + n_1 p + n_2 p^2 + \ldots + n_k p^k$ e $m = m_0 + m_1 p + m_2 p^2 + \ldots + m_k p^k$ dois números naturais escritos ambos na base p. Então,

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_k}{m_k}(mod\, p). \tag{4.2}$$

Prova. A demonstração segue do teorema 4.4, fazendo-se indução sobe k e observando que $k+1$ é o número de dígitos da expansão base p de m ou de n.

Se $k = 1$, temos

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}(mod\, p),$$

sendo válido o caso base pelo teorema 4.4. Suponhamos então que a expressão 4.2 seja verdadeira para $k = l$. Assim, sendo os inteiros $n' = n_1 + n_2 p + \ldots + n_{l+1} p^l$ e $m' = m_1 + m_2 p + \ldots + m_{l+1} p^l$, ambos têm $l+1$ dígitos em sua expansão base p, o que, pela hipótese de indução nos garante

$$\binom{n'}{m'} \equiv \binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_{l+1}}{m_{l+1}}(mod\, p).$$

Por outro lado, $n = n' p + n_0$ e $m = m' p + m_0$. Logo, pelo teorema 4.4,

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n'}{m'}(mod\, p)$$

$$\Longrightarrow \quad \binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_{l+1}}{m_{l+1}}(mod\, p).$$

Ou seja, a validez para $k = l$, implica na validez para $k = l+1$. Desta forma, a expressão 4.2 é válida para todo k natural, o que completa nossa prova por indução.

□

Exemplo 4.9 Se $\binom{n}{m}$ é ímpar para todo $m \leq n$, mostrar que existe um número k inteiro não negativo tal que $n = 2^{k+1} - 1$.

Solução. Seja $n = n_0 + n_1 \cdot 2 + \ldots + n_r \cdot 2^r$ a expansão binária do número n. Se $r = 0$, temos $n = 0$ ou $n = 1$, o que nos dá $\binom{n}{m}$ igual a $\binom{0}{0}$ ou $\binom{1}{0}$, que são iguais a 1, portanto ímpares. Nesse caso, k existe, pois

$$0 = 2^{-1+1} - 1 \quad \text{e} \quad 1 = 2^{0+1} - 1.$$

Seja, então $r \geq 1$. O Teorema de Lucas nos diz que

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_r}{m_r}(mod\ 2).$$

Com $n_j, m_j \in \{0,1\}$. Suponhamos, por absurdo, que para algum $j < r$, tenhamos $n_j = 0$. Se tomarmos $m = 2^j$, o que é possível, pois m pode assumir qualquer valor menor ou igual a n, teremos

$$\begin{aligned}
\binom{n}{m} &\equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_j}{m_j}\ldots\binom{n_r}{m_r}(mod\ 2) \\
\Longrightarrow \quad \binom{n}{m} &\equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{0}{1}\ldots\binom{n_r}{m_r}(mod\ 2) \\
\Longrightarrow \quad \binom{n}{m} &\equiv 0\ (mod\ 2).
\end{aligned}$$

Ou, seja, uma contradição, já que $\binom{n}{m}$ é ímpar para todo $m \leq n$. Portanto, nenhum dos n_j pode ser igual a 0, e assim, a expansão binária de n é

$$\begin{aligned}
n &= 1\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + \cdots 1\cdot 2^r \\
&= 1 + 2 + 2^2 + \cdots 2^r \\
&= 2^{r+1} - 1.
\end{aligned}$$

Portanto, para $r \geq 1$, k existe e é igual a r, e o resultado segue.

□

Corolário 4.10 Sejam n e m inteiros não negativos tais que $n = n_0 + n_1 p + n_2 p^2 + \ldots + n_k p^k$ e $m = m_0 + m_1 p + m_2 p^2 + \ldots + m_k p^k$, com p primo. O coeficiente binomial $\binom{n}{m}$ é divisível por p se, e somente se, $m_i > n_i$, para algum $i \in \{0,1,\ldots,k\}$.

Prova. Como vimos no teorema 4.4,

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_k}{m_k}(mod p).$$

Assim, para que $\binom{n}{m}$ seja divisível por p, devemos ter

$$\binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\ldots\binom{n_k}{m_k} \equiv 0\ (mod p).$$

Para que isso ocorra, algum dos $\binom{n_i}{m_i}$ deve ser divisível por p, pois p é primo. Suponhamos, então que p divida $\binom{n_i}{m_i}$ para algum i. Pelo teorema 2.4,

$$\binom{n_i}{m_i} = \frac{n_i(n_i-1)\cdots(n_i-m_i+1)}{1\cdot 2\cdots m_i}.$$

Então p divide algum dos $n_i,(n_i-1),\ldots,(n_i-m_i+1)$, o que só é possível se algum deles for igual a 0, pois $n_i < p$. Desta forma, seja n_i-m_i+l o fator nulo, com $l \geq 1$, temos

$$n_i-m_i+l=0 \quad \Longrightarrow \quad m_i=n_i+l \quad \Longrightarrow \quad m_i > n_i.$$

Reciprocamente, se $m_i > n_i$, de acordo com a definição 2.1, o coeficiente binomial $\binom{n_i}{m_i}=0$, pois o polinômio $(1+x)^{n_i}$ não tem termo em x^{m_i}. Logo, para algum i, teremos

$$\begin{aligned} \binom{n}{m} &\equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\cdots 0\cdots\binom{n_k}{m_k}(mod\,p) \\ \Longrightarrow \quad \binom{n}{m} &\equiv 0\,(mod\,p) \quad \Longrightarrow \quad p \mid \binom{n}{m}. \end{aligned}$$

Portanto, $\binom{n}{m}$ é divisível por p se, e somente se, $m_i > n_i$.

□

Exemplo 4.11 Quantos múltiplos de 3 há na linha 100 do tiângulo de Pascal?

Solução. Vamos, inicialmente, escrever o número 100 na base 3, ou seja,

$$100 = 1\cdot 3^0+0\cdot 3^1+2\cdot 3^2+0\cdot 3^3+1\cdot 3^4.$$

Assim, pelo Teorema de Lucas, os coeficientes binomiais da linha 100 do triângulo de Pascal são tais que

$$\binom{100}{i} \equiv \binom{1}{i_0}\binom{0}{i_1}\binom{2}{i_2}\binom{0}{i_3}\binom{1}{i_4}\,(mod\ 3),$$

com $0 \leq i \leq 100$ e $i_k \in \{0,1,2\}$. Para determinarmos quantos dos $\binom{100}{i}$ são múltiplos de 3 é mais conveniente contarmos quantos não são múltiplos de 3 e subtrairmos do total. Nesse caso, de acordo com o corolário 4.10, cada i_k deve ser maior que zero e menor ou igual ao número

acima dele no coeficiente binomial. Temos, então as seguintes possibilidades:

$i_0 = 0 \quad \text{ou} \quad 1 \quad \longrightarrow \quad 2 \quad \text{possibilidades;}$
$i_1 = 0 \quad \longrightarrow \quad 1 \quad \text{possibilidade;}$
$i_2 = 0, \quad 1 \quad \text{ou} \quad 2 \quad \longrightarrow \quad 3 \quad \text{possibilidades;}$
$i_3 = 0 \quad \longrightarrow \quad 1 \quad \text{possibilidade;}$
$i_4 = 0 \quad \text{ou} \quad 1 \quad \longrightarrow \quad 2 \quad \text{possibilidades.}$

Usando o princípio multiplicativo, contamos um total de $2 \cdot 1 \cdot 3 \cdot 1 \cdot 2 = 12$ possibilidades que nos darão $\binom{100}{i} \not\equiv 0 \, (mod\ 3)$. Logo, dos 101 números da linha 100 do triângulo de Pascal, 12 não são múltiplos de 3. Portanto, os múltiplos de 3 são $101 - 12 = 89$.

Corolário 4.12 Sejam n, m números inteiros não negativos, p um número primo e r um número inteiro positivo, existem, ao todo, $\frac{p^r(p^r+1)}{2}$ números $\binom{n}{m}$, com $0 \leq n < p^r$ e $0 \leq m \leq n$, dois quais exatamente $\frac{p^r(p+1)^r}{2^r}$ não são divisíveis por p.

Prova. Para iniciarmos, é importante observar que essa contagem diz respeito aos coeficientes binomiais dos polinômios $(1+x)^0$, $(1+x)^1, \ldots,$ $(1+x)^{p^r-1}$, ou ainda, aos números do triângulo de Pascal até a linha $p^r - 1$. Para a primeira parte, basta recorrermos ao capítulo 2 e recordarmos que a linha k do triângulo de Pascal tem $k+1$ elementos. Assim, da linha 0 até a linha $p^r - 1$, teremos o total de

$$1 + 2 + 3 + \cdots + p^r = \frac{(1+p^r)p^r}{2} = \frac{p^r(p^r+1)}{2}$$

elementos (aqui utilizamos a fórmula da soma de uma progressão aritmética).

