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

HORÁCIO LEONEL DOS SANTOS SOUSA

APLICAÇÕES COMBINATÓRIAS À TEORIA DOS NÚMEROS

FORTALEZA
2017

HORÁCIO LEONEL DOS SANTOS SOUSA

APLICAÇÕES COMBINATÓRIAS À TEORIA DOS NÚMEROS

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

Orientador: Prof. Dr. José Othon Dantas Lopes.

FORTALEZA

2017

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)

S696a Sousa, Horácio Leonel dos Santos.
Aplicações combinatórias à teoria dos números / Horácio Leonel dos Santos Sousa. – 2017.
65 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, 2017.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Combinatória. 2. Teoria dos Números. 3. Aplicações. I. Título.

CDD 510

HORÁCIO LEONEL DOS SANTOS SOUSA

APLICAÇÕES COMBINATÓRIAS À TEORIA DOS NÚMEROS

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

Aprovada em: 27/07/2017.

BANCA EXAMINADORA

_____

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

_____

Prof. Dr. José Valter Lopes Nunes
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Ângelo Papa Neto
Instituto Federal do Ceará (IFCE)

À minha família.

AGRADECIMENTOS

À minha família, pelo apoio e incentivo.

Ao Prof. Dr. José Othon Dantas Lopes, pela excelente e sábia orientação.

Aos professores participantes da banca examinadora Dr. José Valter Lopes Nunes e Dr. Ângelo Papa Neto pelas valiosas colaborações e sugestões.

“Deus criou os números naturais. O resto é obra dos homens.”

Leopold Kronecker

RESUMO

A Teoria dos Números e a Análise Combinatória são duas áreas importantes da Matemática que possuem alguns de seus conceitos abordados no ensino fundamental e médio, onde são cobrados em avaliações externas como, por exemplo, o Exame Nacional do Ensino Médio e a Olimpíada Brasileira de Matemática das Escolas Públicas. A Teoria dos Números, de modo simples, trata dos números inteiros e suas propriedades e a Combinatória, por sua vez, trata da existência de certos eventos e, se possível, determina quantos deles existem. O presente trabalho apresenta a aplicação de conceitos combinatórios na obtenção de vários resultados em teoria dos números. Apresentam-se Princípios Combinatórios, como os princípios bijetivo, aditivo, fundamental da contagem, da inclusão-exclusão e da casa dos pombos. Por fim, dar-se provas combinatórias do pequeno teorema de Fermat e do teorema de Wilson. Deste modo, pretende-se despertar o aluno para a importância desses assuntos, facilitando assim o processo de ensino-aprendizagem.

Palavras-chave: Combinatória. Teoria dos Números. Aplicações.

ABSTRACT

The Number theory and Combinatorics are two important branches of mathematics that have some of their basic concepts addressed in elementary and high school. In Brazil, these areas of mathematics are the subject covered in several assessment exams, such as the Brazilian Mathematical Olympiad of Public Education, and the Brazilian National High School Exam. The Number theory studies the integers and their properties, while Combinatorics studies the occurrence of certain events and determines how many of them exist, when possible. This work applies combinatorial concepts in the derivation of several results from the Number theory. In this study presented several combinatorial principles, such as the bijection principle, the addition principle, the multiplication principle, the inclusion–exclusion principle, and the pigeonhole principle. At least, they are presented proofs of the Fermat's little theorem and the Wilson's theorem using combinatorial principles. This work seeks to arouse students' interest to the importance of these subjects, thus facilitating and paving the way to teaching-learning process.

Keywords: Combinatorics. Number Theory. Applications.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

PBO	Princípio da Boa Ordenação
PFC	Princípio Fundamental da Contagem
PCP	Princípio da Casa dos Pombos
OBM	Olimpíada Brasileira de Matemática
ENEM	Exame Nacional do Ensino Médio

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\emptyset$	Conjunto Vazio
$\Longrightarrow$	Implica
$\Longleftrightarrow$	Se, e somente se
$\in$	Pertence
$\notin$	Não pertence
$\subset$	Está contido
$\cup$	União
$\cap$	Interseção
α	Alfa
ϕ	Fi
π	Pi
$\bigcup$	Conjunto União
$\sum$	Somatório
$\prod$	Produtório
$a \mid b$	a divide b
$a \nmid b$	a não divide b
$mdc(a, b)$	Máximo Divisor Comum de a e b
f^{-1}	Função Inversa
$f \circ g$	Função Composta
$n!$	Fatorial de n
$\binom{n}{k}$	Número Binomial
■	Final da Prova

SUMÁRIO

1 INTRODUÇÃO

O ensino de Matemática pode tornar-se difícil às vezes, pois a maioria dos alunos demonstra certo desinteresse pela disciplina. De tal modo, uma proposta interessante para atrair a atenção dos estudantes é apresentar conexões e aplicações existentes entre temas distintos da Matemática como a Análise Combinatória e a Teoria dos Números que sempre são cobrados no Enem (Exame Nacional do Ensino Médio) e também em olimpíadas de Matemática.

Este trabalho tem como objetivo apresentar alguns resultados da teoria dos números justificados por conceitos, ideias e métodos combinatórios, fortalecendo os aspectos teóricos e colocando a combinatória em prática através de exemplos ligados à teoria dos números que vão desde assuntos básicos aos mais sofisticados.

Inicialmente, apresentamos os princípios de indução e o princípio da boa ordenação, que constituem ferramentas imprescindíveis na obtenção de vários resultados combinatórios e aritméticos. Em seguida, abordamos definições, propriedades e resultados sobre o conjunto dos números inteiros (divisibilidade, máximo divisor comum e números primos) com destaque para o Algoritmo da Divisão e o Teorema Fundamental da Aritmética.

Por fim, abordamos alguns princípios e conceitos combinatórios como os princípios bijetivo, aditivo e fundamental da contagem com evidência para a fórmula que calcula o número de divisores positivos de um número inteiro, os números binomiais e o binômio de Newton com destaque para a prova do pequeno teorema de Fermat, o princípio da inclusão-exclusão utilizado para calcular o número de inteiros positivos menores ou iguais e relativamente primos com um inteiro positivo, o princípio da casa dos pombos empregado na solução de alguns problemas de existência e finalmente damos provas combinatórias para o pequeno teorema de Fermat baseada na contagem de certas pulseiras construídas usando-se p pérolas de n cores diferentes e também para o teorema de Wilson, baseada na contagem do número de diferentes polígonos estrelados que podemos construir com p pontos distribuídos em um círculo.

2 INDUÇÃO FINITA

O princípio de indução finita é um método eficiente para demonstrar fatos referentes a números naturais, sendo utilizado na obtenção de muitos resultados importantes. Seguiremos Muniz Neto [1] no desenvolvimento das seções 2.1 e 2.2.

2.1 Primeiro Princípio de Indução Finita

Seja A um subconjunto dos números naturais $\mathbb{N} = \{1,2,3, \dots\}$, tal que $1 \in A$ e para todo $k \in A$, temos que $k + 1 \in A$. Então, $1 \in A$ assegura que $2 \in A$. Logo, $2 \in A$ implica que $3 \in A$ e assim por diante. Logo, podemos concluir que A contém todos os números naturais e, portanto, $A = \mathbb{N}$. Essa ideia está formalizada no seguinte axioma.

Axioma 2.1.1 (Primeiro Princípio de Indução Finita) Seja A um subconjunto de $\mathbb{N}$ tal que:

$(i)\ 1 \in A$;
(ii) Se $k \in A$, então $k + 1 \in A$.

Então $A = \mathbb{N}$.

Seja $P(n)$ uma propriedade do natural n, cuja a veracidade desejamos mostrar para todo $n \in \mathbb{N}$. A aplicação do axioma 2.1.1 como ferramenta de demonstração consiste em definir o subconjunto A como $A = \{k \in \mathbb{N} \mid P(k) \text{ é verdeira}\}$ e observando que

$$A = \mathbb{N} \Leftrightarrow P(n) \text{ é verdadeira para todo } n \in \mathbb{N},$$

vemos que, para demonstrar que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, basta mostrar que $A = \mathbb{N}$, ou seja, pelo primeiro princípio de indução, que

$(i)\ 1 \in A$;
$(ii)\ k \in A \Longrightarrow k + 1 \in A$.

E pela definição de A, mostrar os dois itens acima equivale mostrar que

(i) $P(1)$ é verdadeira;
(ii) $P(k)$ verdadeira $\Longrightarrow P(k+1)$ verdadeira.

Essas ideias nos permitem estabelecer a seguinte proposição.

Proposição 2.1.1 Dada uma propriedade $P(n)$ do natural n, temos $P(n)$ verdadeira para todo $n \in \mathbb{N}$ se e só se as duas condições a seguir forem satisfeitas:

(i) $P(1)$ é verdadeira;
(ii) $P(k)$ verdadeira $\Longrightarrow P(k+1)$ verdadeira.

Exemplo 2.1.1 Prove que, para todo $n \in \mathbb{N}$, temos

$$\sum_{i=0}^{n-1} 2^i = 2^n - 1.$$

Prova. Para provarmos, por indução, a validade da propriedade

$$P(n): \sum_{i=0}^{n-1} 2^i = 2^n - 1,$$

temos de verificar que

(i) $P(1)$ é verdadeira;
(ii) $P(k)$ verdadeira $\Longrightarrow P(k+1)$ verdadeira.

A verificação de (i) é imediata, pois

$$\sum_{i=0}^{1-1} 2^i = \sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^1 - 1.$$

Para provarmos (ii), supomos que $P(k)$ é verdadeira, isto é, que

$$1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$$

e queremos deduzir que $P(k+1)$ também é verdadeira, isto é, que

$$1 + 2 + 2^2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1.$$

Mas desde que estamos supondo a validade de $P(k)$, segue que

$$1 + 2 + 2^2 + \cdots + 2^{k-1} + 2^k = 2^k - 1 + 2^k$$

$$= 2 \cdot 2^k - 1$$

$$= 2^{k+1} - 1.$$

Portanto, por indução, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

■

2.1.1 Forma geral do primeiro princípio de indução finita

Uma forma mais geral do primeiro princípio de indução é o seguinte axioma.

Axioma 2.1.2 Seja $a \in \mathbb{N}$ e A um subconjunto de $\{a, a+1, a+2, \ldots\}$ tal que:

(i) $a \in A$.
(ii) Se $k \in A$, então $k + 1 \in A$.

Então $A = \{a, a+1, a+2, \ldots\}$.

Dada uma propriedade $P(n)$ do natural n, cuja veracidade desejamos provar para todo natural $n \geq a$, analogamente ao axioma 2.1.1, a aplicação do axioma 2.1.2 como método de demonstração consiste em definirmos o subconjunto A como $A = \{k \in \mathbb{N} \mid P(k) \text{ é verdeira}\}$ e observar que

$$A = \{a, a+1, a+2, \ldots\} \Leftrightarrow P(n) \text{ é verdadeira para todo } n \geq a \text{ natural.}$$

Assim, podemos estabelecer uma forma mais geral para a proposição 2.1.1 como a seguir.

Proposição 2.1.2 Dados $a \in \mathbb{N}$ e uma propriedade $P(n)$ do natural n, temos $P(n)$ verdadeira para todo natural $n \geq a$ se e só se as duas condições a seguir forem satisfeitas:

(i) $P(a)$ é verdadeira;
(ii) $P(k)$ verdadeira $\Longrightarrow P(k+1)$ verdadeira.

Exemplo 2.1.2 (OBM) Para cada número inteiro $n > 2$, mostre que existem n naturais dois a dois distintos, tais que a soma de seus inversos é igual a 1.

Prova. Façamos indução sobre $n \geq 3$. Para verificar o caso inicial, basta notar que

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1.$$

Agora, suponhamos, por hipótese de indução, que para certo $k \geq 3$ natural existam naturais $x_1 < x_2 < \cdots < x_k$ tais que

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = 1.$$

Multiplicando ambos os membros da igualdade acima por ½ e somando ½ a ambos os membros da igualdade resultante, obtemos então

$$\frac{1}{2} + \frac{1}{2x_1} + \frac{1}{2x_2} + \cdots + \frac{1}{2x_k} = 1.$$

Agora, como $2 < 2x_1 < 2x_2 < \cdots < 2x_k$, obtivemos $k+1$ naturais dois a dois distintos com soma dos inversos igual a 1, completando assim nossa prova por indução.

■

2.2 Segundo Princípio de Indução Finita

Existe outra forma importante de indução, o segundo princípio de indução também chamado de princípio de indução forte ou princípio de indução completa.

Este método consiste em considerar um subconjunto A de $\mathbb{N}$ tal que $1 \in A$ e para $k \in \mathbb{N}$, suponhamos que se $\{1, \dots, k\}$ é um subconjunto de A, então $k+1 \in A$. Como, $1 \in A$ temos que $\{1\} \subset A$ e, portanto $2 \in A$. Sendo assim, $\{1,2\} \subset A$ e então, $3 \in A$ e assim por diante. Podemos concluir então que A contém todos os números naturais e, portanto, $A = \mathbb{N}$. Essa ideia está formalizada no seguinte axioma.

