UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RELATÓRIO DE INICIAÇÃO CIENTÍFICA

Tópicos da Teoria Aditiva dos Números: Partições de um Inteiro

Discente: *Igor Vallis Christ*
Orientador: *Prof. Dr. Victor do Nascimento Martins (DMPA - UFES)*

AGOSTO/2020

SUMÁRIO

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RESUMO

TÓPICOS DA TEORIA ADITIVA DOS NÚMEROS: PARTIÇÕES DE UM INTEIRO

O presente trabalho visa apresentar uma série de resultados e ideias sobre tópicos da teoria aditiva dos números, em particular, sobre as partições de um inteiro, trazendo consigo sua importância histórica no desenvolvimento da teoria dos números. Iniciamos apresentando alguns conceitos básicos da teoria dos números, para depois nos aprofundarmos no que de fato é o objetivo principal deste trabalho, os resultados acerca das partições de um inteiro e algumas de suas aplicações em outras áreas da matemática. Para realização do trabalho foi feita uma revisão bibliográfica dos principais autores do tema no Brasil, nos quais nos baseamos para dar sequência a este trabalho. Quanto aos resultados da pesquisa, podemos perceber a importância do desenvolvimento de pesquisas nessa área, além das fascinantes técnicas de demonstração matemática que utilizamos, e que, aqui serão apresentadas.

Palavras-chave: Teoria dos números, partições de inteiros, provas bijetivas, funções geradoras.

INTRODUÇÃO

Este estudo trata-se de uma explanação sobre um subtópico da teoria aditiva dos números, que chamamos de partições de um inteiro. O conceito básico das partições de um inteiro positivo é bem simples e não soa nada assustador. Como exemplo, imagine que você disponha de 4 camisas e queira guardá-las em uma cômoda que possua 4 gavetas. Você pode realizar essa tarefa das seguintes formas: guardar todas as 4 camisas em apenas uma gaveta; separá-las em dois grupos iguais e usar apenas duas gavetas; colocar 3 camisas em uma gaveta e 1 em outra; 2 camisas em uma gaveta, 1 em outra gaveta e 1 em outra diferente das duas anteriores; cada camisa em uma gaveta da cômoda. Basicamente, estamos separando as camisas em subconjuntos, e no caso das partições não importam as gavetas. Com auxílio do exemplo acima vimos que podemos escrever o número 4 das seguintes formas como soma de inteiros positivos: $4, 3+1, 2+2, 2+1+1$ e $1+1+1+1$. A analogia feita acima usando as camisas e as gavetas nos fez mostrarmos quais são as partições do inteiro 4, ou seja, as possíveis formas de escrever o número 4 como soma de inteiros positivos. Denotamos por $p(n)$ o número de partições de n. Como visto antes, temos que $p(4) = 5$.

A teoria aditiva dos números, pertence a grande área teoria dos números, a qual Gauss apelidou de "rainha da matemática", devido a sua grande importância. A teoria das partições possui muitos resultados clássicos e importantes que ajudaram no desenvolvimento da combinatória no século XX. Ela teve início no século XVIII com o Tratado de Euler, em que foi introduzido as partições de inteiros como nós conhecemos.

Muitos matemáticos, como Hardy, Schur, Sylvester e Ramanujan ajudaram a desenvolver a teoria. Srinivasa Ramanujan, matemático indiano, que em 2015 teve sua trajetória contada no filme "The man who knew infinity", enviou uma carta a Hardy onde demonstrava 120 teoremas que muitos sonhavam em demonstrar. Mais tarde, em Londres, em parceria com Hardy, vários resultados da teoria dos números foram demonstrados por Ramanujan.

E antes de morrer, Ramanujan ainda enunciou outros importantes resultados que posteriormente foram demonstrados por outros matemáticos. Os resultados, identidades e enunciados de Ramanujan impulsionaram consideravelmente a teoria das partições, tornando objeto de estudo de muitos matemáticos.

Neste trabalho, procuramos apresentar os conceitos iniciais da teoria das partições, bem como apresentar alguns resultados importantes. Nosso foco é nas duas mais utilizadas técnicas dentro da teoria: as provas bijetivas e o uso de funções geradoras. Este trabalho foi dividido em dois capítulos, que passamos a descrever a seguir.

O capítulo 1 trata-se de uma explanação sobre os conteúdos básicos da teoria dos números e alguns de seus resultados importantes. Para esta parte do trabalho usamos como base [1, 2, 3] e discorremos dentre outros tópicos sobre, a equivalência entre as duas formas do princípio de indução e o princípio da boa ordenação, além de, conceitos como divisibilidade, números primos, congruência linear e sequências recorrentes lineares.