Para o que falta, utilizaremos um argumento combinatório e o resultado do corolário 4.10. Como sabemos, para que p divida $\binom{n}{m}$, em

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\cdots\binom{n_k}{m_k} (mod p),$$

devemos ter $m_i > n_i$, para algum $i \in \{0, 1, \ldots, k\}$. Então, para que p não divida $\binom{n}{m}$, devemos ter $m_i \leq n_i$ para todo i. Sabemos também que $0 \leq n_i, m_i \leq p-1$, pois $n_0, \ldots, n_k, m_0, \ldots, m_k$ são os algarismos de n e m escritos na base p.

Vamos, então, escrever cada n até a linha $p^r - 1$ do triângulo de Pascal na base p usando a mesma quantidade de algarismos, ainda que com zeros à esquerda. Desta forma,

$k = r-1$, pois $n < p^r$ e cada $\binom{n_i}{m_i}$ é dado da seguinte forma:
Se $m_i = n_i$, temos p possibilidades, que são

$$\binom{0}{0}, \binom{1}{1}, \ldots, \binom{p-1}{p-1}.$$

Se $m_i < n_i$, temos C_p^2, possibilidades, ou seja

$$C_p^2 = \frac{p(p-1)}{2}.$$

Ou seja, para cada um dos r possíveis $\binom{n_i}{m_i}$, temos

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

escolhas. Desta forma, o total de coeficientes $\binom{n}{m}$ que não são divisíveis por p é igual a

$$\left[\frac{p(p+1)}{2}\right]^r = \frac{p^r(p+1)^r}{2^r}.$$

□

É interessante percebermos que, para valores grandes de r, o número $\frac{p^r(p+1)^r}{2^r}$ é muito menor que o número $\frac{p^r(p^r+1)}{2}$. Isso nos diz que, quanto maior for n, maior é a probabilidade de o coeficiente binomial $\binom{n}{m}$ ser divisível por p. Por exemplo, para valores de n entre zero e 2^5, temos

$$\frac{p^r(p+1)^r}{2^r} = \frac{2^5(2+1)^5}{2^5} = 243$$

e

$$\frac{p^r(p^r+1)}{2} = \frac{2^5(2^5+1)}{2} = 528,$$

ou seja, a probabilidade de termos um múltiplo de 2 é de $\frac{528-243}{528} \approx 54\%$. Já para valores de n entre zero e 2^{10}, temos

$$\frac{p^r(p+1)^r}{2^r} = \frac{2^{10}(2+1)^{10}}{2^{10}} = 59049$$

e

$$\frac{p^r(p^r+1)}{2} = \frac{2^{10}(2^{10}+1)}{2} = 524800,$$

que nos dá a probabilidade $\frac{524800-59049}{524800} \approx 89\%$ de ocorrência de um coeficiente binomial múltiplo de 2.

Até aqui temos o suficiente para apresentar uma aplicação muito interessante que será o assunto da seção 4.3.

4.3 O Triângulo Aritmético módulo p (primo)

Uma aplicação interessante da aritmética dos coeficientes binomiais é o triângulo aritmético, ou de Pascal, módulo p (primo), que é a estrutura que obtemos ao substituirmos os coeficientes binomiais pelos restos das suas divisões por p. Quando fazemos essa substituição, todas as propriedades mostradas no capítulo 2 sobre os elementos do triângulo aritmético são mantidas, como veremos a seguir.

Exemplo 4.13 A partir dos elementos do triângulo aritmético até a 9ª linha, vamos reescrevê-lo também até a 9ª linha, módulo 3.

Resolução. Vamos inicialmente calcular os valores de cada coeficiente $\binom{n}{m}$, para $0 \leq n \leq 9$. Assim, temos

Figura 2 – Triângulo de Pascal até a linha 9

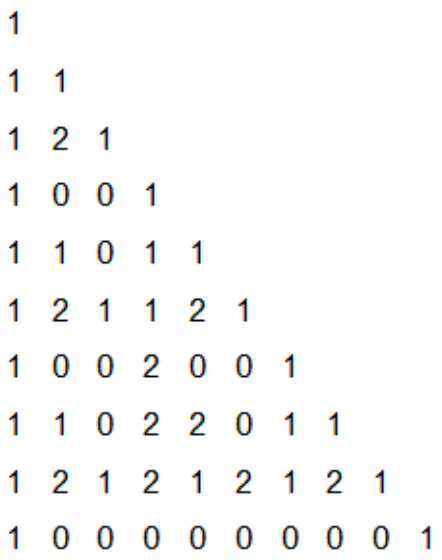
1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1

Fonte: Elaborado pela autora.

Agora, efetuamos a divisão de cada um desses números por 3. Sabemos que os restos dessas divisões só podem ser 0, 1 e 2, pois esses números formam o menor sistema completo de

resíduos módulo 3 com valores não negativos. Vejamos a figura 3, a seguir.

Figura 3 – Triângulo de Pascal até a linha 9 módulo 3



Fonte: Elaborado pela autora.

É possível, pela relação de Stifel e fazendo somas módulo 3, obtermos o triângulo acima até uma linha qualquer. Na figura 4, podemos ver que $\binom{5}{1} + \binom{5}{2} = \binom{6}{2}$, da mesma forma que $2+1 \equiv 0\,(mod\,3)$.

Este fato é aceitável pelas propriedades das congruências e pela relação de Stifel, pois, se

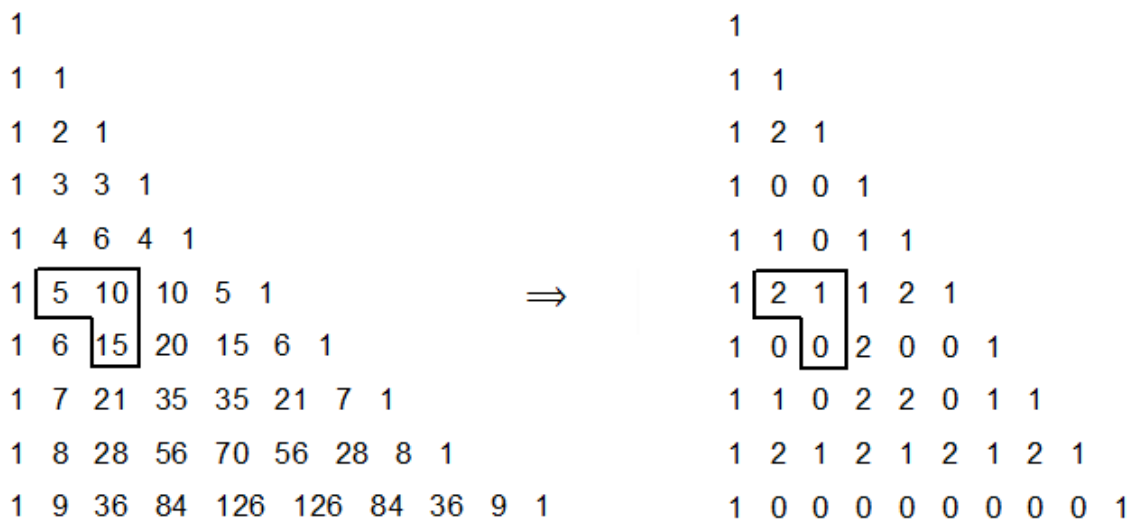
$$x_1 \equiv \binom{n}{k}(mod\,p) \quad \text{e} \quad x_2 \equiv \binom{n}{k+1}(mod\,p),$$

então

$$x_1 + x_2 \equiv \binom{n}{k} + \binom{n}{k+1} \equiv \binom{n+1}{k+1}(mod\,p).$$

Podemos também verificar que valem o teorema das linhas, o das colunas, o das diagonais e o da soma alternada. A forma de demostrarmos esses teoremas é análoga à apresentada

Figura 4 – Exemplo da Relação de Stifel módulo 3

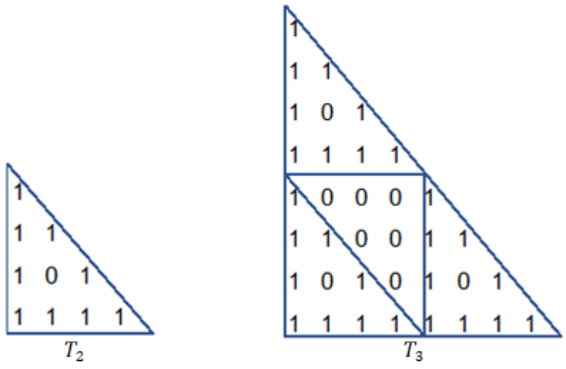


Fonte: Elaborado pela autora.

para a relação de Stifel, pois tratam-se de somas, e em todas elas nos apoiamos nas propriedades das congruências. Não julgamos, pois, necessário apresentarmos aqui tais demonstrações.

Seguiremos observando alguns padrões existentes nessas estruturas, analisando mais profundamente alguns aspectos relacionados ao triângulo aritmético módulo $p = 2$. Para isto, chamaremos de T_n o triângulo de Pascal módulo 2 até a linha $2^n - 1$. Por exemplo, T_2 vai até a linha $2^2 - 1 = 3$ e T_3 vai até a linha $2^3 - 1 = 7$.

Figura 5 – Triângulo de Pascal módulo 2

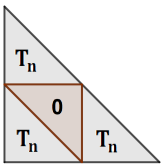


Fonte: Elaborado pela autora.