Axioma 2.2.1 (Segundo Princípio de Indução Finita). Seja A um subconjunto de $\mathbb{N}$ tal que:

(i) $1 \in A$.
(ii) Se $\{1, \dots, k\} \subset A$, então $k+1 \in A$.

Então $A = \mathbb{N}$.

Dada uma propriedade $P(n)$ do natural n, cuja veracidade desejamos provar para todo $n \in \mathbb{N}$. A aplicação do axioma 2.2.1 como ferramenta de demonstração consiste em definir o conjunto A como $A = \{k \in \mathbb{N} \mid P(k) \text{ é verdeira}\}$ e observando que

$$A = \mathbb{N} \Leftrightarrow P(n) \text{ é verdadeira para todo } n \in \mathbb{N},$$

vemos que, para demonstrarmos que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, basta mostrarmos que $A = \mathbb{N}$, ou seja, pelo segundo princípio de indução, que

(i) $1 \in A$;
(ii) $\{1, \dots, k\} \subset A \Longrightarrow k+1 \in A$.

E pela definição de A, mostrar os dois itens acima equivale a mostrar que

(i) $P(1)$ é verdadeira;

(ii) $P(1), \ldots, P(k)$ verdadeiras $\Longrightarrow P(k+1)$ verdadeira.

Podemos então estabelecer a seguinte proposição.

Proposição 2.2.1 Dada uma propriedade $P(n)$ do natural n, temos $P(n)$ verdadeira para todo $n \in \mathbb{N}$ se e só se as duas condições a seguir forem satisfeitas:

(i) $P(1)$ é verdadeira;
(ii) $P(1), \ldots, P(k)$ verdadeiras $\Longrightarrow P(k+1)$ verdadeira.

Exemplo 2.2.1 Considere a sequência $a_1 = 1$, $a_2 = 3$ e $a_n = a_{n-1} + a_{n-2}$, para $n \geq 3$. Prove que $a_n < \left(\frac{7}{4}\right)^n$, para todo $n \geq 1$.

Prova. Considere a propriedade $P(n)$: $a_n < \left(\frac{7}{4}\right)^n$. Note que $P(1)$ e $P(2)$ são verdadeiras, pois

$$a_1 = 1 < \frac{7}{4} = \left(\frac{7}{4}\right)^1 \text{ e } a_2 = 3 < \frac{49}{16} = \left(\frac{7}{4}\right)^2.$$

Agora, suponhamos $P(n)$ válida para todo $n = 1, 2, \ldots, k$. com $k \geq 2$. Desse modo, segue que

$$a_{k+1} = a_k + a_{k-1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1}$$

$$= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right)$$

$$= \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right)$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2$$

$$= \left(\frac{7}{4}\right)^{k+1}.$$

Logo, $P(k+1)$ é verdadeira. Portanto, pela proposição 2.2.1, temos $P(n)$ verdadeira para todo $n \in \mathbb{N}$.

■

2.2.1 Forma geral do segundo princípio de indução finita

Uma forma mais geral do segundo princípio de indução é o seguinte axioma.

Axioma 2.2.2. Seja $a \in \mathbb{N}$ e A um subconjunto de $\{a, a+1, a+2, \dots\}$ tal que:

(i) $a \in A$.
(ii) Se $\{a, a+1, a+2, \dots, k\} \subset A$, então $k+1 \in A$.

Então $A = \{a, a+1, a+2, \dots\}$.

Dada uma propriedade $P(n)$ do natural n, cuja veracidade desejamos provar para todo natural $n \geq a$. Analogamente ao axioma 2.2.1, a aplicação do axioma 2.2.2 como método de demonstração consiste em definir o subconjunto A como $A = \{k \in \mathbb{N} | \ P(k) \text{ é verdeira}\}$ e observar que

$$A = \{a, a+1, a+2, \dots\} \Leftrightarrow P(n) \text{ é verdadeira para todo } n \geq a \text{ natural.}$$

Assim, podemos estabelecer uma forma mais geral para a proposição 2.2.1 como a seguir.

Proposição 2.2.2 Dados $a \in \mathbb{N}$ e uma propriedade $P(n)$ do natural n, temos $P(n)$ verdadeira para todo natural $n \geq a$ se e só se as duas condições a seguir forem satisfeitas:

(i) $P(a)$ é verdadeira;
(ii) $P(a), P(a+1), \dots, P(k)$ verdadeiras $\Longrightarrow P(k+1)$ verdadeira.

Exemplo 2.2.2 Considere a sequência $a_1 = 2$, $a_2 = 3$ e $a_n = a_{n-1} + a_{n-2}$, para $n \geq 3$. Prove que $a_n < \left(\frac{17}{10}\right)^n$, para todo $n \geq 4$.

Prova. Considere a propriedade $P(n) : a_n < \left(\frac{17}{10}\right)^n$, para todo $n \geq 4$. Observe que $P(4)$ e $P(5)$ são verdadeiras, pois

$$a_4 = 8 < \frac{83521}{10000} = \left(\frac{17}{10}\right)^4 \text{ e } a_5 = 13 < \frac{1419857}{100000} = \left(\frac{17}{10}\right)^5.$$

Agora, suponhamos $P(n)$ válida para todo $n = 4, \ldots, k$. com $k \geq 5$. Desse Modo, segue que

$$a_{k+1} = a_k + a_{k-1} < \left(\frac{17}{10}\right)^k + \left(\frac{17}{10}\right)^{k-1}$$

$$= \left(\frac{17}{10}\right)^{k-1}\left(\frac{17}{10} + 1\right)$$

$$= \left(\frac{17}{10}\right)^{k-1}\left(\frac{27}{10}\right)$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(\frac{17}{10}\right)^2$$

$$= \left(\frac{17}{10}\right)^{k+1}.$$

Logo, $P(k+1)$ é verdadeira. Portanto, pela proposição 2.2.2, temos $P(n)$ verdadeira para todo $n \geq 4$.

■

2.3 Princípio da Boa Ordenação

O Princípio da Boa Ordenação (PBO) é um recurso muito útil na prova de resultados em matemática. Um fato interessante é que o PBO, o primeiro princípio de indução e o segundo princípio de indução finita são equivalentes. A seguir, provaremos o PBO partindo do primeiro princípio de indução, o segundo princípio de indução a partir do PBO e o primeiro princípio de indução a partir do segundo princípio de indução, seguindo Lima [2].

Teorema 2.3.1 (PBO) Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

Prova. Sejam A um subconjunto de $\mathbb{N}$ que não possui um menor elemento e X o conjunto

$$X = \{n \in \mathbb{N} \mid I_n \cap A = \emptyset\},$$

onde $I_n = \{p \in \mathbb{N} \mid 1 \leq p \leq n\}$, ou seja, $I_n = \{1, \ldots, n\}$.

Note que $1 \in X$, pois do contrário $I_1 \cap A \neq \emptyset$, isto é, $\{1\} \cap A \neq \emptyset$, então $1 \in A$ e, portanto, A teria um menor elemento, o que é uma contradição já que A é um subconjunto de $\mathbb{N}$ que não possui um menor elemento.

Agora, se $k \in X$, então $I_k \cap A = \emptyset$, isto é, $1, \ldots, k \notin A$. Se $k + 1 \in A$, então $k + 1$ seria o menor elemento de A, novamente uma contradição, deste modo $k + 1 \notin A$. Sendo assim, $1, \ldots, k, k + 1 \notin A$, isto é, $I_{k+1} \cap A = \emptyset$, logo $k + 1 \in X$ e então, pelo axioma 2.1.1, temos que $X = \mathbb{N}$. Consequentemente $A = \emptyset$. Portanto, todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

■

Teorema 2.3.2 PBO $\Longrightarrow$ Segundo Princípio de Indução Finita.

Prova. Seja A um subconjunto de $\mathbb{N}$ tal que:

(i) $1 \in A$.
(ii) Se $\{1, \ldots, k\} \subset A$, então $k + 1 \in A$.

Se $A \neq \mathbb{N}$, então o conjunto $X = \mathbb{N} - A$ é um subconjunto não vazio de $\mathbb{N}$. Daí, pelo PBO, X possui um menor elemento, digamos x. Assim, todos os números naturais menores do que x pertencem a A. Logo, por (ii), tem-se $x \in A$, o que é uma contradição. Portanto $A = \mathbb{N}$.

■

Teorema 2.3.3 Segundo Princípio de Indução Finita $\Longrightarrow$ Primeiro Princípio de Indução Finita.

Prova. Seja A um subconjunto de $\mathbb{N}$ tal que:

(i) $1 \in A$;
(ii) Se $k \in A$, então $k + 1 \in A$.

Suponhamos que $\{1, \dots, k\} \subset A$, então $k \in A$. Logo, por (ii), segue que $k + 1 \in A$. Portanto, pelo segundo princípio de indução finita, $A = \mathbb{N}$.

■

3 FUNDAMENTOS DE TEORIA DOS NÚMEROS.

Abordaremos nesse capitulo algumas definições e resultados sobre o conjunto dos números inteiros $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, onde o subconjunto $\{1, 2, 3, \dots\}$ é chamado conjunto dos inteiros positivos e $\{0, 1, 2, 3, \dots\}$ é dito conjunto dos inteiros não negativos.

3.1 Divisibilidade

A noção de divisibilidade é fundamental em teoria dos números, pois é o objeto de vários resultados importantes. Iniciamos com as definições abaixo que seguem Muniz Neto [3].

Definição 3.1.1 Dados $a, b \in \mathbb{Z}$, $a \neq 0$, dizemos que a **divide** b, e escrevemos $a|b$, se existir $c \in \mathbb{Z}$ tal que $b = ac$. Caso a não divida b, escrevemos $a \nmid b$.

Definição 3.1.2 Seja a um inteiro não nulo. Se a **divide** b, dizemos que a é um **divisor** de b, que b é **divisível** por a ou ainda que b é um **múltiplo** de a. Se a divide b e $a > 0$, então a é um **divisor positivo** de b.

Proposição 3.1.1 Sejam a, b e c, inteiros positivos e x, y inteiros quaisquer.

(i) Se $a|b$, então $a \leq b$.
(ii) Se $a|b$ e $b|a$, então $a = b$.
(iii) Se $a|b$ e $a|c$, então $a|(bx + cy)$.
(iv) Se $a|b$ e $b|c$, então $a|c$.

Prova.

(i) Se $a|b$, então $b = am$, com $m \in \mathbb{Z}$. Como $a, b > 0$, segue que $m > 0$. Logo $m \geq 1$. Então, $am \geq a$ e como $am = b$, segue que $a \leq b$.

(ii) Se $a|b$ e $b|a$, temos, pela proposição 3.1.1 (i), que $a \leq b$ e $b \leq a$. Portanto, $a = b$.

(iii) Se $a|b$ e $a|c$, então existem $m, n \in \mathbb{Z}$ tais que $b = am$ e $c = an$, então

$$bx + cy = (am)x + (an)y = a(mx) + a(ny) = a(mx + ny),$$

Como $(mx + ny) \in \mathbb{Z}$, temos que $a|(bx + cy)$.

(iv) Se $a|b$ e $b|c$, então existem $m, n \in \mathbb{Z}$ tais que $b = ma$ e $c = nb$, logo $c = n(ma)$, então $c = (nm)a$ e, portanto $a|c$.

■

Proposição 3.1.2 Sejam $a, b_1, \dots, b_n$ números inteiros e positivos, tais que $a \mid b_1, \dots, b_n$, então $a \mid (b_1x_1 + \cdots + b_nx_n)$ para todos $x_1, \dots, x_n \in \mathbb{Z}$.

Prova. Se $n = 1$, o resultado segue da proposição 3.1.1 (iii), para $b = b_1$, $x = x_1$ e $y = 0$. Se $n = 2$, o resultado segue da proposição 3.1.1 (iii), para $b = b_1$, $c = b_2$, $x = x_1$ e $y = x_2$.

Agora, suponhamos o resultado válido para $n = k$. Se $a \mid b_1, \dots, b_k, b_{k+1}$, temos que $a \mid b_1, \dots, b_k$. Assim, por hipótese de indução, $a \mid (b_1x_1 + \cdots + b_kx_k)$ para todos $x_1, \dots, x_k \in \mathbb{Z}$. Como $a \mid b_{k+1}$, temos, pela proposição 3.1.1 (iii), que

$$a \mid [1 \cdot (b_1x_1 + \cdots + b_kx_k) + b_{k+1}x_{k+1}] \Longrightarrow a \mid (b_1x_1 + \cdots + +b_kx_k + b_{k+1}x_{k+1})$$

para todos $x_1, \dots, x_k, x_{k+1} \in \mathbb{Z}$. Logo, o resultado vale para $n = k + 1$. Assim, pela proposição 2.1.2, temos que $a \mid (b_1x_1 + \cdots + b_nx_n)$ para todos $x_1, \dots, x_n \in \mathbb{Z}$.

■

Exemplo 3.1.1 Se a e b são inteiros positivos, tais que

$$\frac{1}{a}+\frac{1}{b}\in\mathbb{Z},$$

prove que $a=b=1$ ou 2.