O capítulo 2 é voltado diretamente para a teoria das partições de inteiros. Conceitos básicos serão definidos e então, passaremos a tratar das duas principais técnicas de seu desenvolvimento, as provas bijetivas e as funções geradoras. Buscamos demonstrar ou ao menos dar uma ideia dos resultados enunciados neste capítulo desenvolvidos pelos grandes matemáticos da área. Baseamos esta parte do trabalho em [4].

CAPÍTULO 1

FUNDAMENTOS DE ARITMÉTICA

Neste capítulo iremos de maneira sucinta introduzir alguns conceitos da teoria básica dos números, além de alguns resultados de extrema importância. Mostraremos a equivalência entre as duas formas do princípio de indução e o princípio da boa ordenação, além de tópicos de teoria números como divisibilidade, números primos, congruência linear e sequências recorrentes lineares. Para mais detalhes sugerimos [1, 2, 3].

1.1 Indução e boa ordenação

Nesta seção apresentaremos as duas formas do princípio de indução finita e o princípio da boa ordenação, que como veremos são equivalentes. Estas são ferramentas importantes na demonstração de muitos resultados na teoria dos números.

Princípio de indução finita (PIF) (1ª forma)

Suponha que para cada $n \geq n_0$ inteiro tenha-se uma afirmativa $P(n)$ que satisfaça as seguintes propriedades:

(i) $P(n_0)$ é verdadeira;

(ii) Sempre que $P(k)$ é verdadeira para algum $k \geq n_0$, então $P(k+1)$ é verdadeira.

Então $P(n)$ é verdadeiro para todo $n \geq n_0$.

Exemplo 1.1 *Vamos mostrar utilizando indução sobre n que*

$$S_n = \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}, \quad \forall n \geq 1.$$

(i) $S_1 = \frac{1}{1\times 2} = \frac{1}{2} = \frac{1}{1+1}$, *logo* $P(1)$ *é verdadeira.*

(ii) Suponha por hipótese de indução (HI) que o resultado seja válido para $n = k$*, isto é*

$$S_k = \frac{1}{1\times 2} + \frac{1}{2\times 3} + ... + \frac{1}{k(k+1)} = \frac{k}{k+1}.$$

Daí, se $n = k+1$*, temos*

$$\begin{aligned} S_{k+1} &= \frac{1}{1\times 2} + ... + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} \\ &\underbrace{=}_{HI} \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{k^2+2k+1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+1+1} \end{aligned}$$

Portanto, pelo princípio de indução finita, o resultado é valido para todo $n \geq 1$.

Princípio de indução finita (2ª forma)

Suponha que para cada inteiro $n \geq n_0$ se tenha uma afirmativa $P(n)$ que satisfaça:

(i) $P(n_0)$ é verdadeira.

(ii) Se $P(k)$ é verdadeira para todo k tal que $n_0 \leq k \leq n$ então $P(n+1)$ é verdadeiro.

Então $P(n)$ é verdadeira para todo $n \geq n_0$.

Exemplo 1.2 *A sequência de Fibonacci* F_n *é a sequência definida recursivamente por*

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}, \quad \forall n \geq 1.$$

Vamos mostrar que $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$*, onde* $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$ *são as raízes de* $x^2 = x+1$.

Primeiro note que $\alpha^2 = \alpha + 1$ *e* $\beta^2 = \beta + 1$*, daí temos*

$$\alpha^{n+1} = \alpha^n + \alpha^{n-1} \quad e \quad beta^{n+1} = \beta^n + \beta^{n-1}. \tag{1.1}$$

Agora, fazendo indução sobre n *temos:*

(i)

$$F_0 = \frac{\alpha^0 - \beta^0}{\alpha - \beta} = \frac{1-1}{\alpha - \beta} = 0; \qquad F_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta} = \frac{\alpha - \beta}{\alpha - \beta} = 1.$$

(ii) Suponha por hipótese de indução que a fórmula é válida para todo k, tal que $0 \leq k \leq n$, isto é,

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}.$$

Daí,

$$\begin{aligned} F_{n+1} = F_n + F_{n-1} &= \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \quad \text{(Pela hipótese de indução)} \\ &= \frac{\alpha^n + \alpha^{n-1} - (\beta^n + \beta^{n-1})}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \quad \text{(Por (1.1))}. \end{aligned}$$

Princípio da boa ordenação (PBO)

Dizemos que um conjunto $S \subset \mathbb{R}$ é **limitado inferiormente**, se existe um número $a \in \mathbb{R}$ tal que $a \leq s, \forall s \in S$. Neste caso , a é dito uma **cota inferior** de S. Se a cota inferior pertence a S, dizemos que ela é o **menor elemento** de S.