Proposição 4.14 Para $n \geq 1$, T_{n+1} apresenta a estrutura apresentada na figura 6 a seguir.

Prova. Sobre o T_n de cima, nada temos a demonstrar, pois corresponde exatamente às $2^n - 1$ primeiras linhas do triângulo. A segunda parte do padrão vai da linha 2^n a $2^{n+1} - 1$. Essas linhas

Figura 6 – Estrutura do triângulo de Pascal módulo 2



Fonte: Elaborado pela autora.

são, portanto, da forma $2^n + i$, com $i \in \{0, \ldots, 2^n - 1\}$. Fixemos um destes $i's$. Como $i \leq 2^n - 1$, a expansão binária de $2^n + i$ é igual a expansão binária de i com um dígito 1 acrescentado na posição $n+1$ e possivelmente alguns zeros, pois

$$i = i_0 + i_1 \cdot 2 + i_2 \cdot 2^2 + \ldots + i_{n-1} \cdot 2^{n-1}$$

e

$$2^n = 0 + 0 + \ldots + 0 + 2^n.$$

Vejamos que, se $0 \leq k \leq i$, então os elementos do triângulo T_n no canto inferior esquerdo da figura 6 são os números $\binom{2^n+i}{k}$, enquanto que os elementos do T_n de cima são os números $\binom{i}{k}$. Escrevendo a expansão binária de k, temos

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_{n-1} \cdot 2^{n-1},$$

e pelo Teorema de Lucas,

$$\begin{aligned}
\binom{2^n + i}{k} &\equiv \binom{i_0}{k_0}\binom{i_1}{k_1}\binom{i_2}{k_2}\cdots\binom{i_{n-1}}{k_{n-1}}\binom{1}{0} \, mod\, 2 \\
&\equiv \binom{i_0}{k_0}\binom{i_1}{k_1}\binom{i_2}{k_2}\cdots\binom{i_{n-1}}{k_{n-1}} \, mod\, 2 \\
&\equiv \binom{i}{k} \, mod\, 2.
\end{aligned}$$

Assim, explicamos o fato de T_n se repetir no canto inferior esquerdo da estrutura mostrada na figura 6. O teorema 2.5, que trata dos binomiais complementares, explica o triângulo T_n no canto inferior direito. Resta-nos, então, mostrar que entre esses dois triângulos há um triângulo somente com zeros. De fato, se $i < k < 2^n$, então os números binomiais $\binom{2^n+i}{k}$ ocupam exatamente a região que desejamos descrever. Como $i < k$, algum dígito da expansão binária de k (digamos o que está na posição j) tem de ser maior que o dígito correspondente de i. E

como $k < 2^n$, este dígito tem de estar antes da posição $n+1$, pelo que ainda é maior que o dígito correspondente da expansão de $2^n + i$. Desta forma, escrevemos

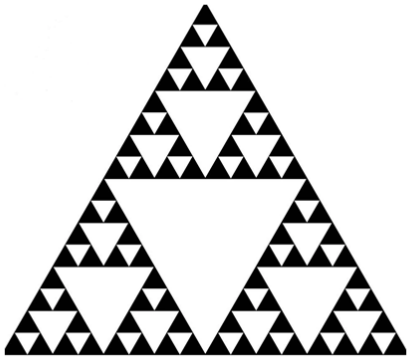
$$\begin{aligned}\binom{2^n+i}{k} &\equiv \binom{i_0}{k_0}\binom{i_1}{k_1}\binom{i_2}{k_2}\cdots\binom{i_j}{k_j}\cdots\binom{i_{n-1}}{k_{n-1}}\binom{1}{0} \, mod\, 2 \\ &\equiv \binom{i_0}{k_0}\binom{i_1}{k_1}\binom{i_2}{k_2}\cdots 0 \cdots \binom{i_{n-1}}{k_{n-1}} \, mod\, 2 \\ &\equiv 0 \, mod\, 2.\end{aligned}$$

Portanto, verifica-se o padrão apresentado na figura 6 para o triângulo de Pascal módulo 2.

□

Se substituirmos no triângulo de Pascal módulo 2 os números 1 por quadrados pretos e os números 0 por quadrados brancos, podemos visualizar melhor o padrão descrito na proposição 4.14, como foi feito na figura abaixo. Este diagrama é conhecido como triângulo de Sierpinski[2].

Figura 7 – Triângulo de Sierpinski a partir do triângulo de Pascal módulo 2



Fonte: ElPaís. Ciência/Matéria /02/11/2016.

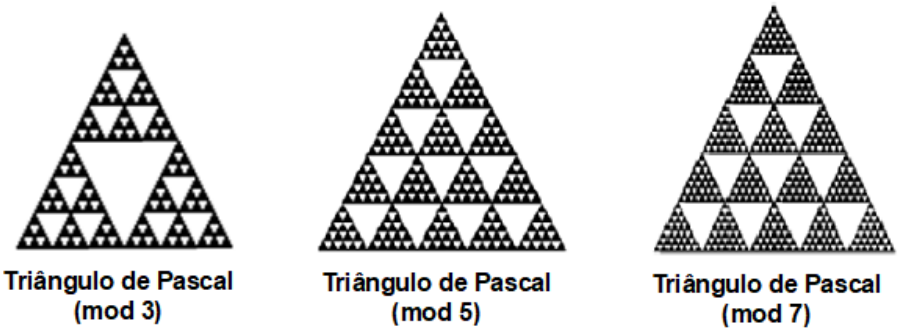
O triângulo de Sierpinski é uma figura geométrica que obtermos recursivamente. Esta figura apresenta muitas propriedades interessantes e que, aparentemente, não se relacionam com os coeficientes binomiais. No entanto, mostramos por meio desta proposição que é possível obtê-lo a partir do triângulo de Pascal módulo 2.

Algo semelhante pode ser observado considerando-se o triângulo módulo p para outros números

[2] Sierpinski, Waclaw (1882-1969), matemático polonês.

primos. Vamos apenas mostrar algumas imagens. Não apresentaremos, neste trabalho, um estudo sobre essas estruturas.

Figura 8 – Triângulo de Pascal módulo 3, módulo 5 e módulo 7



Fonte: Factoring binomial coefficients, and Pascal's Triangle mod p.

Com esta aplicação, encerramos o capítulo 4, certos de que há muito a ser estudado sobre as propriedades dos coeficientes binomiais do triângulo aritmético ou de Pascal. No entanto, passaremos à análise de outras características dos coeficientes binomiais, não relacionadas ao triângulo. O triângulo de Pascal módulo p é uma estrutura fascinante, e seus curiosos padrões são temas mais que suficientes para investigações exclusivas sobre este assunto. Deixemos como sugestão para trabalhos posteriores.

5 CONGRUÊNCIAS BINOMIAIS POR POTÊNCIAS DE PRIMOS

Neste capítulo, mostraremos uma aplicação da divisibilidade dos coeficientes binomiais através de dois teoremas que tratam sobre diferenças entre coeficientes binomiais cujos numeradores e denominadores são potências consecutivas de um dado número primo. Durante todo o capítulo, são mostrados conceitos que levam o leitor a uma ampliação de seus conhecimentos matemáticos e mesmo a uma maneira mais formal, porém clara, de enxergar conceitos corriqueiros da matemática do ensino médio.

5.1 O caso $p = 2$.

Teorema 5.1 Para $n > 1$, o número

$$a_n = \binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}} \tag{5.1}$$

é divisível por 2^{2n+2}.

Prova. Inicialmente observemos que a restrição para $n > 1$ é necessária, pois

$$a_1 = \binom{2^{1+1}}{2^1} - \binom{2^1}{2^{1-1}} = \binom{2^2}{2^1} - \binom{2^1}{2^0} = \binom{4}{2} - \binom{2}{1} = 6 - 2 = 4$$

e

$$2^{2\cdot 1+2} = 16.$$

Como $16 \nmid 4$, a asserção não é válida para $n = 1$. Devemos, então, considerar $n > 1$.
Definindo o polinômio

$$P(x) = (1+x)^{2^{n+1}} - (1-x^2)^{2^n},$$

é verdade que o termo em x^{2^n} tem coeficiente $\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$. De fato, segue imediatamente da definição 2.1 que $\binom{2^{n+1}}{2^n}$ é o coeficiente de x^{2^n} em $(1+x)^{2^{n+1}}$. Em $(1-x^2)^{2^n}$ temos

$$\binom{2^n}{2^{n-1}}(-x^2)^{2^{n-1}} = \binom{2^n}{2^{n-1}}(-1)^{2^{n-1}} \cdot (x^2)^{2^{n-1}} = \binom{2^n}{2^{n-1}}x^{2^n},$$

pois $n > 1$.
Agora devemos mostrar que o coeficiente de x^{2^n} em $P(x)$ é divisível por 2^{2n+2}. Para isso, efetuaremos o desenvolvimento binomial de $P(x)$. Antes disso, para facilitar nossos cálculos,

façamos

$$\begin{aligned} P(x) &= (1+x)^{2^{n+1}} - (1-x^2)^{2^n} \\ &= (1+x)^{2^n \cdot 2} - [(1+x)(1-x)]^{2^n} \\ &= (1+x)^{2^n} \cdot (1+x)^{2^n} - (1+x)^{2^n}(1-x)^{2^n} \\ &= (1+x)^{2^n}[(1+x)^{2^n} - (1-x)^{2^n}]. \end{aligned}$$