Prova. Seja $k\in\mathbb{Z}$ tal que

$$\frac{1}{a}+\frac{1}{b}=k.$$

Logo,

$$\frac{1}{a}+\frac{1}{b}=k\Longrightarrow\frac{a+b}{ab}=k\Longrightarrow a+b=abk\Longrightarrow b=abk-a\Longrightarrow b=a(bk-1)\Longrightarrow a|b.$$

Analogamente, $b|a$. Portanto, pela proposição 3.1.1 (ii), segue que $a=b$. Assim sendo, temos

$$\frac{1}{a}+\frac{1}{a}=k\Longrightarrow\frac{2}{a}=k\Longrightarrow ka=2\Longrightarrow a|2\Longrightarrow a=1 \text{ ou } a=2.$$

■

3.2 Algoritmo da Divisão

Sejam $a,b\in\mathbb{Z}, b\neq 0$. Se $b|a$, então $a=bq, q\in\mathbb{Z}$. Porém, se $b\nmid a$, qual a relação entre a e b? A proposição a seguir, conhecida como algoritmo da divisão, responderá isso.

Proposição 3.2.1 (Algoritmo da Divisão) Dados $a,b\in\mathbb{Z}$, com $b>0$, existem únicos $q,r\in\mathbb{Z}$ tais que $a=bq+r$, com $0\leq r<b$.

Prova. Seja q o maior número inteiro tal que $bq\leq a$. Então $bq\leq a<b(q+1)$, de modo que $0\leq a-bq<b$, e assim, $r=a-bq$ é tal que $a=bq+r$, com $0\leq r<b$.

Agora, supondo $a=bq+r=bq'+r'$, onde $q,q',r,r'\in\mathbb{Z}$ e $0\leq r,r'<b$, temos que $r-r'=b(q'-q)$. Supondo, sem perda de generalidade, $r\geq r'$, temos $0\leq r-r'<b$ e

assim, $0 \leq b(q' - q) < b$ e como $b > 0$, tem-se, $0 \leq (q' - q) < 1$, então $q' - q = 0$, ou seja, $q = q'$. Desse modo, $r - r' = b(q' - q) = b \cdot 0 = 0$ e, portanto $r = r'$.

■

Definição 3.3.1 Os inteiros q e r, obtidos na proposição 3.2.1, são chamados, respectivamente, de quociente e de resto da divisão de a por b.

Proposição 3.2.2 Sejam a, b e n inteiros, com $n > 0$. Se a e b possuem restos iguais na divisão por n, então $n|(a - b)$.

Prova. Se a e b possuem restos iguais na divisão por n, então, pela proposição 3.2.1, segue que $a = nq + r$ e $b = nq' + r$, com $q, q' \in \mathbb{Z}$. Logo $a - b = n(q - q')$, ou seja, $n|(a - b)$ já que $(q - q') \in \mathbb{Z}$.

■

3.3 Máximo Divisor Comum

Definição 3.3.2 O máximo divisor comum de dois números inteiros e positivos a e b, denotado por $mdc(a, b)$, é o maior inteiro que divide a e b.

Definição 3.3.3 Dois inteiros positivos a e b são ditos primos entre si, ou relativamente primos, se $mdc(a, b) = 1$.

Proposição 3.3.1 Para todo inteiro positivo n, temos que $mdc(n, n + 1) = 1$.

Prova. Seja $d = mdc(n, n + 1)$, logo, pela definição 3.3.2, temos que $d \geq 1$, $d|n$ e $d|(n + 1)$. Assim, pela proposição 3.1.1 (iii), temos que $d|(n + 1 - n)$, ou seja, $d|1$. Daí, pela proposição 3.1.1 (i), segue que $d \leq 1$ e, portanto $d = 1$.

■

Teorema 3.3.1 Sejam a e b números inteiros e positivos, então existem inteiros x e y tais que

$$mdc(a, b) = ax + by.$$

Prova. Seja $S = \{am + bn \mid am + bn > 0; m, n \in \mathbb{Z}\}$, um subconjunto não vazio de $\mathbb{N}$, já que $a \cdot 1 + b \cdot 0 = a \in S$. Deste modo, pelo PBO, S possui um menor elemento $c = ax + by$ e pelo algoritmo da divisão, existem inteiros q e r tais que $a = qc + r$, com $0 \leq r < c$. Então

$$r = a - qc = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Se $r > 0$, então $r \in S$, pois $1 - qx, -qy \in \mathbb{Z}$, o que é uma contradição, pois $r < c$ e c é o menor elemento de S. Portanto, $r = 0$ e assim, $a = qc$, ou seja $c|a$. De maneira análoga, $c|b$.

Agora, seja $d = mdc(a, b)$, então $d|a$ e $d|b$, daí, $a = hd$ e $b = kd$, com $h, k \in \mathbb{Z}$. Logo

$$c = ax + by = hdx + kdy = d(hx + ky) \Longrightarrow d|c.$$

Daí, pela proposição 3.1.1 (i), $d \leq c$ e como $c|a$, $c|b$ e d é o maior inteiro que divide a e b, só nos resta $d = c$, isto é, $mdc(a, b) = ax + by$.

■

Proposição 3.3.2 Sejam a, b e c inteiros positivos. Se $a|bc$ e $mdc\ (a, b) = 1$, então $a|c$.

Prova. Como $mdc(a, b) = 1$, pelo teorema 3.3.1, existem inteiros x e y tais que $ax + by = 1$, logo $acx + bcy = c$. Como $a|a$ e $a|bc$, temos, pela proposição 3.1.1 (iii), que $a|(acx + bcy)$, ou seja, $a|c$.

■

3.4 Números Primos

Definição 3.4.1 Um inteiro $p > 1$ é chamado de número primo, ou simplesmente primo, se seus únicos divisores positivos são 1 e p, um inteiro $n > 1$ que não é primo é denominado composto.

Proposição 3.4.1 Sejam p e q primos e a e b inteiros positivos quaisquer.

(i) Se $p|q$, então $p = q$.

(ii) Se $p \nmid a$, então $mdc(p, a) = 1$.
(iii) Se $p|ab$, então $p|a$ ou $p|b$.

Prova.

(i) Se $p|q$, então $p = 1$ ou $p = q$, pois q é primo. Sendo p primo, temos $p > 1$. Logo, $p = q$.

(ii) Sendo p primo, seus únicos divisores positivos são 1 e p. De tal modo, $mdc(p, a) = 1$ ou $mdc(p, a) = p$. Como $p \nmid a$, não podemos ter $mdc(p, a) = p$, portanto $mdc(p, a) = 1$.

(iii) Por hipótese, p é primo. Se $p \nmid a$, pela proposição 3.4.1 (ii), temos que $mdc(p, a) = 1$ e como $p|ab$, pela proposição 3.3.2, segue que $p|b$.

■

Proposição 3.4.2 Sejam $p, p_1, \dots, p_n$ números primos e $a_1, \dots, a_n$ inteiros positivos quaisquer, para todo inteiro $n \geq 2$.

(i) Se $p|a_1 \cdots a_n$, então $p|a_i$ para algum $i = 1,2, \cdots, n$.
(ii) Se $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1,2, \cdots, n$.

Prova.

(i) Façamos indução sobre $n \geq 2$, sendo o caso $n = 2$ verdadeiro pela proposição 3.4.1(iii).

Agora, suponhamos o resultado válido para $n = k$. Se $p|a_1 \cdots a_k a_{k+1}$, segue que $p|(a_1 \cdots a_k)a_{k+1}$. Como p é primo, pela proposição 3.4.1(iii), temos que $p|a_1 \cdots a_k$ ou $p|a_{k+1}$. Pela hipótese de indução, se $p|a_1 \cdots a_k$, então $p|a_i$ para algum $i = 1,2, \cdots, k$. Caso contrário $p|a_{k+1}$. Daí, temos que $p|a_i$ para algum $i = 1,2, \cdots, k, k+1$. Portanto, pela proposição 2.1.2, segue o resultado.

(ii) Se p é primo e $p|p_1 \cdots p_n$, então, pela proposição 3.4.2 (i), $p|p_i$ para algum $i = 1,2, \cdots, n$. Como p_i é primo, pela proposição 3.4.1(i), temos que $p = p_i$ para algum $i = 1,2, \cdots, n$.

■

Proposição 3.4.3 Se um inteiro $n > 1$ é composto, então existem $a, b \in \mathbb{Z}$ tais que $n = ab$, com $1 < a, b < n$.

Prova. Se n é composto, então existe um inteiro positivo a, diferente de 1 e n, tal que $a|n$. Pela proposição 3.1.1 (i), temos que $1 < a < n$. Mas, se $a|n$, então existe um inteiro positivo b tal que $n = ab$. Se $b = 1$ ou $b = n$, então $a = n$ ou $a = 1$, que contradiz $1 < a < n$. Assim, segue que $1 < b < n$.

■

Teorema 3.4.1 (Teorema Fundamental da Aritmética) Todo número inteiro $n > 1$ se escreve de modo único como um produto

$$n = p_1 \cdots p_r$$

onde $r \geq 1$ é um inteiro e $p_1 \leq \cdots \leq p_r$ são primos.

Prova. Façamos indução completa sobre $n \geq 2$, sendo o caso $n = 2$ válido, pois para $r = 1$ e $p_1 = 2$ temos uma e única escrita.

Agora, suponhamos o resultado válido para todo inteiro menor do que n e provemos que vale para n. Se n é primo, então $r = 1$ e $p_1 = n$ garantem a escrita e de modo único. Se n é composto, pela proposição 3.4.3, temos $n = ab$, com $a, b \in \mathbb{Z}$ e $1 < a, b < n$. Pela hipótese de indução, podemos escrever

$$a = p_1 \cdots p_k \text{ e } b = q_1 \cdots q_l,$$

onde $1 \leq k, l \in \mathbb{Z}$, $p_1 \leq \cdots \leq p_k$ e $q_1 \leq \cdots \leq q_l$ são primos. Portanto, $n = p_1 \cdots p_k q_1 \cdots q_l$ e ordenando esses $r = k + l$ primos em ordem crescente, obtemos a escrita.

Suponhamos agora, que $n = p_1 \cdots p_r = q_1 \cdots q_s$, com $1 < r, s \in \mathbb{Z}$, $p_1 \leq \cdots \leq p_r$ e $q_1 \leq \cdots \leq q_s$ primos. Logo, $p_1 | q_1 \cdots q_s$ e pela proposição 3.4.2 (ii), tem-se $p_1 = q_i$ para algum $i = 1,2, \cdots, s$. Como $q_1 \leq \cdots \leq q_s$, temos $p_1 \geq q_1$. Analogamente temos $q_1 \geq p_1$, de modo que $p_1 = q_1$. Então, $p_2 \cdots p_r = q_2 \cdots q_s$. Como $p_2 \cdots p_r < n$, por hipótese de indução, temos $r = s$ e $p_i = q_i$ para todo $i = 2, \cdots, s$.

■

Agrupando em potências os números primos repetidos que figuram na escrita única, apresentada no teorema fundamental da aritmética, temos

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

onde $k, \alpha_1, \ldots, \alpha_k \geq 1$ são inteiros e $p_1 < \cdots < p_k$ são primos. Essa representação de um inteiro $n > 1$ como um produto de potências de primos distintos é dita sua fatoração ou decomposição canônica em fatores primos.

Proposição 3.4.4 Sejam p_1 e p_2 primos distintos e $\alpha_1, \alpha_2 \geq 1$ inteiros quaisquer. Então

$$mdc\left(p_1^{\alpha_1}, p_2^{\alpha_2}\right) = 1.$$

Prova. Seja $d = mdc\left(p_1^{\alpha_1}, p_2^{\alpha_2}\right)$. Se $d > 1$, pelo teorema fundamental da aritmética, existe um primo q tal que $q|d$. Como $d|p_1^{\alpha_1}$ e $d|p_2^{\alpha_2}$ temos, pela proposição 3.1.1 (iv), que $q|p_1^{\alpha_1}$ e $q|p_2^{\alpha_2}$ e então, pela proposição 3.4.2 (ii), temos $q = p_1$ e $q = p_2$, de modo que $p_1 = p_2$, o que é uma contradição, pois por hipótese, temos $p_1 \neq p_2$. Logo, $d = 1$ e, portanto $mdc\left(p_1^{\alpha_1}, p_2^{\alpha_2}\right) = 1$.

■

Proposição 3.4.5 Seja $n = p_1^{b_1} \cdots p_k^{b_k}$ a decomposição canônica do inteiro $n > 1$ e d um inteiro positivo. Então

$$d|n \Leftrightarrow d = p_1^{a_1} \cdots p_k^{a_k}, \text{ com } 0 \leq a_i \leq b_i, \text{ para todo } i = 1, \cdots, k.$$

Prova. Seja d um inteiro positivo que divide n. Se $d = 1$, então $d = p_1^{a_1} \cdots p_k^{a_k}$, com $a_i = 0$ para todo $i = 1, \cdots, k$.