Proposição 1.1 (PBO) *Seja $S \subset \mathbb{Z}$ um conjunto não vazio limitado inferiormente. Então S possui menor elemento.*

Exemplo 1.3 *Usando o PBO vamos mostrar que*

$$S_n = \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}, \quad n \geq 1$$

Seja $F = \left\{n \in \mathbb{N}^* : S_n \neq \frac{n}{n+1}\right\}$ e suponha $F \neq \emptyset$. Já temos $F \subset \mathbb{Z}$, por construção e ainda

$$S_1 = \frac{1}{1 \times 2} = \frac{1}{1+1} \Rightarrow 1 \notin F \Rightarrow 1 \quad \text{é cota inferior de} \quad F.$$

Pelo PBO existe $a \in F$ menor elemento de F, daí $a - 1 \notin F$, isto é, $S_{a-1} = \dfrac{a-1}{a-1+1}$. Note *que,*

$$\begin{aligned} S_a &= \frac{1}{1\times 2} + \cdots + \frac{1}{(a-1)a} + \frac{1}{a(a+1)} \\ &= S_{a-1} + \frac{1}{a(a+1)} \\ &= \frac{a-1}{a} + \frac{1}{a(a+1)} \\ &= \frac{(a-1)(a+1)+1}{a(a+1)} \\ &= \frac{a^2}{a(a+1)} \\ &= \frac{a}{a+1}, \end{aligned}$$

o que é um absurdo, pois $a \in F$). *Portanto* $F = \emptyset$, *isto é,* $S_n = \frac{n}{n+1}, \forall n \geq 1$.

Proposição 1.2 *São equivalentes os seguintes princípios:*

(i) *PBO;*

(ii) *PIF(1ª forma);*

(iii) *PIF(2ª forma).*

Demonstração: Vamos mostrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$

Hipóteses:

- $P(n_0)$ é verdadeiro.
- $P(k)$ é verdadeiro $\Rightarrow P(k+1)$ é verdadeiro.
- PBO.

Tese: $P(n)$ é verdadeiro para todo $n \geq n_0$.

Seja F o conjunto dado por

$$F = \{n \geq n_0, n \in \mathbb{Z} : P(n) \quad \text{é falsa}\}.$$

Suponha $F \neq \emptyset$. $F \subset \mathbb{Z}$, por construção. Por hipótese $P(n_0)$ é verdadeiro, logo $n_0 \notin F$ e então n_0 é cota inferior de F. Pelo PBO, existe $k \in F$ menor elemento. Daí, $k-1 \notin F$ e então $P(k-1)$ é verdadeiro. Logo por hipótese $P(k)$ é verdadeiro, que é um absurdo, pois $k \in F$. Portanto $F = \emptyset$ e daí $P(n)$ é verdadeiro para todo inteiro $n \geq n_0$.

$(ii) \Rightarrow (iii)$

Hipóteses:

- $P(n_0)$ é verdadeiro.
- Se $P(k)$ é verdadeiro $\forall k \in \mathbb{N}$ tal que $n_0 \leq k \leq n$, então $P(n+1)$ também é verdadeiro.
- PIF (1ª forma).

Tese: $P(n)$ é verdadeiro $\forall n \geq 1$.

Por hipótese $P(n_0)$ é verdadeira, além disso, se $P(k)$ é verdadeira $\forall k \in \mathbb{N}$ tal que $n_0 \leq k \leq n$ então $P(n+1)$ é verdadeira. Em particular, $P(k+1)$ é verdadeira, logo pelo PIF (1ª forma), $P(n)$ é verdadeira $\forall\ n \geq n_0$.

$(iii) \Rightarrow (i)$

Hipóteses:

- $S \subset \mathbb{Z}$.
- $S \neq \emptyset$.
- S limitado inferiormente.
- PIF (2ª forma).

Tese: S possui menor elemento.

Suponha que S não possua menor elemento e considere a sentença $P(n)$: n não é um elemento de S. Como S é limitado inferiormente e não possui menor elemento, existe n_0 tal que $n_0 < s \quad \forall\ s \in S$. Portanto $n_0 \notin S$ e daí $P(n_0)$ é verdadeiro.

Assuma que $P(n)$ é verdadeiro $\forall\ n_0 \leq n \leq k$, logo $P(k+1)$ é verdadeiro também, pois se não fosse implicaria que $k+1$ seria um elemento de S e neste caso seria o menor elemento de S que por hipótese não existe. Então temos,

- $P(n_0)$ verdadeiro.