Dentro dos colchetes, temos

$$\begin{aligned} (1+x)^{2^n} - (1-x)^{2^n} &= (1+x)^{2^n} - (1+(-x))^{2^n} \\ &= 1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n} \\ &\quad -1 - \binom{2^n}{1}(-x) - \binom{2^n}{2}(-x)^2 - \binom{2^n}{3}(-x)^3 + \cdots - (-x)^{2^n} \\ &= 1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n} \\ &\quad -1 - \binom{2^n}{1}(-x) - \binom{2^n}{2}x^2 - \binom{2^n}{3}(-x)^3 + \cdots - x^{2^n} \\ &= 2\left[\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \cdots + \binom{2^n}{2^n-1}x^{2^n-1}\right]. \end{aligned}$$

Observemos que este desenvolvimento nos deu somente expoentes ímpares para x. Agora, para obtermos os coeficientes de $P(x)$, basta multiplicarmos este resultado pelo desenvolvimento de $(1+x)^{2^n}$. Então,

$$\begin{aligned} P(x) &= [(1+x)^{2^n} - (1-x)^{2^n}] \cdot (1+x)^{2^n} \\ &= 2 \cdot \left[\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \cdots + \binom{2^n}{2^n-1}x^{2^n-1}\right] \cdot \left[1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \cdots + x^{2^n}\right]. \end{aligned}$$

No entanto, precisamos apenas do coeficiente de x^{2^n}. Esta potência é obtida sempre que multiplicamos dois termos cujas somas dos expoentes de x sejam iguais a 2^n, como x^{2^n-1} e x, x^{2^n-3} e x^3, e assim por diante. Desta forma, o coeficiente de x^{2^n} será dado pela soma

$$2 \cdot \left[\binom{2^n}{1} \binom{2^n}{2^n-1} + \binom{2^n}{3} \binom{2^n}{2^n-3} + \cdots + \binom{2^n}{2^n-1} \binom{2^n}{1} \right].$$

De acordo com o teorema 4.1, os números $\binom{2^n}{1}, \binom{2^n}{3}, \cdots, \binom{2^n}{2^n-1}$ são todos divisíveis por 2^n, assim, cada parcela da soma acima é divisível por $2^n \cdot 2^n$, ou seja, por 2^{2n}. Para concluirmos, basta notarmos que cada parcela dessa soma aparece duas vezes, e que todo o produto está multiplicado por dois. Assim, o coeficiente de x^{2^n} em $P(x)$ é múltiplo de $2^{2^n} \cdot 2 \cdot 2$ que é igual a 2^{2^n+2}.
Portanto, $a_n = \binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$, que também nos dá o coeficiente de x^{2^n} em $P(x)$, é divisível por 2^{2^n+2}.

□

Por exemplo,

$$\binom{4}{2} - \binom{2}{1} = 6 - 2 = 4 = 2^2$$

$$\binom{8}{4} - \binom{4}{2} = 70 - 6 = 64 = 2^6$$

$$\binom{16}{8} - \binom{8}{4} = 12870 - 70 = 12800 = 2^9 \cdot 25$$

$$\binom{32}{16} - \binom{16}{8} = 601080390 - 12870 = 601067520 = 2^{12} \cdot 146745.$$

Diferenças do tipo $\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$, todas divisíveis por potências de 2, e em particular, por 2^{2^n+2}.

Substituindo o número 2 dentro dos números binomiais por 3, 5 ou 7, podemos observar a ocorrência de algo semelhante. Vejamos os cálculos abaixo.

$$\binom{9}{3} - \binom{9}{1} = 84 - 3 = 81 = 3^4$$

$$\binom{27}{9} - \binom{9}{3} = 4686825 - 84 = 4686741 = 3^7 \cdot 2143$$

$$\binom{25}{5} - \binom{5}{1} = 43130 - 5 = 43125 = 5^5 \cdot 69$$

$$\binom{49}{7} - \binom{7}{1} = 85900584 - 7 = 85900577 = 7^5 \cdot 5111.$$

Cada uma das diferenças é divisível por potências de 3, 5, ou 7, conforme seja um desses o número dentro dos coeficientes binomiais. Por outro lado, quando substituímos 2 por 4 ou 6, por exemplo, percebemos que o mesmo não acontece, como nos exemplos a seguir.

$$\binom{16}{4} - \binom{4}{1} = 1820 - 4 = 1816 = 4 \cdot 454$$

$$\binom{36}{6} - \binom{6}{1} = 1947792 - 6 = 1947786 = 6 \cdot 324631$$

As diferenças encontradas não são divisíveis nem mesmo por 4^2 e 6^2, respectivamente. Podemos conjecturar então que, para p primo, o número

$$\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}} \tag{5.2}$$

seja divisível por alguma potência de p, com expoente maior que ou igual a 2. Isso, na verdade, é um fato, e pode ser provado como faremos através do próximo teorema. Antes, porém, demostraremos alguns lemas que serão usados nesta prova.

5.2 O caso geral

Para uma configuração adequada do resultado que queremos mostrar, faremos a alteração da expressão 5.2 para

$$\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}}, \tag{5.3}$$

e consideraremos $k \geq 3$.

Lema 5.2 Seja n um número inteiro positivo, então,

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{5.4}$$

Prova. Esta prova é simples, feita por indução sobre n.
Considerando o caso base $n = 1$, temos

$$1^2 = 1 = \frac{1(1+1)(2\cdot 1+1)}{6},$$

e o lema vale para $n = 1$.
Assumindo, agora, que a expressão 5.4 seja verdadeira para algum $n > 1$, verifiquemos se também é válida para $n+1$. Fazendo os cálculos e utilizando a hipótese de indução, podemos ver que

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \ldots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1)[(2n^2+n) + (6n+6)]}{6} \\
&= \frac{(n+1)(2n^2+4n+3n+6)}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)[(n+1)+1][2(n+1)+1]}{6}
\end{aligned}$$

A validez da expressão 5.4 para algum n inteiro positivo implica na validez para $n+1$. Então, pelo princípio da indução, ela é válida para todo n inteiro positivo.

□

Lema 5.3 Se os números m e s são tais que $1 \leq s < m$ e $mdc\,(m,s) = 1$, então existe um único número s', com $1 \leq s' < m$ para o qual $ss' - 1$ é divisível por m, ou seja,

$$ss' - 1 = mr, \tag{5.5}$$

com r inteiro positivo. Sendo assim definido, o número s' é o inverso multiplicativo módulo m do número s, pois $ss' \equiv 1\,(mod\,m)$.

Prova. Para o que precisamos provar, é suficiente mostrar que entre os números $0,1,2,\ldots,m-1$ existe um número s' tal que ss' deixa resto 1 na divisão euclidiana por m. Se olharmos para os números

$$0, s, 2s, 3s, \ldots, (m-1)s, \tag{5.6}$$

veremos que constituem um sistema completo de resíduos módulo m, pela proposição 3.15, já que $mdc\,(s,m) = 1$. Desta forma, pela definição 3.14, esses números são dois a dois incongruentes módulo m. Como temos m números em 5.6, e são m os restos possíveis na divisão euclidiana por m, sendo um desses resto o 1, então apenas um dos $s, 2s, 3s, \ldots, (m-1)s$ deixa resto 1 na divisão por m, validando o presente lema.

□

Lema 5.4 Dados os números $s_1, s_2, \ldots, s_q$, todos distintos, com $1 \leq s_i < m$ e $mdc\,(m,s_i) = 1$ para $i = 1,2,\ldots,q$, então os números $s'_1, s'_2, \ldots, s'_q$, que existem em virtude do lema 5.3, são os mesmos que os números $s_1, s_2, \ldots, s_q$ em alguma ordem.

Prova. Pela equação $s_i s'_i - 1 = mr_i$, como vimos em 5.5, afirmamos que $mdc\,(m,s'_i) = 1$, para $i = 1,2,\ldots,q$. De fato, o lema anterior nos diz que s'_i é o inverso multiplicativo de s_i módulo m, ou seja, s'_i é invertível módulo m, o que implica $mdc\,(m,s'_i) = 1$. Como $m \nmid 1$, então $m \nmid s_i s'_i$, o que implica $m \nmid s'_i$. Além disso, os números $s'_1, s'_2, \ldots, s'_q$ são todos diferentes, pois se $s'_i = s'_j$ e supondo $s_i > s_j$, teríamos

$$s_i s'_i - 1 - (s_j s'_j - 1) = (mr_i - mr_j)$$

$$\Longrightarrow \qquad s_i s'_i - 1 - (s_j s'_i - 1) = m(r_i - r_j)$$

$$\Longrightarrow \qquad \frac{(s_i - s_j)s'_i}{m} = (r_i - r_j) \in \mathbb{Z},$$

o que não é possível já que $mdc(m, s_i') = 1$ e $0 < s_i - s_j < m$.

Portanto, os números $s_1', s_2', \ldots, s_q'$ são todos diferentes, com $1 \leq s_i' < m$ (como definido no lema 5.3) e $mdc(m, s_i') = 1$, o que mostra que esses são os mesmos números $s_1, s_2, \ldots, s_q$, mudando, no máximo, a ordem em que aparecem.