Se $d > 1$, então, pelo teorema fundamental da aritmética, existe um número primo p tal que $p|d$. Como $d|n$, pela proposição 3.1.1 (iv), temos que $p|n$, ou seja, $p|p_1^{b_1} \cdots p_k^{b_k}$. Daí, pela proposição 3.4.2 (i), $p|p_i^{b_i}$ para algum $i = 1, \cdots, k$. Logo, pela proposição 3.4.2 (ii), temos $p = p_i$ para algum $i = 1, \cdots, k$. Logo, os fatores primos de d pertencem ao conjunto $\{p_1, \ldots, p_k\}$,

podendo ocorrer que $p_i \nmid d$ para um ou mais valores de $i = 1, \cdots, k$. Portanto, $d = p_1^{a_1} \cdots p_k^{a_k}$, com $a_i \geq 0$ para todo $i = 1, \cdots, k$.

Agora, seja $p_i^{a_i}$ para algum $i = 1, \cdots, k$. Se $a_i = 0$, temos que $a_i \leq b_i$, pois $b_i \geq 1$ para todo $i = 1, \cdots, k$. Portanto, temos $d = p_1^{a_1} \cdots p_k^{a_k}$, com $0 \leq a_i \leq b_i$, para todo $i = 1, \cdots, k$ tal que $a_i = 0$.

Agora, suponhamos $a_i > 0$. Como $p_i^{a_i} | d$ e $d | n$, pela proposição 3.1.1 (iv), decorre que $p_i^{a_i} | p_1^{b_1} \cdots p_k^{b_k}$. Mas, pela proposição 3.4.5, $mdc\left(p_i^{a_i}, p_l^{b_l}\right) = 1$ para todo $i \neq l$. Logo, pela proposição 3.3.2, segue que $p_i^{a_i} | p_i^{b_i}$. Daí, pela proposição 3.1.1 (i), temos que $p_i^{a_i} \leq p_i^{b_i}$ e assim $a_i \leq b_i$. Portanto, $d = p_1^{a_1} \cdots p_k^{a_k}$, com $0 \leq a_i \leq b_i$, para todo $i = 1, \cdots, k$.

Reciprocamente, seja $m = p_1^{c_1} \cdots p_k^{c_k}$, com $c_i = b_i - a_i$ para todo $i = 1, \cdots, k$. Como $0 \leq a_i \leq b_i$, temos que $c_i = b_i - a_i \geq 0$ para todo $i = 1, \cdots, k$. Dessa forma, temos que $m \in \mathbb{Z}$ e $n = md$, ou seja, $d | n$.

■

4 COMBINATÓRIA APLICADA À TEORIA DO NÚMEROS

Neste capitulo abordaremos alguns conceitos, métodos e princípios combinatórios que permitem a contagem de determinados subconjuntos de um conjunto finito, sem a explícita necessidade de listá-los, ou que assegurem a existência de determinados subconjuntos, também, sem a explícita necessidade de exibi-los, exemplificando suas aplicações na teoria dos números.

4.1 Princípio Bijetivo

Contar é uma das ações primitivas do ser humano, por exemplo, existem indícios históricos que os pastores de ovelhas contavam os rebanhos utilizando pedrinhas, separando em uma bolsa uma pedrinha para cada ovelha que era solta para pastar. No retorno dos animais, o pastor retirava da bolsa uma pedra para cada ovelha que retornava. Dessa forma, se sobrassem pedrinhas na bolsa, o pastor saberia que perdeu ovelhas, se faltassem pedrinhas, ele saberia que outras ovelhas se juntaram ao rebanho.

Em linguagem matemática moderna, a correspondência feita pelo pastor de ovelhas ao separar uma pedrinha para cada ovelha é dita uma bijeção entre conjuntos, que é um tipo de função. Conforme Muniz Neto [4], dados dois conjuntos não vazios X e Y, informalmente, uma função f de X em Y é uma regra que associa a cada $x \in X$ um único $y \in Y$. Escrevemos $f: X \longrightarrow Y$ para denotar que f é uma função de Xem Y. Nesse caso, o elemento $y \in Y$ associado a $x \in X$ por f é denotado por $y = f(x)$.

As seguintes definições e resultados são fundamentais para o desenvolvimento dos princípios de enumeração combinatória.

Definição 4.1.1 [4] Uma função $f: X \longrightarrow Y$ é dita:

(a) **Injetora**, ou **injetiva** ou, ainda, uma **injeção**, se, para todo $y \in Y$, existir no máximo um $x \in X$ tal que $f(x) = y$.

(b) **Sobrejetora**, ou **sobrejetiva** ou, ainda, uma **sobrejeção**, se, para todo $y \in Y$, existir pelo menos um $x \in X$, tal que $y = f(x)$.

(c) **Bijetora**, ou **bijetiva** ou, ainda, uma **bijeção**, se for ao mesmo tempo injetora e sobrejetora.

Definição 4.1.2 [4] Dadas as funções $f: X \longrightarrow Y$ e $g: Y \longrightarrow Z$, a **função composta** de f e g (nessa ordem) é a função $g \circ f: X \longrightarrow Z$ definida, para cada $x \in X$, por $(g \circ f)(x) = g(f(x))$.

Proposição 4.1.1 [4] Sejam $f: X \longrightarrow Y$ e $g: Y \longrightarrow Z$ funções dadas. Se g e f são bijetoras, então $g \circ f$ é bijetora.

Definição 4.1.3 [4] Seja $f: X \longrightarrow Y$ uma bijeção. A função inversa de f é a função $f^{-1}: Y \longrightarrow X$ tal que, para $x \in X$, $y \in Y$, temos $f^{-1}(y) = x \Leftrightarrow y = f(x)$.

Proposição 4.1.2 Conforme Lima [5], uma função $f: X \longrightarrow Y$ possui inversa se, e somente se, é uma bijeção.

Definição 4.1.1 [5] Denotaremos por I_n o conjunto $\{1, \ldots, n\}$ dos números naturais de 1 até n,

mais precisamente, dado $n \in \mathbb{N}$, temos $I_n = \{p \in \mathbb{N} \mid 1 \leq p \leq n\}$.

Definição 4.1.2 [5] Um conjunto A é finito quando é vazio ou quando existe, para algum $n \in \mathbb{N}$, uma bijeção

$$f: I_n \longrightarrow A.$$

No primeiro caso, diremos que A possui zero elementos. No segundo caso, diremos que $n \in \mathbb{N}$ é o número de elementos de A, ou seja, que A possui n elementos.

Denotaremos por $|A|$ o número de elementos de um conjunto finito. Agora, temos bagagem suficiente para enunciar e provar o princípio bijetivo, seguindo Muniz Neto [6].

Proposição 4.1.3 (Princípio Bijetivo) Se A e B são conjuntos finitos e não vazios, então

$$|A| = |B| \text{ se e só se existe uma bijeção } f: A \longrightarrow B.$$

Prova. Suponhamos que $|A| = |B| = n$, então, pela definição 4.1.2, existem bijeções

$$g: I_n \longrightarrow A \text{ e } h: I_n \longrightarrow B.$$

Logo, pelas proposições 4.1.2 e 4.1.1, a função $f = h \circ g^{-1}: A \longrightarrow B$ é uma bijeção de A em B.

Reciprocamente, suponhamos que exista uma bijeção $f: A \longrightarrow B$. Se $|A| = n$, existe uma bijeção $g: I_n \longrightarrow A$. Daí, $f \circ g: I_n \longrightarrow B$ também é bijeção, de modo que $|B| = n$ e, portanto $|A| = |B|$.

■

4.2 Princípio Aditivo

Uma consequência do princípio bijetivo é o princípio aditivo da contagem, que nos diz como contar o número de elementos da união de dois conjuntos finitos e disjuntos, ou seja, conjuntos cuja interseção é vazia.

Proposição 4.2.1 (Princípio Aditivo) Se A e B são conjuntos finitos, disjuntos e não vazios, Então

$$|A \cup B| = |A| + |B|.$$

Prova. Sejam A e B conjuntos finitos e não vazios com $|A| = m$, $|B| = n$ e bijeções

$$g: I_m \longrightarrow A \text{ e } h: I_n \longrightarrow B.$$

Consideremos a função $f: I_{m+n} \longrightarrow A \cup B$, dada por $f(x) = g(x)$, se $1 \leq x \leq m$ e $f(m + x) = h(x)$, se $1 \leq x \leq n$. Como $A \cap B = \emptyset$, f é uma bijeção e, pelo princípio bijetivo, segue que

$$|A \cup B| = |I_{m+n}| = m + n = |A| + |B|.$$

■

4.2.1 Extensão do princípio aditivo

Podemos generalizar o princípio aditivo da contagem para n conjuntos finitos e dois a dois disjuntos, como na proposição a seguir.

Proposição 4.2.2 Sejam $A_1, \ldots, A_n$ conjuntos finitos tais que $A_i \cap A_j = \emptyset$, para todo $i \neq j$, então

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

Prova. Façamos indução sobre $n \geq 2$, sendo o caso $n = 2$ válido pela proposição 4.2.1. Agora, suponhamos, por hipótese de indução, que

$$\left|\bigcup_{i=1}^{k} A_i\right| = \sum_{i=1}^{k} |A_i|,$$

para todo $k \in \mathbb{N}$ tal que $2 \leq k \leq n - 1$. Agora, como

$$\bigcup_{i=1}^{n} A_i = \left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n,$$

que é uma união disjunta, pois $A_i \cap A_j = \emptyset$ para todo $i \neq j$, segue, pela proposição 4.2.1, que

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n|,$$

e por hipótese de indução, temos que

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left(\sum_{i=1}^{n-1} |A_i|\right) + |A_n|,$$

e portanto

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

■

4.3 Princípio Fundamental da Contagem

Uma consequência do princípio aditivo é o princípio multiplicativo ou fundamental da contagem (PFC), que nos diz como contar o número de elementos do produto cartesiano de dois conjuntos finitos e não vazios.

Definição 4.3.1 Dados A e B conjuntos finitos e não vazios, seu produto cartesiano é o conjunto $A \times B$, formado por todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$, isto é,

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Proposição 4.3.1 (PFC) Se A e B são conjuntos finitos e não vazios, então

$$|A \times B| = |A| \cdot |B|.$$

Prova. Seja $B = \{b_1, \dots, b_n\}$, para algum $n \in \mathbb{N}$, ou seja,

$$B = \bigcup_{i=1}^{n} \{b_i\}.$$

Logo

$$A \times B = A \times \left(\bigcup_{i=1}^{n} \{b_i\} \right) = \bigcup_{i=1}^{n} (A \times \{b_i\}),$$

que é uma união disjunta, e assim, pela proposição 4.2.2, temos

$$|A \times B| = \left| \bigcup_{i=1}^{n} (A \times \{b_i\}) \right| = \sum_{i=1}^{n} |A \times \{b_i\}|.$$

No entanto $|A \times \{b_i\}| = |A|$ para todo $i = 1,2, \cdots, n$. Portanto,

$$|A \times B| = \sum_{i=1}^{n} |A \times \{b_i\}| = \sum_{i=1}^{n} |A| = |A| \cdot n = |A| \cdot |B|.$$

■

4.3.1 Extensão do princípio fundamental da contagem

Definição 4.3.2 Dados $A_1, A_2, \dots, A_n$ conjuntos finitos e não vazios, seu produto cartesiano é o conjunto $A_1 \times A_2 \times \cdots \times A_n$, formado por todas as n-uplas $(a_1, a_2, \dots, a_n)$, tais que $a_1 \in A_1$, $a_2 \in A_2, \dots, a_n \in A_n$. Isto é,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) | a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Proposição 4.3.2 (Extensão do PFC) Se $A_1, \dots, A_n$ são conjuntos finitos e não vazios, então

$$|A_1 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

Prova. Façamos indução sobre $n \geq 2$, sendo o caso $n = 2$ válido pela proposição 4.3.1. Agora, suponhamos, por hipótese de indução, que

$$|A_1 \times \cdots \times A_k| = \prod_{j=1}^{k} |A_j|,$$

para todo $k \in \mathbb{N}$ tal que $2 \leq k \leq n-1$ e seja $A_n = \{a_1, \ldots, a_m\}$, $m \in \mathbb{N}$. Segue que

$$A_n = \bigcup_{i=1}^{m} \{a_i\}.$$

Logo

$$A_1 \times \cdots \times A_{n-1} \times A_n = A_1 \times \cdots \times A_{n-1} \times \left(\bigcup_{i=1}^{m} \{a_i\} \right) = \bigcup_{i=1}^{m} (A_1 \times \cdots \times A_{n-1} \times \{a_i\})$$

que é uma união disjunta, e assim, pela proposição 4.2.2, temos

$$|A_1 \times \cdots \times A_{n-1} \times A_n| = \left| \bigcup_{i=1}^{m} (A_1 \times \cdots \times A_{n-1} \times \{a_i\}) \right| = \sum_{i=1}^{m} |A_1 \times \cdots \times A_{n-1} \times \{a_i\}|.$$

No entanto $|A_1 \times \cdots \times A_{n-1} \times \{a_i\}| = |A_1 \times \cdots \times A_{n-1}|$ para todo $i = 1,2,\cdots,n$. Portanto,

$$|A_1 \times \cdots \times A_{n-1} \times A_n| = \sum_{i=1}^{m} |A_1 \times \ldots \times A_{n-1}|,$$

e, por hipótese de indução, podemos concluir que

$$|A_1 \times \cdots \times A_{n-1} \times A_n| = \sum_{i=1}^{m} \left(\prod_{j=1}^{n-1} |A_j| \right) = \left(\prod_{j=1}^{n-1} |A_j| \right) \cdot m = \left(\prod_{j=1}^{n-1} |A_j| \right) \cdot |A_n| = \prod_{j=1}^{n} |A_j|.$$

■

Proposição 4.3.1 Se $n = p_1^{b_1} \cdots p_k^{b_k}$ é a decomposição canônica de um inteiro $n > 1$ e $d(n)$ é o seu número de divisores positivos, então

$$d(n) = \prod_{i=1}^{k} (b_i + 1).$$

Prova. Pela proposição 3.4.5, os divisores positivos de $n = p_1^{b_1} \cdots p_k^{b_k}$ são da forma $p_1^{a_1} \cdots p_k^{a_k}$, com $0 \leq a_i \leq b_i$ para todo $i = 1, \ldots, k$. Então, para cada a_i temos $b_i + 1$ possibilidades e pelo PFC, temos que

$$d(n) = (b_1 + 1) \cdots (b_k + 1) = \prod_{i=1}^{k} (b_i + 1).$$

■

Exemplo 4.3.1 Pela proposição 4.3.1, o número de divisores positivos de $360 = 2^3 3^2 5^1$, é

$$d(360) = (3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = 24.$$

Exemplo 4.3.2 (ENEM 2014 - ***Adaptada***) Durante a Segunda Guerra Mundial, para decifrarem as mensagens secretas, foi utilizada a técnica de decomposição em fatores primos. Um número N é dado pela expressão $2^x \cdot 5^y \cdot 7^z$, na qual x, y e z são números inteiros não negativos. Sabe-se que N é múltiplo de 10 e não é múltiplo de 7.