- $P(n)$ verdadeiro, $\forall\ n_0 \leq n \leq k \Rightarrow P(k+1)$ verdadeiro.

Daí, pelo PIF(2^{a} forma), $P(n)$ é verdadeiro para todo $n \geq n_0$. Logo $S = \emptyset$, o que contradiz a hipótese. Portanto S possui menor elemento.

■

1.2 Divisibilidade

Dentre os resultados apresentados nesta seção destacamos o Algoritmo da Divisão (Teorema 1.2), que nos garante a existência e a unicidade do quociente e resto na divisão de inteiros. Outro resultado importante será apresentado no Teorema 1.5 sobre a reprentação de um número em uma base. Demonstraremos também, alguns critérios de divisibilidade de números escritos na base 10.

Dados dois inteiros d e a, dizemos que d divide a e denotamos por $d \mid a$ se existir um inteiro q tal que $a = qd$. Caso contrário, escrevemos $d \nmid a$.

Exemplo 1.4 $-5 \mid 10$, *pois* $10 = -5(-2)$.

$10 \nmid -5$, *pois não existe* $q \in \mathbb{Z}$, *tal que* $-5 = q10$.

Lema 1.1 *Sejam* $a, b, c, d \in \mathbb{Z}$. *Temos:*

(i) Se $d \mid a$ *e* $d \mid b$ *então* $d \mid ax + by$ *para qualquer combinação linear* $ax + by$ *de* a *e* b *com coeficientes* $x, y \in \mathbb{Z}$.

(ii) (Limitação) Se $d \mid a$, *então* $a = 0$ *ou* $|d| \leq |a|$

(iii) (Transitividade) Se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração:

(i) Se $d \mid a$ e $d \mid b$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $a = q_1 d$ e $b = q_2 d$. Logo, $ax + by = q_1 dx + q_2 dy = d(q_1 x + q_2 y)$ e como $(q_1 x + q_2 y) \in \mathbb{Z}$ então $d \mid ax + by$.

(ii) Suponha que $d \mid a$ e $a \neq 0$. Daí, $a = qd$ e $q \neq 0$. Logo, $|q| \geq 1$ e $|a| = |q|\,|d| \geq |d|$ e portanto $|d| \leq |a|$.

(iii) Se $a \mid b$ e se $b \mid c$ então existem $d, e \in \mathbb{Z}$ tais que $b = ad$ e $c = be$. Daí, $c = ade = (de)a$. Portanto $a \mid c$.

■

1.2.1 Algoritmo da divisão, mdc, mmc

Apresentaremos a seguir o algortimo da divisão de Euclides (Teorema 1.2), tal algoritmo aparece no livro VII dos "Elementos"de Euclides, escrito por volta de 300 a.C. e nos garante existência e a unicidade do quociente e resto na divisão de inteiros. Antes disso, veremos o Teorema de Eudoxius (Teorema 1.1).

Teorema 1.1 (Eudoxius) *Se a e b são inteiros com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b. Em outras plavaras, se a e b são inteiros com $b \neq 0$, então existe um inteiro q tal que*

$$qb \leq a < (q+1)b \quad (se \quad b > 0) \quad e \quad qb \leq a < (q-1)b \quad (se \quad b < 0)$$

Teorema 1.2 (Algoritmo da Divisão) *Dados dois inteiros a e b com $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r \quad e \quad 0 \leq r < b$$

Demonstração: (Existência) Sejam a e b inteiros tais que $b > 0$. Pelo Teorema de Eudoxius, existe um inteiro q tal que $qb \leq a < (q+1)b$. Agora observe que, $a = qb + (a - qb)$ e $0 \leq a - qb < b$, já que

$$qb \leq a < (q+1)b \Rightarrow qb - qb \leq a - qb < (q+1)b - qb \Rightarrow 0 \leq a - qb < b.$$

Logo, existem inteiros q e $r = a - qb$ tais que $a = qb + r$ e $0 \leq r < b$.

(Unicidade) Suponha que existam inteiros r_1, r_2, q_1, q_2 tais que $a = q_1 b + r_1$, $a = q_2 b + r_2$, $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Daí, seque que

$$(q_1 - q_2)b = r_2 - r_1 \quad \text{e} \quad -b < r_2 - r_1 < b. \tag{1.2}$$

Em outras palavras, $r_2 - r_1$ é um múltiplo de b e está entre $-b$ e b. Logo $r_2 - r_1 = 0$, isto é, $r_1 = r_2$. Assim, de (1.2) obtemos $(q_1 - q_2)b = 0$. Como $b \neq 0$, temos que $q_1 - q_2 = 0$ e, consequentemente $q_1 = q_2$.