□

Lema 5.5 Se m, s e a são números inteiros positivos tais que $mdc(m,s) = 1$ e $\frac{a}{s(m-s)}$ é um número inteiro, então o número $\frac{a}{s(m-s)} + a(s')^2$ é divisível por m, onde s' é como definido no lema 5.3.

Prova. Fazendo alguns cálculos básicos e utilizando a equação 5.5, temos

$$\begin{aligned}
\frac{a}{s(m-s)} + a(s')^2 &= \frac{a + a(s')^2 s(m-s)}{s(m-s)} \\
&= \frac{a[1 + s's's(m-s)]}{s(m-s)} \\
&= \frac{a}{s(m-s)}[1 + s's(m-s)s'] \\
&= \frac{a}{s(m-s)}[1 + (mr+1)(ms' - ss') \\
&= \frac{a}{s(m-s)}[1 + (mr+1)(ms' - mr - 1)] \\
&= \frac{a}{s(m-s)}[1 + m^2rs' - m^2r^2 - mr + ms' - mr - 1] \\
&= m\frac{a}{s(m-s)}[mrs - mr^2 - 2r + s] \\
&= mt, \quad \text{com} \quad t \in \mathbb{Z}.
\end{aligned}$$

E assim, $\frac{a}{s(m-s)} + a(s')^2$ é divisível por m.

□

Para enunciarmos o próximo lema, adotaremos uma notação, proveniente do artigo *on a certain property of binomial coefficients*, publicado em (TABACHNIKOV, 1999), que é o símbolo $[k,s]_n$, com k, s e n números inteiros positivos. Este símbolo denota o produto de todos os números inteiros positivos t, tais que $k \leq t \leq s$ e $mdc(t,n) = 1$. Por exemplo,

$$[2,13]_3 = 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \cdot 10 \cdot 11 \cdot 13.$$

Vamos também inserir uma escrita muito comum no ensino médio, que é o fatorial. Ele é indicado por um ponto de exclamação e expressa o produto de todos os inteiros positivos de 1 até n, ou seja,

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Inserida a notação de fatorial, podemos reescrever a fórmula 2.4 como

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}, \tag{5.7}$$

que utilizaremos em lemas posteriores.

Lema 5.6 Se p é primo e $k > 1$, então o número

$$M = [1, p^{k-1} - 1]_p \cdot N,$$

onde

$$\begin{aligned} N &= \frac{1}{1 \cdot (p^{k-1}-1)} + \frac{1}{2 \cdot (p^{k-1}-2)} + \ldots + \frac{1}{(p-1) \cdot (p^{k-1}-p+1)} + \\ &+ \frac{1}{(p+1) \cdot (p^{k-1}-p-1)} + \ldots + \frac{1}{(p^{k-1}-1) \cdot 1} + \\ &+ 1^2 + 2^2 + \ldots + (p-1)^2 + (p+1)^2 + \ldots + (p^{k-1}-1)^2, \end{aligned}$$

é inteiro e divisível por p^{k-1}.

Prova. O número N é composto de uma soma de frações, cujos denominadores são produtos de dois entre os números

$$1, 2, \ldots, p-1, p+1, \ldots, p^2-1, p^2+1, \ldots, p^{k-1}-1. \tag{5.8}$$

Mais especificamente, o produto de dois extremos dessa sequência. Observemos que, em 5.8, estão todos os números de 1 a $p^{k-1}-1$ que são primos com p. Desta forma, satisfazem a condição do lema 5.4, com $m = p^{k-1}$. Utilizando a distributividade da multiplicação em relação à adição e rearranjando as parcelas de N podemos dizer que M é uma soma de números da forma

$$[1, p^{k-1}]_p \left[\frac{1}{s\,(p^{k-1}-s)} + (s')^2 \right], \tag{5.9}$$

onde s assume os valores 5.8. Agora, para provar que cada uma das parcelas de M é um número inteiro, faremos uso do lema 5.5, definindo $a = [1, p^{k-1}]_p$. Assim, devemos ter

$$\frac{[1, p^{k-1}]_p}{s\,(p^{k-1}-s)}$$

inteiro. E, de fato, temos, pois de acordo com a definição da notação $[1, p^{k-1}]_p$, os números s e $(p^{k-1}-s)$ são dois de seus fatores. Portanto, os números da forma 5.9 são inteiros e divisíveis por p^{k-1}, o que confere a M a mesma condição.

□

Lema 5.7 Se p é um número primo, k e c inteiros positivos, então

$$(p^k c)! = [1, p^k c]_p\,(p^{k-1}c)!\,p^{p^{k-1}c}. \tag{5.10}$$

Prova. Como vimos na definição de fatorial, o lado esquerdo da igualdade em 5.10, pode ser escrito como

$$(p^k c)! = (p^k c)(p^k c-1)\cdots(p^k c-(p-1))(p^k c-p)\cdots(p^k c-2p)\cdots(p^k c-3p)\cdots \\ \cdots(p^k c-(p^{k-1}c)p-1)$$

No produto acima, os fatores

$$p^k c,\, p^k c-p,\, p^k c-2p, \ldots, p^k c-(p^{k-1}c-1)p$$

são divisíveis por p. Um total de $p^{k-1}c$ números. Colocando p em evidência em cada um desses números, temos

$$p(p^{k-1}c),\ p(p^{k-1}c-1),\ p(p^{k-1}c-2), \ldots,\ p(p^{k-1}c-p^{k-1}c+1).$$

No desenvolvimento de $(p^k c)!$, temos os fatores que são primos com p, que denotamos por $[1, p^k c]_p$ e os fatores que são divisíveis por p, listados acima. Desta forma, podemos escrever

$$\begin{aligned}(p^k c)! &= [1, p^k c]_p \cdot p(p^{k-1}c)p(p^{k-1}c-1)p(p^{k-1}c-2)\cdots p(p^{k-1}c-p^{k-1}c+1).\\ &= [1, p^k c]_p \cdot p(p^{k-1}c)p(p^{k-1}c-1)p(p^{k-1}c-2)\cdots p\cdot 1\\ &= [1, p^k c]_p\,(p^{k-1}c)!\,p^{p^{k-1}c}.\end{aligned}$$

Sendo, portanto, válido o presente lema.

□

Lema 5.8 Para p primo e k inteiro positivo, são verdadeiras as asserções

$$(p^k)! = [1, p^k]_p[1, p^{k-1}]_p \cdots [1, p^2]_p[1, p]_p\, p^{\frac{p^k-1}{p-1}}. \tag{5.11}$$

$$(p^k - p^{k-1})! = [1, p^k - p^{k-1}]_p[1, p^{k-1} - p^{k-2}]_p \cdots [1, p^2 - p]_p[1, p-1]_p\, p^{p^{k-1}-1}. \tag{5.12}$$

Prova. Ambas as fórmulas são provadas por indução em k, usando na hipótese o resultado do lema 5.7.

Considerando como caso base $k = 1$, temos, para as duas asserções,

$$\begin{aligned}(p^1)! &= p! = p(p-1)(p-2)\cdots 1 = [1, p]_p p = [1, p]_p p^{\frac{p^1-1}{p-1}} \quad \text{e}\\ (p^1 - p^{1-1})! &= (p-1)! = (p-1)(p-2)\cdot 1 = [1, p-1]_p = [1, p-1]_p p^{p^{1-1}-1}.\end{aligned}$$

Ou seja, vale o caso base.

Suponhamos por hipótese de indução que, para algum $k > 1$, sejam verdadeiras as igualdades 5.11 e 5.12 e mostremos que também são verdadeiras para $k+1$. Para a asserção 5.11, queremos mostrar que

$$(p^{k+1})! = [1, p^{k+1}]_p[1, p^k]_p \cdots [1, p^2]_p[1, p]_p\, p^{\frac{p^{k+1}-1}{p-1}}. \tag{5.13}$$

De fato, calculando $(p^{k+1})!$ por meio do lema 5.7, e usando a hipótese de indução, constatamos o desejado, ou seja,

$$\begin{aligned}(p^{k+1})! &= (p^k p)! = [1p^k p]_p (p^{k-1}p)! p^{p^{k-1}p}\\ &= [1, p^{k+1}]_p (p^k)! p^{p^k}\\ &= [1, p^{k+1}]_p[1, p^k]_p[1, p^{k-1}]_p \cdots [1, p^2]_p[1, p]_p\, p^{\frac{p^k-1}{p-1}} \cdot p^{p^k}\\ &= [1, p^{k+1}]_p[1, p^k]_p[1, p^{k-1}]_p \cdots [1, p^2]_p[1, p]_p\, p^{\frac{p^{k+1}-1}{p-1}}.\end{aligned}$$

Da mesma forma, para a asserção 5.12, queremos mostrar que

$$(p^{k+1}-p^k)! = [1, p^{k+1}-p^k]_p [1, p^k - p^{k-1}]_p \cdots [1, p^2-p]_p [1, p-1]_p \, p^{p^k-1}. \tag{5.14}$$

O que conseguimos facilmente usando o lema 5.7 e a hipótese de indução. Pois,

$$\begin{aligned}
(p^{k+1}-p^k)! &= (p^k(p-1))! = [1, p^k(p-1)]_p (p^{k-1}(p-1))! p^{p^{k-1}(p-1)} \\
&= [1, p^{k+1}-p^k]_p (p^k - p^{k-1})! p^{p^k - p^{k-1}} \\
&= [1, p^{k+1}-p^k][1, p^k - p^{k-1}]_p [1, p^{k-1} - p^{k-2}]_p \cdots [1, p-1]_p \, p^{p^{k-1}-1} \cdot p^{p^k - p^{k-1}} \\
&= [1, p^{k+1}-p^k][1, p^k - p^{k-1}]_p [1, p^{k-1} - p^{k-2}]_p \cdots [1, p-1]_p \, p^{p^k-1}.
\end{aligned}$$

Assim, se 5.11 e 5.12 valem para k, valem também para $k+1$, e está provado por indução o lema 5.8.