O número de divisores ***positivos*** de N, diferentes de N, é

A) $x \cdot y \cdot z$
B) $(x + 1) \cdot (y + 1)$
C) $x \cdot y \cdot z - 1$
D) $(x + 1) \cdot (y + 1) \cdot z$
E) $(x + 1) \cdot (y + 1) \cdot (z + 1) - 1$

Solução. Como N não é múltiplo de 7, temos que $z = 0$. Desse modo, pela proposição 4.3.1, o número de divisores positivos de N, diferentes de N, é $(x + 1) \cdot (y + 1) - 1$. Entretanto, como $z = 0$, segue que

$$(x+1)\cdot(y+1)\cdot(z+1)-1=(x+1)\cdot(y+1)-1.$$

Portanto, a alternativa correta é o item E.

Proposição 4.3.2 Seja A um conjunto finito e não vazio com n elementos. Então, há exatamente $n(n-1)\cdots(n-k+1)$ escolhas ordenadas de k elementos distintos de A.

Prova. Temos n modos de escolher qual elemento de A será o 1º. Tendo escolhido o 1º, temos $n-1$ modos de escolher qual elemento de A será o 2º e sucessivamente, $n-k+1$ modos de escolher qual elemento de A será o kº. Portanto, pelo princípio fundamental da contagem, temos $n(n-1)\cdots(n-k+1)$ escolhas ordenadas de k elementos distintos de A.

■

4.4 Números Binomiais

Os números binomiais têm um papel importante na combinatória, e também, como veremos, na teoria dos números. Eles utilizam a noção de fatorial, que apresentamos a seguir.

Definição 4.4.1 Dado um inteiro não negativo n, o fatorial de n, é o número

$$n!=\begin{cases}1, & se\ n=0.\\ \prod_{k=0}^{n-1}(n-k), & se\ n\geq 1.\end{cases}$$

Assim,

$$0!=1;$$

$$1!=\prod_{k=0}^{0}(1-k)=1-0=1;$$

$$2!=\prod_{k=0}^{1}(2-k)=(2-0)(2-1)=2\cdot 1=2;$$

$$3!=\prod_{k=0}^{2}(3-k)=(3-0)(3-1)(3-2)=3\cdot 2\cdot 1=6.$$

Mais geralmente, temos que

$$(n+1)! = (n+1) \cdot n!, \text{ para todo inteiro } n \geq 0.$$

Proposição 4.4.1 Seja A um conjunto finito e não vazio com n elementos. Então, há exatamente $n!$ modos distintos de ordenar os elementos de A.

Prova. Temos n modos de escolher qual elemento de A será o 1º. Tendo escolhido o 1º, temos $n-1$ modos de escolher qual elemento de A será o 2º e sucessivamente, 1 modo de escolher qual elemento de A será o último. Portanto, pelo princípio fundamental da contagem, temos

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

modos distintos de ordenar os elementos de A.

■

Proposição 4.4.2 Para todo inteiro $n \geq 2$, existem n inteiros consecutivos e compostos. Isto é, existem lacunas arbitrariamente grandes na sequência dos números primos, chamadas desertos de números primos.

Prova. Dado um inteiro $n > 1$, a sequência

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1).$$

De números inteiros positivos é formada por n números consecutivos, todos compostos, pois k divide $(n+1)!+k$, para todo $k \in \mathbb{N}$ tal que $2 \leq k \leq n+1$.

■

Exemplo 4.4.1 Pela proposição 4.4.2, a sequência de inteiros positivos

$$(10^6+1)!+2, (10^6+1)!+3, \ldots, (10^6+1)!+(10^6+1),$$

É formada por um milhão de números consecutivos, todos compostos.

Definição 4.4.2 Dados inteiros n e k, com $0 \leq k \leq n$, definimos o número binomial $\binom{n}{k}$ por

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

Proposição 4.4.3 (Relação de Stifel) Se n e k são naturais tais que $1 \leq k < n$, então

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

Prova. Pela definição de número binomial, segue que

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

$$= \frac{(\boldsymbol{n-k})(n-1)!}{k!\,(\boldsymbol{n-k})(n-k-1)!} + \frac{\boldsymbol{k}(n-1)!}{\boldsymbol{k}(k-1)!\,(n-k)!}$$

$$= \frac{(n-k)(n-1)!}{k!\,(n-k)!} + \frac{k(n-1)!}{k!\,(n-k)!}$$

$$= \frac{[(n-k)+k](n-1)!}{k!\,(n-k)!}$$

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

■

Proposição 4.4.4 Para todos os inteiros n e k tais que $0 \leq k \leq n$, temos que $\binom{n}{k} \in \mathbb{N}$.

Prova. Se $k = n$, segue que

$$\binom{n}{k} = \binom{k}{k} = \frac{k!}{k!\,(k-k)!} = \frac{k!}{k!\,0!} = \frac{k!}{k!} = 1 \in \mathbb{N}.$$

Se $k = 0 < n$, segue que

$$\binom{n}{k} = \binom{n}{0} = \frac{n!}{0!\,(n-0)!} = \frac{n!}{0!\,n!} = \frac{n!}{n!} = 1 \in \mathbb{N}.$$

Se $0 < k < n$, façamos indução completa sobre $n \geq 2$, sendo o caso $n = 2$ válido, pois o único número binomial nessas condições é $\binom{2}{1} = 2 \in \mathbb{N}$.

Agora, suponhamos, por hipótese de indução, que $\binom{n-1}{i} \in \mathbb{N}$, para todo inteiro i tal que $0 \leq i \leq n-1$. Logo, $\binom{n-1}{k}$ e $\binom{n-1}{k-1}$ são naturais e pela relação de Stifel, segue que

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

■

Exemplo 4.4.2 Prove que, para todo $n \in \mathbb{N}$, o número $n^3 + 5n$ é um múltiplo de 6.

Prova. Se $n = 1$, então $n^3 + 5n = 1^3 + 5 \cdot 1 = 1 + 5 = 6$, que é um múltiplo de 6.

Se $n = 2$, então $n^3 + 5n = 2^3 + 5 \cdot 2 = 8 + 10 = 18$, que é outro múltiplo de 6.

Se $n \geq 3$, pela proposição 4.4.4, temos que $\binom{n}{1}, \binom{n}{2}, \binom{n}{3} \in \mathbb{N}$, isto é,

$$\binom{n}{1} = \frac{n!}{1!\,(n-1)!} = \frac{n(n-1)!}{(n-1)!} = n \in \mathbb{N};$$

$$\binom{n}{2} = \frac{n!}{2!\,(n-2)!} = \frac{n(n-1)(n-2)!}{2(n-2)!} = \frac{n(n-1)}{2} \in \mathbb{N};$$

$$\binom{n}{3} = \frac{n!}{3!\,(n-3)!} = \frac{n(n-1)(n-2)(n-3)!}{6(n-3)!} = \frac{n(n-1)(n-2)}{6} \in \mathbb{N}.$$

Desse modo,

$$6\left[\binom{n}{1}+\binom{n}{2}+\binom{n}{3}\right]=6\left[n+\frac{n(n-1)}{2}+\frac{n(n-1)(n-2)}{6}\right]$$

é um múltiplo de 6. Daí,

$$6n+3n(n-1)+n(n-1)(n-2)=$$

$$n[6+3(n-1)+(n-1)(n-2)]=$$

$$n[6+(n-1)(3+n-2)]=$$

$$n[6+(n-1)(n+1)]=$$

$n[6+n^2-1]=n[n^2+5]=n^3+5n$ é um múltiplo de 6.

■

Exemplo 4.4.3 Prove que o produto de k naturais consecutivos é sempre divisível por $k!$.

Prova. Seja $P=(m+1)(m+2)\cdots(m+k)$ o produto de k números naturais consecutivos, para todo inteiro não negativo m. Então

$$P=\boldsymbol{k!}\frac{\boldsymbol{m!}\,[(m+1)(m+2)\cdots(m+k)]}{\boldsymbol{k!}\,\boldsymbol{m!}}\Longrightarrow$$

$$P=k!\frac{(m+k)!}{k!\,m!}\Longrightarrow$$

$$P=k!\binom{m+k}{k}\Longrightarrow k!\,|P,$$

pois, pela proposição 4.4.4, temos que $\binom{m+k}{k}\in\mathbb{N}$.

■

Proposição 4.4.5 Se p é primo, então $p\mid\binom{p}{k}$ para todo inteiro k tal que $1\leq k\leq p-1$.

Prova. Decorre, da definição de número binomial, que

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \Longrightarrow p! = k!\,(p-k)!\binom{p}{k}.$$

Daí, p divide $k!\,(p-k)!\binom{p}{k}$, pois p divide $p!$. Logo, pela proposição 3.4.2 (i), temos que $p|k!$ ou $p|(p-k)!$ ou $p \mid \binom{p}{k}$.

Suponhamos que $p|k!$, então, pela proposição 3.4.2 (i), temos que $p|r$ para algum inteiro r tal que $1 \leq r \leq k \leq p-1$, um absurdo pela proposição 3.1.1 (i). Portanto, $p \nmid k!$.

Analogamente, $p \nmid (p-k)!$, já que $1 \leq p-k \leq p-1$. Portanto, $p \mid \binom{p}{k}$.

■

4.5 Combinação Simples

Definição 4.5.1 Seja A um conjunto finito com n elementos. Uma combinação simples dos n elementos de A, tomados k a k, com $0 \leq k \leq n$, é um subconjunto de A com k elementos.

Definição 4.5.2 Denotamos o número de combinações simples de n elementos tomados k a k, com $0 \leq k \leq n$, por C_n^k.

Proposição 4.5.1 Para quaisquer inteiros n e k, tais que $0 \leq k \leq n$, temos que $C_n^k = \binom{n}{k}$.

Prova. Seja A um conjunto finito com n elementos. Se $k = 0$, então $C_n^0 = 1$, pois $\emptyset$ é o único subconjunto de A com 0 elementos. Por outro lado, $\binom{n}{0} = 1$ e, portanto $C_n^k = \binom{n}{k}$ nesse caso.

Agora, suponhamos que $0 < k \leq n$. Pela proposição 4.3.2, o número de escolhas ordenadas de k elementos distintos de A é

$$n(n-1)\cdots(n-k+1).$$

Por outro lado, $k!\,C_n^k$ é também o número de escolhas ordenadas de k elementos distintos de A, pois dado um subconjunto de A com k elementos, pela proposição 4.4.1, podemos ordená-lo de $k!$ modos e como existem C_n^k subconjuntos de A com k elementos, o total é $k!\,C_n^k$. Portanto,

$$k!\,C_n^k = n(n-1)\cdots(n-k+1) \Longrightarrow$$

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)}{k!} \Longrightarrow$$

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)(\boldsymbol{n-k})!}{k!\,(\boldsymbol{n-k})!} \Longrightarrow$$

$$C_n^k = \frac{n!}{k!\,(n-k)!} = \binom{n}{k}.$$

■

Observamos que, em outras palavras, a proposição 4.5.1 calcula o número de modos de se escolher k objetos distintos entre n objetos distintos dados.

4.6 Binômio de Newton

Nessa seção, apresentaremos uma expressão para o desenvolvimento de $(a+b)^n$, para todo $n \in \mathbb{N}$, conhecida como fórmula do binômio de Newton, que possui várias aplicações importantes em teoria dos números.