■

Definição 1.1 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$ e D_a e D_b o conjunto de divisores de a e b, respectivamente. $D_a \cap D_b$ é finita (pela"Limitação"(ii)) e não vazia já que o 1 pertence a $D_a \cap D_b$. Como $D_a \cap D_b$é finita, este conjunto possui elemento máximo, que chamaremos de **máximo divisor comum (mdc)** dos números a e b e denotamos mdc(a,b).*

Quando $a = b = 0$ convencionamos $mdc(0,0) = 0$ e quando $mdc(a,b) = 1$ dizemos que a e b são **primos entre si**.

Teorema 1.3 (Teorema de Bézout) *Se d é o máximo divisor comum de a e b, então existem inteiros m e n tais que*
$$d = ma + nb$$

Teorema 1.4 *Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração: Como $mdc(a,b) = 1$ pelo Teorema de Bézout existem inteiros m e n tais que $ma+nb = 1$. Multiplicando ambos os lados desta igualdade por c temos $m(ac)+n(bc) = c$. Como $a \mid ac$ e por hipótese, $a \mid bc$, então $a \mid c$. ■

Se denotarmos por M_n o conjunto dos múltiplos positivos de n, dados $a, b \in \mathbb{Z}$ com $a, b \neq 0$, então a interseção $M_a \cap M_b$ é não vazia (já que $|ab| \in M_a \cap M_b$), logo pelo PBO, $M_a \cap M_b$ possui elemento mínimo. Tal número é chamado **mínimo multiplo comum (mmc)** dos números a e b e o denotamos por mmc(a,b).

1.2.2 Representação de um número em uma base

Estamos tão acostumados com nosso sistema de representação na base 10, que dificilmente nos atentamos que essa, apesar de mais utilizada, não é a única forma de representar um número inteiro. Os computadores, por exemplo, trabalham na base 2. Vejamos de maneira bem simplificada como funciona a representação em outras bases. Seja $b \geq 2$ um número inteiro. Então todo número inteiro positivo a pode ser escrito de maneira única da seguinte forma:
$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$$
em que, $0 \leq a_i < b$, para todo $0 \leq i \leq n$.

Exemplo 1.5 *Vamos representar 32 na base 5. Primeiro observe que*

$$32 = 6 \times 5 + 2$$

$$6 = 1 \times 5 + 1$$

$$1 = 0 \times 5 + 1.$$

Agora note que

$$32 = 6 \times 5 + 2 = (1 \times 5 + 1) \times 5 + 2 = 1 \times 5^2 + 1 \times 5 + 2,$$

ou seja, a representação de 32 *na base* 5 *é* $(112)_5$*. Os algarismos* 1,1,2 *são exatamente os restos das divisões efetuadas, tomadas de baixo para cima.*

Teorema 1.5 *Dado um número natural $a \geq 0$ e um natural $b \geq 2$, existe e é única a representação de a na base b.*

Demonstração: Para $a = 0$, vemos que o resultado é, trivialmente, verdadeiro. Para $a > 0$, suponhamos por indução, que o resultado seja válido para todo natural c, $0 \leq c < a$, ou seja, suponhamos que c possa ser escrito de maneira única como

$$c = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0; \quad 0 \leq a_i < b.$$

Devemos mostrar que o resultado é verdadeiro para o natural a. Pelo Algoritmo da Divisão, existem e são únicos os naturais $q \geq 0$ e $0 \leq r < b$, tais que $a = qb + r$.

Se $q = 0$, então $a = r$. Neste caso a coincide com sua representação na base b.
Se $q > 0$, como $b \geq 2$, temos que

$$a = qb + r \geq 2q + r \geq 2q > q.$$

Logo, pela hipótese de indução, podemos escrever de modo único

$$q = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$$

e, portanto,

$$a = qb + r = a_n b^{n+1} + a_{n-1} b^n + \cdots + a_1 b^2 + a_0 b + r; 0 \leq r < b.$$

Obtemos, então, uma representação de a na base b. A unicidade dessa representação segue da unicidade de q e r, dados pelo Algoritmo da Divisão, e da unicidade da representação de q na base b (hipótese de indução).

■

Critérios de divisibilidade na base 10

Enunciaremos e demonstraremos agora alguns critérios de divisibilidade, supondo sempre que o número esteja na base 10, que é a mais utilizadas na prática.

Critério de divisibilidade por 2: Um número natural é divisível por 2 se, e somente se, o algarismo das unidades for divisível por 2.