□

Lema 5.9 Se p é um número primo e k um número inteiro positivo, então

$$\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} = \frac{p\left([p^k - p^{k-1}, p^k]_p - [1, p^{k-1}]_p\right)}{[1, p^{k-1}-p^{k-2}]_p [1, p^{k-2}-p^{k-3}]_p \cdots [1, p^2-p]_p [1, p-1]_p}. \tag{5.15}$$

Prova. Como já podemos visualizar, a expressão do lado direito da igualdade deriva-se da expressão do lado esquerdo por meio da fórmula 5.7, para calcular coeficientes binomiais, e do lema 5.8. Façamos abaixo, separadamente, o cálculo de cada coeficiente binomial.

$$\begin{aligned}
\binom{p^k}{p^{k-1}} &= \frac{(p^k)!}{(p^{k-1})!(p^k - p^{k-1})!} \\
&= \frac{[1, p^k]_p [1, p^{k-1}]_p \cdots [1, p^2]_p [1, p]_p \, p^{\frac{p^k-1}{p-1}}}{[1, p^{k-1}]_p [1, p^{k-2}]_p \cdots [1, p^2]_p [1, p]_p \, p^{\frac{p^{k-1}-1}{p-1}} (p^k - p^{k-1})!} \\
&= \frac{[1, p^k]_p \, p^{p^{k-1}}}{[1, p^k - p^{k-1}]_p [1, p^{k-1} - p^{k-2}]_p \cdots [1, p^2-p]_p [1, p-1]_p \, p^{p^{k-1}-1}} \\
&= \frac{[1, p^k]_p \, p}{[1, p^k - p^{k-1}]_p [1, p^{k-1} - p^{k-2}]_p \cdots [1, p^2-p]_p [1, p-1]_p}.
\end{aligned}$$

Analogamente, temos

$$\binom{p^{k-1}}{p^{k-2}} = \frac{[1,p^{k-1}]_p\, p}{[1,p^{k-1}-p^{k-2}]_p[1,p^{k-2}-p^{k-3}]_p\cdots[1,p^2-p]_p[1,p-1]_p}.$$

Assim,

$$\begin{aligned}
\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} &= \frac{[1,p^k]_p\, p - [1,p^k-p^{k-1}]_p[1,p^{k-1}]_p\, p}{[1,p^k-p^{k-1}]_p[1,p^{k-1}-p^{k-2}]_p\cdots[1,p^2-p]_p[1,p-1]_p} \\
&= \frac{[1,p^k-p^{k-1}]_p[p^k-p^{k-1},p^k]_p\, p - [1,p^k-p^{k-1}]_p[1,p^{k-1}]_p\, p}{[1,p^k-p^{k-1}]_p[1,p^{k-1}-p^{k-2}]_p\cdots[1,p^2-p]_p[1,p-1]_p} \\
&= \frac{p[1,p^k-p^{k-1}]_p\left([p^k-p^{k-1},p^k]_p - [1,p^{k-1}]_p\right)}{[1,p^k-p^{k-1}]_p[1,p^{k-1}-p^{k-2}]_p\cdots[1,p^2-p]_p[1,p-1]_p} \\
&= \frac{p\left([p^k-p^{k-1},p^k]_p - [1,p^{k-1}]_p\right)}{[1,p^{k-1}-p^{k-2}]_p\cdots[1,p^2-p]_p[1,p-1]_p}
\end{aligned}$$

□

Lema 5.10 Para todos os inteiros $a, x_1, x_2, \ldots, x_n$, a seguinte equação é válida:

$$(a+x_1)(a+x_2)\cdots(a+x_n) - x_1x_2\cdots x_n = ax_1x_2\cdots x_n\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)+a^2N \quad (5.16)$$

para algum $N \in \mathbb{Z}$.

Prova. Provaremos por indução sobre n.

A equação é verdadeira para $n = 1$, pois

$$(a+x_1) - x_1 = a = ax_1\left(\frac{1}{x_1}\right) + a^2\cdot 0.$$

Consideremos, então, por hipótese de indução, que 5.16 seja válida para algum $n > 1$. Mostremos

que também é válida para $n+1$. Assim, temos

$$(a+x_1)(a+x_2)\cdots(a+x_n)(a+x_{n+1})-x_1x_2\cdots x_nx_{n+1}=$$

$$\begin{aligned}
&= [(a+x_1)(a+x_2)\cdots(a+x_n)](a+x_{n+1})-x_1x_2\cdots x_nx_{n+1}\\
&= \left[x_1x_2\cdots x_n+ax_1x_2\cdots x_n\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)+a^2N'\right](a+x_{n+1})-x_1x_2\cdots x_nx_{n+1}\\
&+ ax_1x_2\cdots x_n+a^2x_1x_2\cdots x_n\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)+a^3N'\\
&+ x_1x_2\cdots x_nx_{n+1}+ax_1x_2\cdots x_nx_{n+1}\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)+a^2x_{n+1}N'-x_1x_2\cdots x_nx_{n+1}\\
&= ax_1x_2\cdots x_n\frac{x_{n+1}}{x_{n+1}}+ax_1x_2\cdots x_nx_{n+1}\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)+a^2N\\
&= ax_1x_2\cdots x_nx_{n+1}\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}+\frac{1}{x_{n+1}}\right)+a^2N.
\end{aligned}$$

Ou seja, a validez para n implica na validez para $n+1$. Portanto, pelo princípio da indução finita, é valido o lema 5.10.

□

Lema 5.11 Se p é um número primo, e k inteiro positivo, então

$$[p^k-p^{k-1},p^k]_p-[1,p^{k-1}]_p=\frac{1}{2}p^{2k-1}(p-1)[1,p^{k-1}]_p$$

$$\times\quad\left[\frac{1}{1\cdot(p^{k-1}-1)}+\ldots+\frac{1}{(p^{k-1}-1)\cdot 1}\right]+p^{4k-2}Q,$$

sendo Q um número inteiro .

Prova. Para iniciar, observemos que

$$(p^k-p^{k-1}+s)(p^k-s)=p^{2k-1}(p-1)+s(p^{k-1}-s). \tag{5.17}$$

O resultado acima é simples de ser verificado por meio de uma multiplicação.

Vamos agora estender o produto $[p^k-p^{k-1},p^k]_p$ e multiplicar em pares os fatores que são

equidistantes das extremidades. Assim, temos

$$\begin{aligned}
[p^k - p^{k-1}, p^k]_p &= (p^k - p^{k-1} + 1)(p^k - p^{k-1} + 2)\cdots \\
&\times (p^k - p^{k-1} + p - 1)(p^k - p^{k-1} + p + 1)\cdots(p^k - 2)(p^k - 1) \\
&= (p^k - p^{k-1} + 1)(p^k - 1)(p^k - p^{k-1} + 2)(p^k - 2)\cdots \\
&\times (p^k - p^{k-1} + p - 1)(p^k - p + 1)(p^k - p^{k-1} + p + 1)(p^k - p - 1)\cdots \\
&\times \left(p^k - p^{k-1} + \frac{1}{2}(p^{k-1} - 1)\right)\left(p^k - p^{k-1} + \frac{1}{2}(p^{k-1} + 1)\right).
\end{aligned}$$

Com esta configuração, podemos aplicar a equação 5.17, ou seja,

$$\begin{aligned}
&[p^k - p^{k-1}, p^k]_p = \\
= \;& [p^{2k-1}(p-1) + 1(p^{k-1} - 1)][p^{2k-1}(p-1) + 2(p^{k-1} - 2)]\cdots \\
\times \;& [p^{2k-1}(p-1) + (p-1)(p^{k-1} - p + 1)][p^{2k-1}(p-1) + (p+1)(p^{k-1} - p - 1)]\cdots \\
\times \;& \left[p^{2k-1}(p-1) + \frac{1}{2}(p^{k-1} - 1)\cdot\frac{1}{2}(p^{k-1} + 1)\right].
\end{aligned}$$

Neste ponto, aplicamos o lema 5.10, fazendo $a = p^{2k-1}(p-1)$ e substituindo cada x_i pelos números

$$1\cdot(p^{k-1} - 1),\ 2\cdot(p^{k-1} - 2), \ldots, \frac{1}{2}(p^{k-1} - 1)\cdot\frac{1}{2}(p^{k-1} + 1),$$

observando que

$$1\cdot(p^{k-1} - 1)\cdot 2\cdot(p^{k-1} - 2)\cdot\frac{1}{2}(p^{k-1} - 1)\cdot\frac{1}{2}(p^{k-1} + 1) = [1, p^{k-1}]_p.$$