Teorema 4.6.1 (Binômio de Newton) Para todo $n \in \mathbb{N}$, temos que

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

Prova. Façamos indução sobre $n \geq 1$, sendo o caso $n = 1$ válido, pois

$$\sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1.$$

Agora, supondo o resultado válido para n e observando que

$$(a+b)^{n+1} = (a+b)(a+b)^n = a(a+b)^n + b(a+b)^n,$$

temos, por hipótese de indução, que

$$\begin{aligned} a(a+b)^n &= a\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k \\ &= \binom{n}{0}a^{n+1}b^0 + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k \end{aligned}$$

E

$$\begin{aligned} b(a+b)^n &= b\sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^j \\ &= \sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^{j+1} \\ &= \sum_{j=0}^{n-1}\binom{n}{j}a^{n-j}b^{j+1} + \binom{n}{n}a^0b^{n+1} \\ &= \sum_{k=1}^{n}\binom{n}{k-1}a^{n+1-k}b^k + b^{n+1} \end{aligned}$$

onde $j = k-1$. Desse modo, temos que

$$(a+b)^{n+1} = a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=1}^{n}\binom{n}{k-1}a^{n+1-k}b^k + b^{n+1}$$

$$= a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k} b^k + b^{n+1}.$$

Assim, pela relação de Stifel, segue que

$$(a+b)^{n+1} = a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + b^{n+1}$$
$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.$$

Ou seja, o resultado vale também para $n+1$ e, portanto, vale para todo $n \in \mathbb{N}$.

■

Exemplo 4.6.1 [3] Prove que, para todo $k \in \mathbb{N}$, o número $10^k - 1$ é um múltiplo de 9.

Prova. Pelo teorema 4.6.1, temos que

$$10^k - 1 = (9+1)^k - 1 = \sum_{j=0}^{k} \binom{k}{j} 9^{k-j} - 1 = \sum_{j=0}^{k-1} \binom{k}{j} 9^{k-j} = 9 \left(\sum_{j=0}^{k-1} \binom{k}{j} 9^{k-j-1} \right).$$

Novamente um múltiplo de 9, pois

$$\sum_{j=0}^{k-1} \binom{k}{j} 9^{k-j-1} \in \mathbb{N}$$

visto que $0 \leq j \leq k-1$ e desse modo $\binom{k}{j} \in \mathbb{N}$.

■

Proposição 4.6.1 Para todo $n \in \mathbb{N}$, temos que

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

(ii) $\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0.$

Prova.

(i) Pelo teorema 4.6.1, temos que

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

(ii) Pelo teorema 4.6.1, temos que

$$0 = \big(1 + (-1)\big)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n}.$$

■

Exemplo 4.6.2 Prove que, se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a decomposição canônica de um inteiro $n > 1$, então n pode ser escrito como produto de dois números relativamente primos de 2^{k-1} modos.

Prova. Seja $n = ab$, com $mdc(a, b) = 1$ e $j \in \mathbb{Z}$ tal que $0 \leq j \leq k$. Se exatamente j primos de $\{p_1, p_2, \ldots, p_k\}$ figuram na decomposição canônica de a, então todos os outros $k - j$ figuram na decomposição canônica de b, pois $mdc(a, b) = 1$. Assim, é suficiente contar de quantos modos podemos escolher j primos distintos entre k primos distintos, para formarem o número a, o que pode ser feito, pela proposição 4.5.1, de C_k^j modos. Portanto, para todo $j \in \mathbb{Z}$ tal que $0 \leq j \leq k$, esse total de modos, pela proposição 4.6.1 (i), é

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

Porém, nessa contagem, para cada produto $n = ab$ também contamos $n = ba$. Portanto, n pode ser escrito como produto de dois números relativamente primos de $(2^k/2) = 2^{k-1}$ modos.

■

Exemplo 4.6.3 (Pequeno Teorema de Fermat) Se p é um primo e n um inteiro positivo, então $p|(n^p - n)$.

Prova. Façamos indução sobre $n \geq 1$, sendo o caso $n = 1$ válido, pois $1^p - 1 = 0$ e $p|0$.

Agora, supondo o resultado válido para n, iremos prová-lo para $n + 1$. Pela fórmula do Binômio de Newton, temos

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

Como, por hipótese de indução, $p|(n^p - n)$ e, pela proposição 4.4.5, p divide $\binom{p}{1}, \cdots, \binom{p}{p-1}$, temos, pela proposição 3.1.2, que p divide $(n^p - n) + \binom{p}{1} n^{p-1} + \cdots + \binom{p}{p-1} n$. Portanto, p divide $(n+1)^p - (n+1)$, o que conclui nossa prova por indução finita.

■

4.7 Princípio da inclusão-exclusão

O princípio da inclusão-exclusão é uma extensão do princípio aditivo da contagem, pois determina o número de elementos da união finita de conjuntos finitos, não necessariamente disjuntos dois a dois.

A proposição a seguir diz como calcular o número de elementos da diferença de um conjunto finito e um subconjunto.

Proposição 4.7.1 [6] Se A é um conjunto finito e $B \subset A$, então $|A \backslash B| = |A| - |B|$.

Prova. Como $A = B \cup (A \backslash B)$ é uma união disjunta, temos pelo princípio aditivo que

$$|A| = |B \cup (A \backslash B)| = |B| + |A \backslash B| \Longrightarrow$$

$$|A \backslash B| = |A| - |B|.$$

■

A forma mais simples do princípio da inclusão-exclusão, que calcula o número de elementos da união de dois conjuntos finitos, consta na seguinte proposição.

Proposição 4.7.2 [6] Se A e B são conjuntos finitos, então $|A \cup B| = |A| + |B| - |A \cap B|$.

Prova. Como A e $B\backslash A$ são conjuntos disjuntos e tais que $A \cup B = A \cup (B\backslash A)$, temos

$$|A \cup B| = |A| + |B\backslash A|.$$

Por outro lado, temos também a união disjunta $B = (A \cap B) \cup (B\backslash A)$, donde segue que

$$|B| = |A \cap B| + |B\backslash A|.$$

Substituindo essa relação na expressão para $|A \cup B|$, obtemos

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

■

Para a união de três conjuntos finitos A, B e C, temos, pela proposição 4.7.2, que

$$|A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|.$$

Como $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, pela proposição 4.7.2, temos que

$$|A \cup B \cup C| = |A \cup B| + |C| - |(A \cap C) \cup (B \cap C)|$$

$$= |A \cup B| + |C| - (|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|).$$

Como $(A \cap C) \cap (B \cap C) = A \cap B \cap C$, pela proposição 4.7.2, segue que

$$|A \cup B \cup C| = |A| + |B| - |A \cap B| + |C| - (|A \cap C| + |B \cap C| - |A \cap B \cap C|)$$

$$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Então, motivados pela proposição 4.7.2 e pela relação obtida acima, o Princípio da inclusão-exclusão para a união de n conjuntos finitos é o resultado do próximo teorema.

Teorema 4.7.1 (Princípio da inclusão-exclusão) Se A_1, A_2, ..., A_n são conjuntos finitos, então

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \le i_1 \le n} |A_{i_1}| \quad - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \quad + \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$$

$$- \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|. \tag{4.1}$$

Prova. Seja $a \in (A_1 \cup A_2 \cup \cdots \cup A_n)$ tal que a pertença a exatamente p dos conjuntos A_1, A_2, ... , A_n. Mostremos que a é contado exatamente uma vez pelo segundo membro de (4.1). Pela Proposição 4.5.1, a é contado exatamente:

$$\binom{p}{1} \text{ vezes em } \sum_{1 \le i_1 \le n} |A_{i_1}|;$$

$$\binom{p}{2} \text{ vezes em } \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}|;$$

$$\binom{p}{3} \text{ vezes em } \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|;$$

$$\vdots$$

$$\binom{p}{p} \text{ vezes em } \sum_{1 \le i_1 < i_2 < \cdots < i_p \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_p}|;$$

E claramente, nenhuma vez em

$$\sum_{1 \le i_1 < i_2 \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|,$$

para todo inteiro k tal que $p < k \le n$, pois a interseção de mais de p conjuntos não contem a.

Logo, o número de vezes que a é contado pelo segundo membro de (4.1) é igual a

$$\binom{p}{1} - \binom{p}{2} + \binom{p}{3} + \cdots + (-1)^{p-1}\binom{p}{p}.$$

Mas, pela proposição 4.6.1 (ii),

$$\binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \binom{p}{3} + \cdots + (-1)^{p}\binom{p}{p} = 0 \Longrightarrow$$

$$\binom{p}{0} - \left[\binom{p}{1} - \binom{p}{2} + \binom{p}{3} + \cdots + (-1)^{p-1}\binom{p}{p}\right] = 0 \Longrightarrow$$

$$\binom{p}{1} - \binom{p}{2} + \binom{p}{3} + \cdots + (-1)^{p-1}\binom{p}{p} = \binom{p}{0} \Longrightarrow$$

$$\binom{p}{1} - \binom{p}{2} + \binom{p}{3} + \cdots + (-1)^{p-1}\binom{p}{p} = 1.$$

■

Definição 4.7.1 Dado um inteiro positivo n, denotamos por $\phi(n)$ o número de inteiros positivos menores ou iguais a n que são relativamente primos com n.

Teorema 4.7.2 Se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a decomposição canônica de um inteiro $n > 1$, então

$$\phi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Prova. Seja I_n o conjunto dos inteiros positivos menores ou iguais a n e A_i o conjunto dos elementos de I_n que são múltiplos de p_i, para todo inteiro i tal que $1 \leq i \leq k$. Como

$$I_n \backslash (A_1 \cup A_2 \cup \cdots \cup A_k) = \{1 \leq a \leq n \mid mdc(a,n) = 1\}$$

e $\phi(n) = |\{1 \leq a \leq n \mid mdc(a,n) = 1\}|$, temos, que

$$\phi(n) = |I_n \backslash (A_1 \cup A_2 \cup \cdots \cup A_k)|.$$

Logo, pela proposição 4.7.1, segue que

$$\phi(n) = |I_n| - |A_1 \cup A_2 \cup \cdots \cup A_k| \Longrightarrow$$

$$\phi(n) = n - |A_1 \cup A_2 \cup \cdots \cup A_k|. \tag{4.2}$$

Agora, observando que

$$A_i = \left\{p_i, 2p_i, \ldots, \frac{n}{p_i}p_i\right\} \Longrightarrow |A_i| = \frac{n}{p_i};$$

$$A_i \cap A_j = \left\{p_i p_j, 2p_i p_j, \ldots, \frac{n}{p_i p_j}p_i p_j\right\} \Longrightarrow \left|A_i \cap A_j\right| = \frac{n}{p_i p_j} (i \neq j);$$

$$\vdots$$

$$|A_1 \cap A_2 \cap \cdots \cap A_k| = \frac{n}{p_1 p_2 \cdots p_k}.$$

Temos, pelo teorema 4.7.1, que (4.2) equivale a

$$\phi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \cdots + \frac{n}{p_{k-1} p_k}\right) - \cdots$$

$$+ (-1)^k \frac{n}{p_1 p_2 \cdots p_k}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

$$= n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

■

Exemplo 4.7.1 Pelo teorema 4.8.2, $\phi(n)$ para $n = 360 = 2^3 3^2 5$, é

$$\phi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 96.$$

Ou seja, existem 96 inteiros k, tais que $1 \leq k \leq 360$ e $mdc(k, 360) = 1$.

4.8 Princípio da Casa dos Pombos

O Princípio da Casa dos Pombos (PCP) tem um enunciado simples e bem intuitivo, mas permite resolver vários problemas, especialmente os que tratam de provar a existência de certos elementos ou subconjuntos.

Teorema 4.8.1 (Princípio da Casa dos Pombos) Se $n + 1$ pombos são colocados em n gaiolas, então pelo menos uma gaiola conterá mais de um pombo.

Prova. Se cada uma das gaiolas contiver, no máximo, 1 pombo, o número total de pombos nelas colocados será, no máximo n, o que é uma contradição, pois foram colocados $n + 1$ pombos.

■

Exemplo 4.8.1 Mostre que todo inteiro positivo n tem um múltiplo que se escreve apenas com os algarismos 0 e 1.

Solução. Considere a sequência $1, 11, 111, 1111, \ldots, 11\ldots1$, formada por $n + 1$ números, onde o último número tem $n + 1$ algarismos 1. Dividindo-os por n, pela proposição 3.2.1, os restos dessas divisões só podem ser iguais a $0, 1, 2, \ldots, n - 1$.

Agora, pensando nos números como pombos e nos restos como gaiolas, temos, pelo PCP, que pelo menos dois números dessa sequência têm restos iguais na divisão por n, digamos $11\ldots1$ (p algarismos) e $11\ldots1$ (q algarismos), com $p < q$. Assim sendo, pela proposição 3.2.2, a diferença desses números é um múltiplo de n, escrito como $11\ldots10\ldots0$, com p algarismos 0 e $q - p$ algarismos 1.

Exemplo 4.8.2 Mostre que todo inteiro positivo n, primo com 10, possui um múltiplo que se escreve apenas com algarismos 1.