Critério de divisibilidade por 3: Um número natural é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.

Critério de divisibilidade por 5: Um número natural é divisível por 5 se, e somente se, o algarismo das unidades for 0 ou 5.

Critério de divisibilidade por 9: Um número natural é divisível por 9 se, e somente se, a soma de seus algarismos for divisível por 9.

Critério de divisibilidade por 10: Um número natural é divisível por 10 se, e somente se, o algarismo das unidades for 0.

Demonstração: Começaremos com as demonstrações dos critérios de divisibilidade por 2, 5 e 10.

Seja a um número inteiro na base 10, assim podemos escrever

$$a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

em que, $0 \leq a_i \leq 9$, para todo $0 \leq i \leq n$. Colocando 10 em evidência temos:

$$a = 10(a_n 10^{n-1} + a_{n-1}10^{n-2} + \cdots + a_2 10 + a_1) + a_0$$

em que, $0 \leq a_i \leq 9$, para todo $0 \leq i \leq n$. Daí, a será divisível por 10 se, e somente se, a_0 for 0.

Se abrirmos o número 10 como o produto 2×5 temos

$$a = 2 \times 5(a_n 10^{n-1} + a_{n-1}10^{n-2} + \cdots + a_2 10 + a_1) + a_0$$

em que, $0 \leq a_i < 9$, para todo $0 \leq i \leq n$. Logo, a será um número divisível por 2 se, e somente se, a_0 for um número divisível por 2 e a será um número divisível por 5 se, e somente se, a_0 for 0 ou 5.

Agora para a demonstração dos critérios de divisibilidade por 3 e por 9 começaremos observando que

$$\begin{aligned} 10 &= 9 + 1 \\ 100 &= 99 + 1 \\ 1000 &= 999 + 1 \\ &\vdots \\ 10^n &= 999\cdots 9 + 1 \end{aligned}$$

e como a é um número inteiro na base 10, podemos escrever

$$a = a_n 10^n + \cdots + a_2 10^2 + a_1 10 + a_0$$

em que, $0 \leq a_i \leq 9$, para todo $0 \leq i \leq n$. Substituindo os valores das potências de 10 em a temos:

$$a = a_n(999\cdots 9 + 1) + \cdots + a_2(99 + 1) + a_1(9 + 1) + a_0$$

em que, $0 \leq a_i < 9$, para todo $0 \leq i \leq n$.

Fazendo a distributiva e colocando o 9 em evidência temos:

$$a = 9(a_n 111 \cdots 1 + \cdots + a_2 11 + a_1) + a_n + \cdots + a_1 + a_0$$

em que, $0 \leq a_i \leq 9$, para todo $0 \leq i \leq n$. Daí, a será divisível por 9 se, e somente se, a soma de seus algarismos for divisível por 9.

Agora se abrirmos o número 9 como o produto 3×3 e distribuirmos um três temos:

$$a = 3(a_n 333 \cdots 3 + \cdots + a_2 33 + a_1 3) + a_n + \cdots + a_1 + a_0$$

em que, $0 \leq a_i \leq 9$, para todo $0 \leq i \leq n$. Logo a será divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.

■

1.3 Números primos

Um número inteiro n ($n > 1$) possuindo somente dois divisores positivos, n e 1, é chamado **primo**. Se $n > 1$ não é primo dizemos que n é **composto**. Os números primos tem papel fundamental dentro da teoria dos números e seu estudo foi, e é objeto de trabalho de inúmeros matemáticos que se sentem desafiados e intrigados com a falta de resultados mais precisos sobre a distribuição destes números ou sobre quais os primos conhecidos. Diversas conjecturas sobre tais números ainda se encontram abertas até os dias atuais. Nesta seção traremos importantes resultados como o Teorema Fundamental da Aritmética (Teorema 1.6), que trata sobre a unicidade da representação de um inteiro como produto de potências de primos, o Teorema de Euclides (Teorema 1.7), sobre a infinidade de números primos e os teoremas 1.8 e 1.9, sobre os desertos arbitrariamente grandes de números primos e sobre o produto de k inteiros consecutivos ser divisível por $k!$.

Proposição 1.3 *Se $p \mid ab$, p primo, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \nmid a$, então $mdc(a, p) = 1$ o que implica, pelo Teorema 1.4, $p \mid b$ ■

Teorema 1.6 (Teorema Fundamental da Aritmética) *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m,$$

onde $m \geq 1$ é um natural e $p_1 \leq \cdots \leq p_m$ são primos.