Desta forma, podemos escrever,

$$\begin{aligned}
&[p^k - p^{k-1}, p^k]_p - [1, p^{k-1}]_p = p^{2k-1}(p-1)[1, p^{k-1}]_p \times \\
\times \;& \left[\frac{1}{1\cdot(p^{k-1} - 1)} + \ldots + \frac{1}{\frac{1}{2}(p^{k-1} - 1)\cdot\frac{1}{2}(p^{k-1} + 1)}\right] + \left(p^{2k-1}\right)^2 Q \\
= \;& p^{2k-1}(p-1)[1, p^{k-1}]_p \times \frac{1}{2}\left[\frac{1}{1\cdot(p^{k-1} - 1)} + \ldots + \frac{1}{(p^{k-1} - 1)\cdot 1}\right] + \left(p^{2k-1}\right)^2 Q \\
= \;& \frac{1}{2}p^{2k-1}(p-1)[1, p^{k-1}]_p \times \left[\frac{1}{1\cdot(p^{k-1} - 1)} + \ldots + \frac{1}{(p^{k-1} - 1)\cdot 1}\right] + p^{4k-2}Q.
\end{aligned}$$

Encerrando, assim, a prova deste lema.

□

Lema 5.12 Sendo os números $1,2,\ldots,p-1,p+1,\ldots,p^{k-1}-1$, todos os números de 1 a $p^{k-1}-1$ que são primos com p, e $p>2$ um número primo, então

$$1^2+2^2+\ldots+(p-1)^2+(p+1)^2+\ldots+(p^{k-1}-1)^2=\frac{1}{6}p^{k-1}(p^{k-1}+1)(2p^{k-1}+1)-p^kL, \tag{5.18}$$

onde k é um inteiro positivo e L um número inteiro.

Prova. Aqui temos a soma dos quadrados de todos os números de 1 a p^{k-1} menos a soma dos quadrados dos números de 1 a p^{k-1} múltiplos de p. Assim, podemos representar o lado esquerdo da expressão 5.18 sob a forma

$$\sum_{i=1}^{p^{k-1}} i^2 - p^2 \sum_{i=1}^{p^{k-2}} i^2 \tag{5.19}$$

e calcularmos ambas as somas de acordo com o lema 5.2, ou seja,

$$\sum_{i=1}^{p^{k-1}} i^2 = \frac{p^{k-1}(p^{k-1}+1)(2p^{k-1}+1)}{6} \qquad \text{e}$$

$$p^2\sum_{i=1}^{p^{k-1}} i^2 = \frac{p^2p^{k-2}(p^{k-2}+1)(2p^{k-2}+1)}{6} = \frac{p^k(p^{k-2}+1)(2p^{k-2}+1)}{6}.$$

Efetuando a diferença 5.19, obtemos o resultado esperado, pois

$$\begin{aligned}\sum_{i=1}^{p^{k-1}} i^2 - p^2 \sum_{i=1}^{p^{k-2}} i^2 &= \frac{1}{6}\left[p^{k-1}(p^{k-1}+1)(2p^{k-1}+1)-p^k(p^{k-2}+1)(2p^{k-2}+1)\right] \\ &= \frac{1}{6}p^{k-1}(p^{k-1}+1)(2p^{k-1}+1)-p^kL.\end{aligned}$$

Como desejávamos mostrar.

□

Com os resultados mostrados até aqui, temos o suficiente para enunciarmos e provarmos o teorema central deste capítulo. Fomos instigados pelo caso $p=2$ e por alguns resultados particulares mostrados nos exemplos. Agora veremos que de fato é válido o caso geral.

Teorema 5.13 Para $p > 3$, primo, é válida a expressão:

$$\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} = p^{3k-1}R, \tag{5.20}$$

e se $p = 3$, então vale:

$$\binom{3^k}{3^{k-1}} - \binom{3^{k-1}}{3^{k-2}} = 3^{3k-2}S, \tag{5.21}$$

onde $k \geq 3$ e R, S são números inteiros.

Prova. Antes de iniciarmos, ressaltemos a não necessidade de falarmos sobre o caso $p = 2$, pois já tratamos deste caso mo teorema 5.1. Começaremos com a prova para $p > 3$. De acordo com o lema 5.9,

$$\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} = \frac{p\left([p^k - p^{k-1}, p^k]_p - [1, p^{k-1}]_p\right)}{[1, p^{k-1} - p^{k-2}]_p [1, p^{k-2} - p^{k-3}]_p \cdots [1, p^2 - p]_p [1, p-1]_p}.$$

Na expressão acima, podemos substituir a diferença $\left([p^k - p^{k-1}, p^k]_p - [1, p^{k-1}]_p\right)$ pelo seu equivalente conforme o lema 5.11. Então, temos

$$\begin{aligned}
&\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} = \\
&= \frac{p \cdot \frac{1}{2} p^{2k-1}(p-1)[1, p^{k-1}]_p \cdot \left[\frac{1}{1 \cdot (p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1) \cdot 1}\right] + p^{4k-2}Q}{[1, p^{k-1} - p^{k-2}]_p [1, p^{k-2} - p^{k-3}]_p \cdots [1, p^2 - p]_p [1, p-1]_p}. \\
&= \frac{\frac{1}{2} p^{2k}(p-1)[1, p^{k-1}]_p \cdot \left[\frac{1}{1 \cdot (p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1) \cdot 1}\right] + p^{4k-2}Q}{[1, p^{k-1} - p^{k-2}]_p [1, p^{k-2} - p^{k-3}]_p \cdots [1, p^2 - p]_p [1, p-1]_p}.
\end{aligned}$$

A partir daqui, precisaremos mostrar que o número

$$[1, p^{k-1} - 1]_p \cdot \left[\frac{1}{1 \cdot (p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1) \cdot 1}\right]$$

é divisível por p^{k-1}. Para isso, usaremos o lema 5.6, que nos garante que

$$M = [1, p^{k-1}-1]_p \cdot \left[\frac{1}{1\cdot(p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1)\cdot 1} + 1^2 + \ldots + (p^{k-1}-1)^2 \right]$$

é divisível por p^{k-1}.

Sobre a soma de quadrados que também aparece dentro dos colchetes. O lema 5.12 nos diz que

$$1^2 + \ldots + (p^{k-1}-1)^2 = \frac{1}{6} p^{k-1}(p^{k-1}+1)(2p^{k-1}+1) - p^k L,$$

o que substituímos na expressão de M, e obtemos como resultado

$$M = [1, p^{k-1}-1]_p \cdot \left[\frac{1}{1\cdot(p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1)\cdot 1} + \frac{1}{6} p^{k-1}(p^{k-1}+1)(2p^{k-1}+1) - p^k L \right].$$

Agora, fazendo o produto de $[1, p^{k-1}-1]_p$ por cada uma das parcelas dentro dos colchetes, temos

$$\begin{aligned} M &= [1, p^{k-1}-1]_p \cdot \left[\frac{1}{1\cdot(p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1)\cdot 1} \right] \\ &+ [1, p^{k-1}-1]_p \cdot \left[\frac{1}{6} p^{k-1}(p^{k-1}+1)(2p^{k-1}+1) \right] \\ &- [1, p^{k-1}-1]_p \cdot p^k L. \end{aligned}$$

A parcela $[1, p^{k-1}-1]_p \cdot p^k L$ é obviamente divisível por p^{k-1}. Como estamos analisando o caso $p > 3$, o fator $[1, p^{k-1}-1]_p$ é divisível por 6, pois 2 e 3 são menores que p e primos com ele, sendo

$$[1, p^{k-1}-1]_p \cdot \left[\frac{1}{6} p^{k-1}(p^{k-1}+1)(2p^{k-1}+1) \right]$$

também divisível por p^{k-1}. Portanto, pela proposição 3.3 item (g), a parcela

$$[1, p^{k-1}-1]_p \cdot \left[\frac{1}{1\cdot(p^{k-1}-1)} + \ldots + \frac{1}{(p^{k-1}-1)\cdot 1} \right]$$

é divisível por p^{k-1}, como precisávamos mostrar. Desta forma, podemos escrever

$$\begin{aligned}\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} &= \frac{\frac{1}{2}p^{2k}\cdot p^{k-1}(p-1)\cdot R_1 + p^{4k-2}Q}{[1,p^{k-1}-p^{k-2}]_p[1,p^{k-2}-p^{k-3}]_p\cdots[1,p^2-p]_p[1,p-1]_p}.\\ &= \frac{\frac{1}{2}p^{3k-1}(p-1)\cdot R_1 + p^{3k-1}\cdot p^{k-1}Q}{[1,p^{k-1}-p^{k-2}]_p[1,p^{k-2}-p^{k-3}]_p\cdots[1,p^2-p]_p[1,p-1]_p}.\\ &= \frac{p^{3k-1}\left[\frac{1}{2}(p-1)\cdot R_1 + p^{k-1}Q\right]}{[1,p^{k-1}-p^{k-2}]_p[1,p^{k-2}-p^{k-3}]_p\cdots[1,p^2-p]_p[1,p-1]_p}.\end{aligned}$$

Notemos que $\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}}$ é inteiro, pois é a diferença entre dois números inteiros. Por outro lado, o produto $[1,p^{k-1}-p^{k-2}]_p[1,p^{k-2}-p^{k-3}]\cdots[1,p^2-p]_p[1,p-1]_p$ não divide p, então este produto divide $\left[\frac{1}{2}(p-1)\cdot R_1 + p^{k-1}Q\right]$. Portanto,

$$\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}} = p^{3k-1}\cdot R.$$

E está provado o teorema para o caso $p > 3$.