Solução. Pelo exemplo 4.8.1, n possui um múltiplo da forma $11\ldots10\ldots0$, com p algarismos 0 e $q-p$ algarismos 1, ou seja, n divide $11\ldots1 \times 10^p$. Como n é relativamente primo com 10, temos que $mdc(n, 10^p) = 1$, o que implica, pela proposição 3.3.2, que n divide $11\ldots1$, ou seja, $11\ldots1$, com $q-p$ algarismos 1, é um múltiplo de n .

Exemplo 4.8.3 Mostre que todo subconjunto de $\{1, 2, \ldots, 2n\}$, com $n+1$ elementos, possui um par de elementos consecutivos e consequentemente primos entre si.

Solução. Como $\{1, 2, \ldots, 2n\} = \{1, 2\} \cup \{3, 4\} \cup \cdots \cup \{2n-1, 2n\}$, que é uma união disjunta de n subconjuntos (gaiolas), temos, pelo PCP, que ao tomarmos $n+1$ elementos (pombos) de $\{1, 2, \ldots, 2n\}$, acabamos por escolher os dois elementos de pelo menos um desses subconjuntos, os quais são consecutivos e, pela proposição 3.3.1, primos entre si.

Exemplo 4.8.4 Mostre que todo subconjunto de $\{1, 2, \ldots, 2n\}$, com $n+1$ elementos, possui um par de elementos tais que um deles divide o outro.

Solução. Primeiro, observamos que todo inteiro a pode ser escrito na forma $a = 2^k b$, sendo b um número ímpar e k um inteiro não negativo, com $k > 0$, caso a seja um número par e $k = 0$, caso a seja um número ímpar. Desse modo, se $a \in \{1, 2, \ldots, 2n\}$, então $a = 2^k b$ onde b só pode um dos n inteiros ímpares $1, 3, 5, \ldots, 2n-1$. Daí, ao tomar-se $n+1$ elementos de $\{1, 2, \ldots, 2n\}$, temos, pelo PCP, que pelo menos dois deles terão o mesmo b. Sejam $a_1 = 2^r b$ e $a_2 = 2^s b$ tais números, onde $r < s$. Segue então, que $a_2 = 2^{s-r} a_1$, ou seja, $a_1 | a_2$.

Exemplo 4.8.5 Prove que em qualquer conjunto de 52 inteiros existe um par de inteiros cuja soma ou cuja diferença é divisível por 100.

Solução. Dividindo os 52 inteiros por 100, temos, pela proposição 3.2.1, que os possíveis restos são $0, 1, 2, \ldots, 49, 50, 51, \ldots, 98, 99$. Organizando esses restos em 51 gaiolas como abaixo

$$\{0\}, \{1, 99\}, \{2, 98\}, \ldots, \{49, 51\}, \{50\},$$

Temos, pelo PCP, que há dois inteiros dentre os 52, que têm restos numa mesma gaiola. Se essa gaiola for $\{0\}$ ou $\{50\}$, então a soma e a diferença desses números será divisível por 100. Se a gaiola for qualquer uma das outras, então a diferença será divisível por 100, se os restos forem iguais e a soma será divisível por 100, se os restos forem diferentes.

Exemplo 4.8.6 Mostre que qualquer conjunto com n inteiros possui subconjunto cuja soma dos elementos é divisível por n.

Solução. Seja $A = \{a_1, a_2, \dots, a_n\}$ um conjunto de n inteiros e considere as n somas abaixo

$$S_1 = a_1$$
$$S_2 = a_1 + a_2$$
$$S_3 = a_1 + a_2 + a_3$$
$$\vdots$$
$$S_n = a_1 + a_2 + a_3 + \cdots + a_n$$

Se alguma dessas somas for divisível por n, não há mais o que mostrar. Suponhamos agora, que nenhuma dessas somas seja divisível por n. Segue então, que nenhuma pode ter resto nulo na divisão por n, ou seja, os únicos restos possíveis são, $1, 2, \dots, n-1$. Como existem n somas e apenas $n-1$ restos possíveis, pelo PCP, pelo menos duas delas, digamos S_i e S_j, com $i < j$, possuem restos iguais na divisão por n. Logo, pela proposição 3.2.2, temos que

$$S_j - S_i = a_{i+1} + a_{i+2} + \cdots + a_j$$

é divisível por n e, portanto, $\{a_{i+1}, a_{i+2}, \dots, a_j\}$ é o subconjunto procurado.

Exemplo 4.8.7 Seja n um inteiro positivo ímpar, mostre que existe um inteiro positivo k tal que

$$\sum_{i=0}^{k} 2^i$$

é divisível por n.

Solução. Considere as potências $2^0, 2^1, 2^2, \dots, 2^n$. Dividindo-as por n, temos, pela proposição

3.2.1, que os possíveis restos são $0, 1, 2, \ldots, n-1$. Como temos $n+1$ potências (pombos) e n restos (gaiolas), temos, pelo PCP, que pelo menos duas potências, digamos 2^r e 2^s, com $r < s$, possuem restos iguais na divisão por n. Logo, pela proposição 3.2.2, segue que $n \mid (2^s - 2^r)$, ou seja, $n \mid 2^r(2^{s-r} - 1)$. Mas, como n é ímpar, temos que $mdc(n, 2^r) = 1$, de modo que, pela proposição 3.3.2, $n \mid (2^{s-r} - 1)$. Por fim, observando que, para $n > 1$, temos $s \neq r + 1$, pois do contrário, $n \mid (2^{s-r} - 1) = (2^{r+1-r} - 1) = 2 - 1 = 1$, o que é uma contradição; e também, pelo exemplo 2.1.1, tem-se

$$2^{s-r} - 1 = \sum_{i=0}^{s-r-1} 2^i.$$

Portanto, $k = s - r - 1$ é o inteiro positivo procurado.

Teorema 4.8.2 (Generalização do PCP) Se $nk + 1$ pombos são colocados em n gaiolas, então pelo menos uma gaiola deverá conter pelo menos $k + 1$ pombos.

Prova. Se cada gaiola contiver no máximo k pombos, como são n gaiolas, no máximo nk terão sido distribuídos, o que é uma contradição.

■

Exemplo 4.8.8 Selecionam-se oito números distintos no conjunto $\{1, 2, \ldots, 15\}$. Mostre que há pelo menos três pares de números selecionados com a mesma diferença entre o maior e o menor número do par.

Solução. Como os números são escolhidos no conjunto $\{1, 2, \ldots, 15\}$, os valores possíveis para a diferença de dois números são $1, 2, \ldots, 14$ (ou seja, há 14 valores possíveis). Por outro lado, os oito números formam $C_8^2 = 28$ pares. Destes, no máximo 1 resulta em uma diferença igual a 14 (quando formado por 1 e 15). Em consequência, há pelo menos 27 pares cujas diferenças pertencem ao conjunto $\{1, 2, \ldots, 13\}$. Como $27 = 13 \cdot 2 + 1$, pelo teorema 4.8.2, há pelo menos uma gaiola (diferença) contendo pelo menos $2 + 1 = 3$ pombos (pares). Assim, há pelo menos três pares de números em que a diferença entre o maior e o menor número do par é a mesma.

Exemplo 4.8.9 Do conjunto $A = \{1, 2, \ldots, 99, 100\}$, escolhemos ao acaso 55 números. Mostre que entre os números escolhidos existem dois cuja a diferença é 9.

Solução. Consideremos as gaiolas numeradas $0, 1, 2, \ldots, 8$, onde o número $n \in A$ é colocado na gaiola i se, e só se, o resto da divisão de n por 9 é i. Desse modo, temos as gaiolas:

$$\text{Gaiola } 0 = \{9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99\};$$

$$\text{Gaiola } 1 = \{1, 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100\};$$

$$\text{Gaiola } 2 = \{2, 11, 20, 29, 38, 47, 56, 65, 74, 83, 92\};$$

$$\text{Gaiola } 3 = \{3, 12, 21, 30, 39, 48, 57, 66, 75, 84, 93\};$$

$$\text{Gaiola } 4 = \{4, 13, 22, 31, 40, 49, 58, 67, 76, 85, 94\};$$

$$\text{Gaiola } 5 = \{5, 14, 23, 32, 41, 50, 59, 68, 77, 86, 95\};$$

$$\text{Gaiola } 6 = \{6, 15, 24, 33, 42, 51, 60, 69, 78, 87, 96\};$$

$$\text{Gaiola } 7 = \{7, 16, 25, 34, 43, 52, 61, 70, 79, 88, 97\};$$

$$\text{Gaiola } 8 = \{8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98\}.$$

Como $55 = 9 \cdot 6 + 1$, pelo teorema 4.8.2, há pelo menos uma gaiola contendo pelo menos $6 + 1 = 7$ dos 55 números escolhidos. Mas em cada gaiola há no máximo 12 números. Então, pelo exemplo 4.8.3, há dois números sucessivos em tal gaiola, isto é, dois números cuja diferença é 9.

4.9 Os Teoremas de Fermat e Wilson

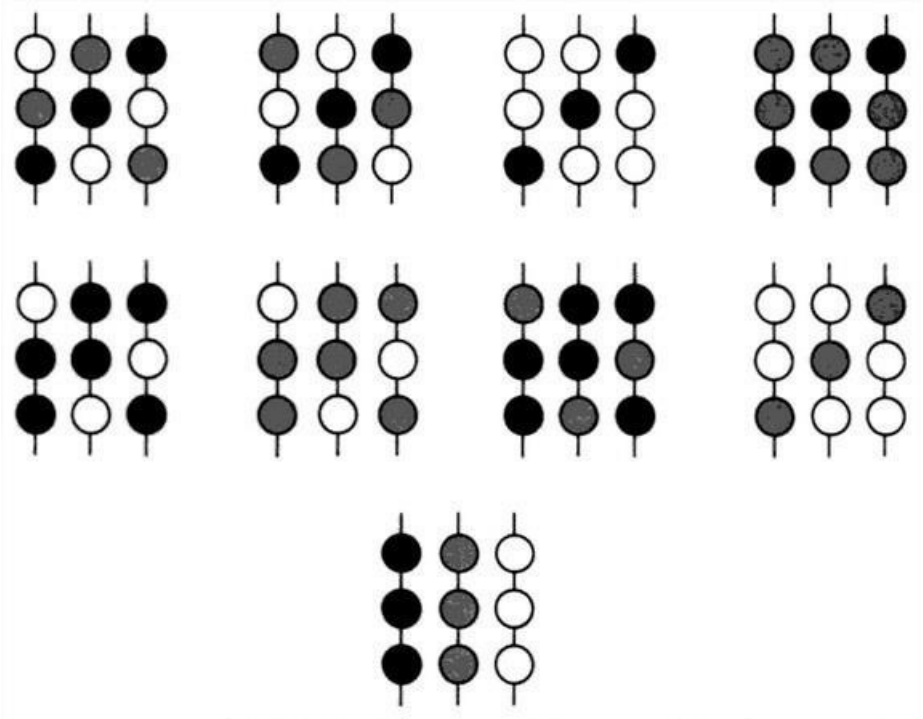
A Teoria dos Números possui vários resultados importantes sobre números primos, dentre eles, o Pequeno Teorema de Fermat e o Teorema de Wilson. Nesse capítulo, provaremos esses dois teoremas empregando técnicas combinatórias.

No exemplo 4.6.3, provamos o Pequeno Teorema de Fermat por Indução, utilizando o Binômio de Newton. A seguir, apresentamos outra prova, seguindo Santos [7] e Andrews [8].

Teorema 4.9.1 Se p é um primo e n é um inteiro positivo, então $p|(n^p - n)$.

Prova. Suponhamos que desejamos formar correntes com p pérolas coloridas cada uma e que possuímos, em mãos, pérolas suficientes que nos permitem o uso ilimitado de cada uma das n cores. Desse modo, pelo PFC, o número de correntes que podemos formar é n^p, pois cada pérola pode ser escolhida de n maneiras e são p escolhas para cada corrente. A Figura 1 ilustra o caso em que $n = 3$ e $p = 3$.

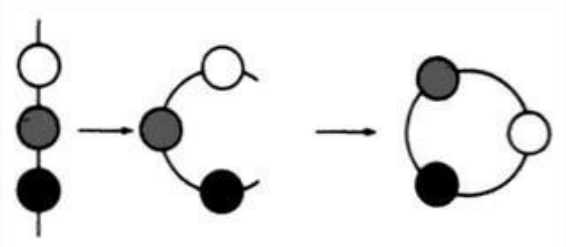
Figura 1 – As vinte e sete correntes de três pérolas com três cores possíveis.



Fonte: Andrews.

Das n^p possibilidades, exatamente n correntes possuem pérolas de apenas uma cor. Colocando estas à parte e, de maneira ilustrada na Figura 2, juntamos as duas extremidades de cada uma das $n^p - n$ correntes formando $n^p - n$ pulseiras.