Teorema 1.7 (Euclides) *A sequência dos números primos é infinita.*

Demonstração: Suponha, por absurdo, que existe apenas um número finito de números primos. Seja $p_1, p_2, \cdots, p_k$ o conjunto de todos os números primos. Considere o número $n = p_1 \cdot p_2 \cdots p_k + 1$. Obviamente, para cada $i \in \{1, 2, \cdots, k\}$, têm-se $p_i \nmid n$. Por outro lado, pelo Teorema Fundamental da Aritmética, ou n é primo ou pode ser escrito como um produto de números primos. Absurdo, pois se n fosse primo teríamos $n = p_i$ (em particular, $p_i \mid n$) para algum $i \in \{1, 2, \cdots, k\}$ e se n tivesse um fator primo então n seria divisível por algum p_i, em que $i \in \{1, 2, \cdots, n\}$. ∎

Teorema 1.8 *Para qualquer inteiro k, existem k inteiros consecutivos todos compostos. Em outras palavras, existem "desertos"arbitrariamente grandes de números primos.*

Demonstração: Para qualquer inteiro $k \geq 1$, o inteiro $(k+1)!$ é divisível por todos os inteiros entre 2 e $k+1$, incluindo o 2 e o $k+1$. Logo os k números consecutivos

$$(k+1)! + 2, \quad (k+1)! + 3, \quad \ldots, \quad (k+1)! + k, \quad (k+1)! + (k+1)$$

são compostos pois, $(k+1)! + 2$ é múltiplo de 2, $(k+1)! + 3$ é múltiplo e 3, e assim sucessivamente até $(k+1)! + (k+1)$ que é múltiplo de $(k+1)$. Isto mostra que existem "desertos"arbitrariamente grandes de números primos. ∎

Teorema 1.9 *O produto de k inteiros consecutivos é divisível por $k!$.*

Demonstração: Sejam a e k inteiros tais que $a \geq 0$ e $k > 0$. Note que

$$\frac{(a+1)(a+2)(a+3)\cdots(a+k)}{k!} = \frac{(a+k)!}{a!k!} = \binom{a+k}{k}.$$

Como $\binom{a+k}{k}$ é inteiro, segue que $(a+1)(a+2)\cdots(a+k)$ é divisível por $k!$. Isto mostra que o produto de k inteiros positivos consecutivos é divisível por $k!$. Se a sequência tiver somente números negativos o resultado pode ser provado de forma análoga (no máximo teremos uma mudança de sinal). Se a sequência tiver números negativos e positivos, ela irá conter o zero e, consequentemente, o produto será zero, que obviamente é múltiplo de $k!$. ∎

1.4 Congruência linear

Uma equação da forma $ax + by = c$, na qual x e y são variáveis e a, b e c são constantes (números inteiros), em que estamos interessados apenas nos pares (x, y) de números inteiros que satisfazem a equação $ax + by = c$, é chamada de *equação diofantina linear.*

Teorema 1.10 *Sejam a e b inteiros e $d = mdc(a, b)$. Temos que*

(i) se $d \nmid c$, então a equação $ax + by = c$ não adimite solução inteira.

(ii) se $d \mid c$, então a equação $ax+by = c$ possui solução e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por

$$x = x_0 + \left(\frac{b}{d}\right) k \quad e \quad y = y_0 - \left(\frac{a}{d}\right) k \quad (k \in \mathbb{Z}).$$

Demonstração:

(i) Suponha que a equação $ax + by = c$ possua solução inteira. Assim, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = c$. Como $d = mdc(a, b)$, segue que $d \mid a$ e $d \mid b$ e, consequentemente, $d \mid (ax_0 + by_0)$, isto é, $d \mid c$. Portanto se $d \nmid c$, então a equação $ax + by = c$ não admite solução inteira.

(ii) Sejam a, b e c inteiros tais que $d = mdc(a, b)$ e $d \mid c$. Como $d = mdc(a, b)$, pelo Teorema de Bézout existem inteiros x_0 e y_0 tais que

$$ax_0 + by_0 = d. \tag{1.3}$$

Mas $d \mid c$, isto é, existe um inteiro k tal que $c = kd$. Multiplicando ambos os lados da igualdade (1.3) por k, obtemos $a(kx_0) + b(ky_0) = c$. Isto mostra que a equação $ax + by = c$ possui pelo menos uma solução inteira.