Se $p = 3$, então

$$\begin{aligned}&\binom{3^k}{3^{k-1}} - \binom{3^{k-1}}{3^{k-2}} =\\ &= \frac{3\left([3^k-3^{k-1},3^k]_3 - [1,3^{k-1}]_3\right)}{[1,3^{k-1}-3^{k-2}]_3[1,3^{k-2}-3^{k-3}]_3\cdots[1,3^2-3]_3[1,3-1]_3}.\\ &= \frac{3\cdot\frac{1}{2}\cdot 3^{2k-1}(3-1)[1,3^{k-1}]_3\left[\frac{1}{1\cdot(3^{k-1}-1)}+\ldots+\frac{1}{(3^{k-1}-1)\cdot 1}\right]+3^{4k+2}Q}{[1,3^{k-1}-3^{k-2}]_3[1,3^{k-2}-3^{k-3}]_3\cdots[1,3^2-3]_3[1,3-1]_3}.\\ &= \frac{3^{2k}\cdot[1,3^{k-1}]_3\left[\frac{1}{1\cdot(3^{k-1}-1)}+\ldots+\frac{1}{(3^{k-1}-1)\cdot 1}\right]+3^{4k+2}Q}{[1,3^{k-1}-3^{k-2}]_3[1,3^{k-2}-3^{k-3}]_3\cdots[1,3^2-3]_3[1,3-1]_3}.\end{aligned}$$

Porém, neste caso, não podemos dizer que

$$[1,3^{k-1}-1]_3\cdot\left[\frac{1}{1\cdot(3^{k-1}-1)}+\ldots+\frac{1}{(3^{k-1}-1)\cdot 1}\right]$$

é divisível por 3^{k-1}. Isto porque

$$[1,3^{k-1}-1]_3 \cdot \frac{1}{6} \cdot 3^{k-1}(3^{k-1}+1)(2\cdot 3^{k-1}+1) = [4,3^{k-1}-1]_3 \cdot 3^{k-2}(3^{k-1}+1)(2\cdot 3^{k-1}+1).$$

Então, como

$$M = [1,3^{k-1}-1]_3 \cdot \left[\frac{1}{1\cdot(3^{k-1}-1)} + \ldots + \frac{1}{(3^{k-1}-1)\cdot 1} + \frac{1}{6}3^{k-1}(3^{k-1}+1)(2\cdot 3^{k-1}+1) - 3^k L \right]$$

é divisível por 3^{k-1}, é também divisível por 3^{k-2}, sendo possível garantir apenas que

$$[1,3^{k-1}-1]_3 \cdot \left[\frac{1}{1\cdot(3^{k-1}-1)} + \ldots + \frac{1}{(3^{k-1}-1)\cdot 1} \right]$$

é divisível por 3^{k-2}. Então, escrevemos

$$\begin{aligned} \binom{3^k}{3^{k-1}} - \binom{3^{k-1}}{3^{k-2}} &= \frac{3^{2k}\cdot 3^{k-2}\cdot S_1 + 3^{3k-2}\cdot 3^{k+4}Q}{[1,3^{k-1}-3^{k-2}]_3[1,3^{k-2}-3^{k-3}]_3\cdots[1,3^2-3]_3[1,3-1]_3}. \\ &= \frac{3^{3k-2}\left(S_1 + \cdot 3^{k+4}Q\right)}{[1,3^{k-1}-3^{k-2}]_3[1,3^{k-2}-3^{k-3}]_3\cdots[1,3^2-3]_3[1,3-1]_3}. \end{aligned}$$

E pela mesma argumentação apresentada no caso $p > 3$, concluímos que

$$\binom{3^k}{3^{k-1}} - \binom{3^{k-1}}{3^{k-2}} = 3^{3k-2}S.$$

É, portanto, válido o teorema 5.13 em seus dois casos.

□

Assim mostramos que diferenças do tipo $\binom{p^k}{p^{k-1}} - \binom{p^{k-1}}{p^{k-2}}$ são sempre divisíveis por grandes potências de p, para todo p primo. Esta é uma aplicação bastante interessante da divisibilidade dos coeficientes binomiais.

6 CONCLUSÃO

No decorrer deste trabalho, buscamos levar o leitor ao conhecimento e apreciação de algumas propriedades aritméticas dos coeficientes binomiais bem como de suas aplicações dentro da própria Matemática. Não houve a pretensão de propor aplicações do tema aos conteúdos da base comum curricular do ensino básico, nem de criar novas aplicações para a teoria apresentada. O objetivo é que um vasto conhecimento acerca da divisibilidade dos coeficientes binomiais, em especial por números primos, fosse reunido em um único texto com linguagem acessível inclusive para os alunos do ensino médio.

Com este intuito, iniciamos por apresentar, com fluidez e riqueza de detalhes, definições preliminares sobre os coeficientes binomiais e suas propriedades. Seguem-se a estas uma explanação sobre os alicerces da Aritmética, que são as propriedades relativas à divisibilidade dos números inteiros e as relações de congruência, devidas aos estudos de grandes matemáticos como Euclides e Gauss. Durante todo o texto, buscamos também fazer referência a estes atores, citando suas contribuições e dando breves informações biográficas em notas de rodapé. O embasamento para as notas históricas fornecidas estão nas referências (BOYER; MERZBACH, 2019), (STEWART, 2014) e (EVES, 1996), as quais recomendamos para um estudo mais aprofundado sobre a vida e a obra dos matemáticos citados.

A ideia central do que nos propomos a escrever é apresentada no capítulo que trata especificamente sobre a arimética dos coeficientes binomiais, ou seja, como se dá a divisibilidade desses números por outros inteiros positivos, particularmente se esses inteiros forem primos. Os capítulos anteriores, não menos importantes, deram o suporte necessário para o perfeito entendimento do que aqui fora escrito, e ainda com eles, abrimos parênteses para esclarecer termos e notações quando julgamos pertinente. Desta forma, temos consciência de estar disponibilizando um material de pesquisa rico em conhecimento e, sobretudo, de agradável leitura.

Ao final do capítulo central, tratamos sobre o interessantíssimo triângulo de Pascal módulo p primo, explorando apenas parte das imensas possibilidades de estudo sobre essa estrutura. Muitos trabalhos futuros podem ser escritos apenas com este tema, ficando como possibilidade para uma continuidade deste ou para trabalhos empreendidos pelos leitores cuja curiosidade tenha sido aguçada. Para encerrar, mostramos uma aplicação de toda a teoria apresentada e mais alguns conceitos e notações especiais discorrendo sobre a divisibilidade de expressões com binomiais por potências de números primos. Neste ponto, utilizamos um

rigor mais acentuado na escrita matemática, sem perder, contudo, a minuciosidade e clareza na exposição das ideias apresentadas.

Embora fique claro na leitura do desenvolvimento, reforçamos aqui que o conteúdo sobre ao qual dissertamos é de difícil acesso em português, e mesmo em outras idiomas. Tivemos o cuidado de demonstrar e exemplificar todos os conceitos deixados em aberto ou mencionados vagamente nos nossos referenciais teóricos. Este estudo, portanto, constitui-se em uma rica fonte de pesquisa e aprendizado, tendo sido idealizado e desenvolvido exatamente para este fim.

REFERÊNCIAS

ALENCAR FILHO, E. de. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. São Paulo: Blücher, 2019.

CAMINHA, A. **Tópicos de Matemática Elementar Volume 5**: teoria dos números. Rio de Janeiro: SBM, 2012.

EDWARDS, A. W. F. **Pascal's arithmetical triangle:** the story of a mathematical idea. New York: Courier Dover Publications, 2019.

EVES, H. **História da Matemática**. São Paulo: Editora da UNICAMP, 1996.

GAUSS, C. F. **Disquisitiones arithmeticae**. New York: Yale University Press, 1966.

HEFEZ, A. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

LANDAU, E. **Teoria elementar dos números**. Rio de Janeiro: Ciência Moderna, 2002.

MORGADO, A. C. d. O.; CARVALHO, J. B. P. d.; CARVALHO, P. C. P.; FERNANDEZ, P. **Análise combinatória e probabilidade**. Rio de Janeiro: Instituto de Matemática pura e aplicada, 1991.

STEWART, I. **Em busca do infinito:** uma história da matemática dos primeiros números à teoria do caos. Rio de Janeiro: Editora Zahar-Companhia das Letras, 2014.

TABACHNIKOV, S. **Kvant Selecta: Algebra and Analysis, I:** Algebra and Analysis. Providence, R.I.: American Mathematical Society., 1999.