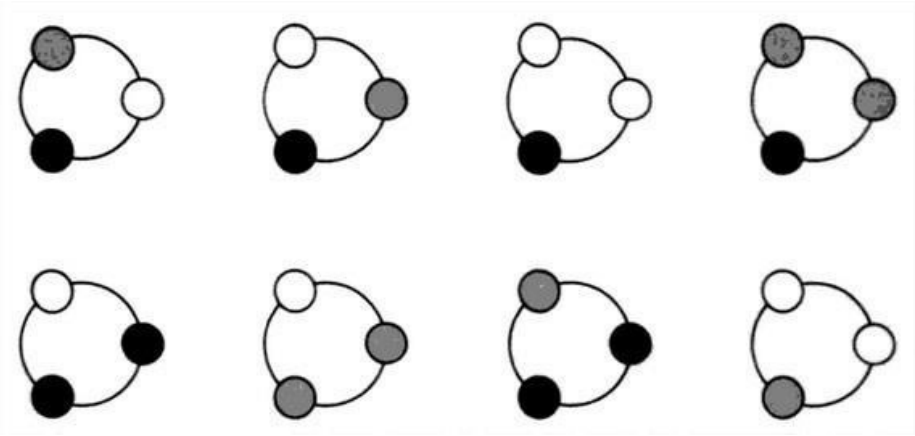
Figura 2 – A formação de uma pulseira a partir de uma corrente



Fonte: Andrews.

Nós podemos alterar qualquer corrente de pérolas, removendo uma pérola da parte de cima e colocando-a na parte de baixo. Tal alteração produz uma corrente diferente sem alterar a pulseira resultante. Quando $n = 3$ e $p = 3$, as 24 correntes multicoloridas podem ser reunidas em 8 grupos de 3 correntes que podem ser obtidas, uma das outras, por uma ou mais repetições da alteração que descrevemos. Veja os oito primeiros grupos da Figura 1. Observamos que, para cada um destes oito diferentes grupos corresponde uma pulseira distinta (veja Figura 3).

Figura 3 – As oito pulseiras de três pérolas com três cores possíveis (pulseiras de uma cor excluídas).



Fonte: Andrews.

Agora, seja k o menor número de vezes que esta alteração pode ser repetida até que a corrente original seja reproduzida. Assim, temos $k > 1$, pois excluímos todas as correntes em que todas as pérolas são de uma mesma cor. Observe que após $2k$ alterações a pulseira original será reproduzida novamente e, de forma semelhante, após $3k$, $4k$, etc. pelo algoritmo da divisão (Proposição 3.1.2) existem h e r tais que $p = hk + r$, com $0 \leq r < k$.

Como uma corrente é reproduzida após hk alterações e é também reproduzida após p alterações, serão necessárias r alterações, após a $hk^{\underline{a}}$ alteração para se obter a reprodução da coloração inicial. Como $r < k$ e k é o menor número inteiro positivo de alterações necessárias para a obtenção de uma reprodução, então $r = 0$. Daí, $p = hk$, ou seja, $k|p$ e, portanto, $k = p$, já que $k > 1$ e p é um primo. Consequentemente, as $n^p - n$ correntes podem ser agrupadas em grupos de p correntes cada, e é claro que cada grupo gera uma pulseira diferente.

Portanto, o número de pulseiras N multiplicado por p fornece o número de correntes que não são formadas de uma única cor, que é $n^p - n$. Logo, $pN = n^p - n$, isto é, $p|(n^p - n)$.

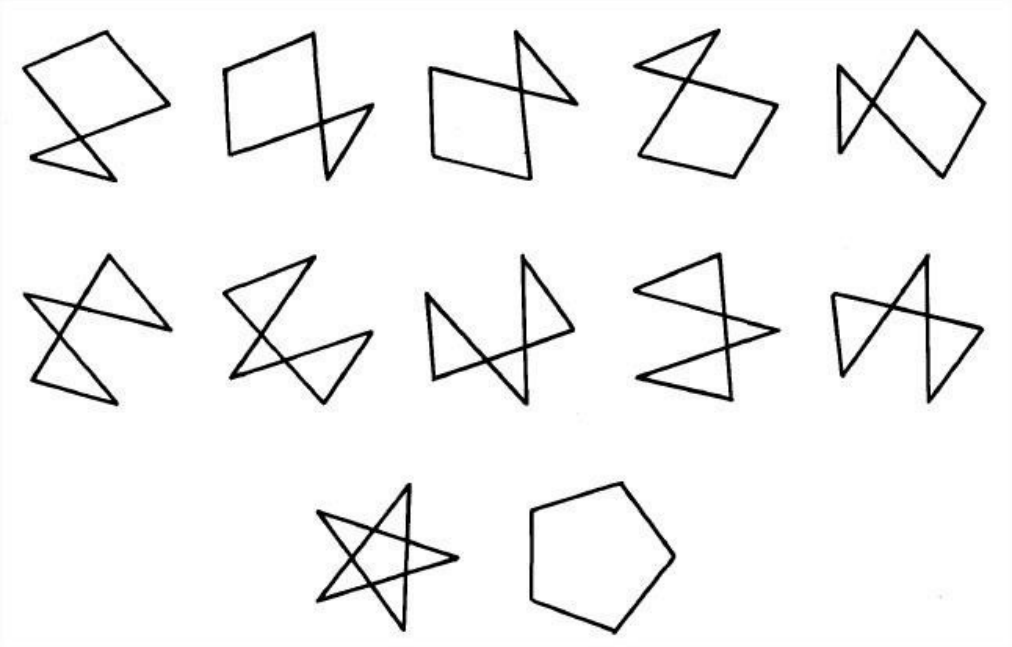
■

A prova do teorema de Wilson, apresentada a seguir, segue [7] e [8].

Teorema 4.9.2 (Wilson) Se p é primo, então $p \mid [(p-1)! + 1]$.

Prova. Se $p = 2$, O resultado é evidente. Suponhamos então, que agora p seja um primo ímpar. Consideramos p pontos em um círculo distribuídos de tal forma que eles dividem o círculo em p arcos iguais. Quantos polígonos podemos formar unindo estes pontos (cruzamentos de arestas são permitidos)? Estes polígonos são chamados p-ágonos estrelados pelo fato de seus vértices serem os vértices de um polígono regular convexo de p lados. É de se esperar que o total de tais polígonos, seja $p!$ Isto porque temos p escolhas para o primeiro vértice, $(p-1)$ para o segundo e assim sucessivamente. Observe, entretanto, que podemos descrever cada um destes p-ágonos de $2p$ maneiras diferentes, isto é, iniciando em qualquer um dos p vértices e escolhendo um ou outro dos dois segmentos naquele vértice como inicial. Portanto, obtemos, na realidade, $p!/2p$ diferentes p-ágonos. A Figura 4 mostra os doze pentágonos estrelados.

Figura 4 – os doze pentágonos estrelados.

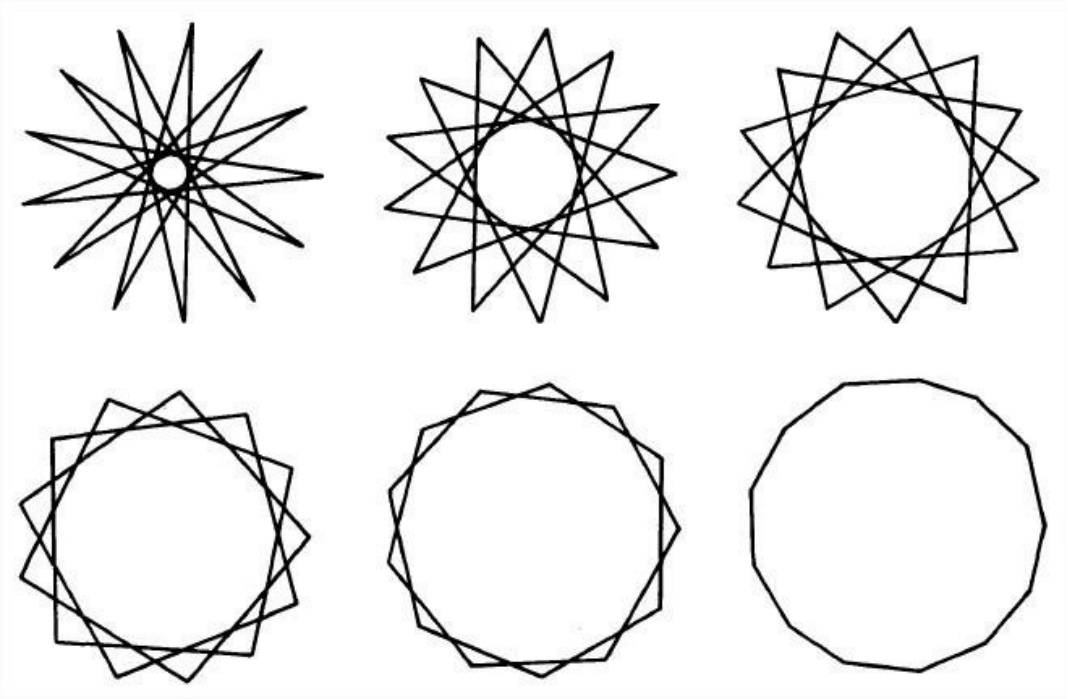


Fonte: Andrews.

Dos $p!/2p$ p-ágonos, exatamente $(p-1)/2$ ficam inalterados quando submetidos a uma rotação de $2\pi/p$ radianos. Estes chamam-se p-ágonos estrelados regulares uma vez que são "estrelas" de p pontos onde cada ponto é o vértice de um ângulo de $(2k+1)\pi/p$ radianos, onde $0 \leq k < (p-1)/2$.

No caso $p = 5$, há duas de tais figuras, mostradas na terceira linha da Figura 4. No caso $p = 13$ as seis figuras estão ilustradas na Figura 5.

Figura 5 – Os seis 13-ágonos estrelados regulares



Fonte: Andrews.

Os restantes $p!/2p - (p-1)/2$ p-ágonos estrelados pertencem, naturalmente, a conjunto de p elementos onde os componentes de cada conjunto podem ser obtidos de um único elemento por sucessivas rotações de $2\pi/p$ radianos. A observação de que existem p elementos em cada conjunto pode ser verificada como na demonstração do Pequeno Teorema de Fermat, onde mostramos que cada pulseira provém de p grupos de pérolas. Quando $p = 5$, existem dois de tais conjuntos que constituem a primeira e segunda linhas da Figura 4. Desta forma, o número total de conjuntos, é

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

Portanto, $2p \mid [(p-1)! - p + 1]$. Consequentemente, $p \mid [(p-1)! + 1]$, como desejado.

■

5 CONCLUSÃO

Despertar o interesse dos alunos para a Matemática não é uma tarefa fácil e na busca pela excelência no processo de ensino-aprendizagem se empregam várias estratégias. Com esse intuito, nossa proposta apresenta uma tática diferenciada para trabalhar análise combinatória e aritmética.

Acreditamos que o ensino de Matemática possa resultar em uma aprendizagem real e significativa para os estudantes, e para que isso ocorra, é fundamental a precisão da linguagem matemática, as demonstrações, as conexões e aplicações entre diferentes temas matemáticos e por isso, foi priorizado nesse trabalho a construção precisa dos conceitos e também a prova dos resultados apresentados sobre combinatória e aritmética.

A Análise Combinatória causa, comumente, um certo temor nos alunos, pela visão de possuir apenas problemas mecânicos envolvendo fórmulas. No entanto, trata-se de uma parte fascinante da Matemática que contém problemas de enunciado extremamente simples, mas que exigem, às vezes, para sua solução, raciocínios perspicazes e engenhosos.

A Teoria dos Números, tida como a rainha das matemáticas, é outra parte fascinante da Matemática que contém problemas muito interessantes, no entanto ainda é pouco trabalhada em sala de aula apesar de sua importância no Enem e em olímpiadas matemáticas.

Portanto, as aplicações combinatórias à teoria dos números nos fornecem caminhos alternativos para se abordar esses temas importantes em sala de aula e desse modo exercer um fascínio nos estudantes, despertando-os para o prazer que é a Matemática.

REFERÊNCIAS

[1] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar – Volume 1 – Números Reais** – Coleção do Professor de Matemática 2. ed. Rio de Janeiro: SBM, 2014.

[2] LIMA, E. L. et al. **A Matemática do Ensino Médio – Volume 1** – Coleção do Professor de Matemática 5. ed. Rio de Janeiro: SBM, 2001.

[3] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar – Volume 5 – Teoria dos Números** – Coleção do Professor de Matemática 2. ed. Rio de Janeiro: SBM, 2013.

[4] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar – Volume 3 – Introdução à Análise** – Coleção do Professor de Matemática 2. ed. Rio de Janeiro: SBM, 2013.

[5] LIMA, E. L. **Curso de Análise – Volume 1** – Projeto Euclides 12. ed. Rio de Janeiro: IMPA, 2007.

[6] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar – Volume 4 – Combinatória** – Coleção do Professor de Matemática 1. ed. Rio de Janeiro: SBM, 2012.

[7] SANTOS, J. P. O. **Introdução à Teoria dos Números** – Coleção Matemática Universitária 3 ed. Rio de Janeiro: Rio de Janeiro: IMPA, 2005.

[8] ANDREWS, G. E. **Number Theory** 1 ed. New York: DOVER, 1994.