Agora vamos mostrar que se (x_0, y_0) é uma solução da equação $ax + by = c$, então $\left(x = x_0 + \left(\frac{b}{d}\right) k, y = y_0 - \left(\frac{a}{d}\right) k\right)$, $k \in \mathbb{Z}$ é também uma solução desta equação. Com efeito, observe que

$$a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) = ax_0 + by_0 + \left(\frac{ab}{d} - \frac{ab}{d}\right) k = ax_0 + by_0 = c.$$

Para concluir a demonstração, resta mostrar que se x e y são inteiros tais que $ax+by = c$ então $x = x_0 + \left(\frac{b}{d}\right) k$ e $y = y_0 - \left(\frac{a}{d}\right) k$ para algum $k \in \mathbb{Z}$. Com efeito, temos que $ax + by = c$ e $ax_0 + by_0 = c$. Logo

$$(ax + by) - (ax_0 + by_0) = 0 \Rightarrow a\,(x - x_0) = b\,(y_0 - y) \Rightarrow \frac{a}{d}\,(x - x_0) = \frac{b}{d}\,(y_0 - y) \tag{1.4}$$

mas $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, logo $\frac{a}{d} \mid (y_0 - y)$ e consequentemente, $y = y_0 - \frac{ak}{d}$ para algum $k \in \mathbb{Z}$. Substituindo $y = y_0 - \frac{ak}{d}$ em (1.4), temos $x = x_0 + \frac{bk}{d}$.

∎

Exemplo 1.6 *Vamos resolver a equação diofantina* $32x + 9y = 3$*. Primeiramente vamos encontrar uma solução particular para a equação:*

$$32 = 3 \times 9 + 5 \Leftrightarrow 5 = 32 - 3 \times 9 \tag{1.5}$$

$$9 = 1 \times 5 + 4 \Leftrightarrow 4 = 9 - 1 \times 5 \tag{1.6}$$

$$5 = 1 \times 4 + 1 \Leftrightarrow 1 = 5 - 1 \times 4 \tag{1.7}$$

$$4 = 4 \times 1 + 0$$

Disso, temos que o $mdc(32, 9) = 1$ *e usando* $(1.5), (1.6), (1.7)$*, temos*

$$\begin{aligned} 1 &= 5 - 1 \times 4 \\ &= 5 - 1 \times (9 - 1 \times 5) \\ &= 2 \times 5 - 1 \times 9 \\ &= 2 \times (32 - 3 \times 9) - 1 \times 9 \\ &= 2 \times 32 - 7 \times 9. \end{aligned}$$

Logo $1 = 2 \times 32 - 7 \times 9$ *e consequentemente,* $3 = 6 \times 32 - 21 \times 9$*. Daí,* $(6, -21)$ *é solução da equação* $32x + 9y = 3$*. Pelo teorema anterior, o conjunto solução da equação diofantina é*

$$S = \{(6 + 9k, -21 - 32k)\,,\ k \in \mathbb{Z}\}\,.$$

Definição 1.2 *Sejam* a *e* b *inteiros. Dizemos que* a *é* ***congruente*** *a* b *módulo* m $(m > 0)$ *se* $m \mid (a - b)$ *e denotamos isto por* $a \equiv b \bmod m$*. Se* $m \nmid (a - b)$ *dizemos que* a *é* ***incongruente*** *a* b *módulo* m *e denotamos isto por* $a \not\equiv b \bmod m$*.*

Definição 1.3 *Uma* ***congruência linear*** *em uma variável é uma congruência da forma* $ax \equiv b \bmod m$ *na qual* x *é a incógnita.*

Teorema 1.11 *Sejam* a*,* b *e* m *inteiros tais que* $m > 0$ *e* $mdc(a, m) = d$*. No caso em que* $d \nmid b$*, a congruência* $ax \equiv b \bmod m$ *não possui nenhuma solução e quando* $d \mid b$*, ela possui exatamente* d *soluções incongruentes módulo* m*.*

Observação 1.1 *Note que o que o Teorema 1.11 nos diz é que dada uma congruência linear do tipo* $ax \equiv b \bmod m$*, aplicando a definição de congruência, estamos procurando* x *inteiro tal que* $m \mid (ax - b)$ *e daí temos* $ax - b = my$ *para algum* $y \in \mathbb{Z}$ *e consequentemente* $ax - my = b$ *para algum* $y \in \mathbb{Z}$*.*

Por outro lado, vimos que a equação diofantina $ax - my = b$ *admite solução inteira se, e somente se,* $d \mid b \quad (d = mdc(a,m))$ *e neste caso a solução geral é*

$$x = x_0 - \left(\frac{m}{d}\right)k, \qquad y = y_0 - \left(\frac{a}{d}\right)k, \quad com \quad k \in \mathbb{Z},$$

onde (x_0, y_0) *é uma solução particular. Logo a congruência linear* $ax \equiv b \ mod \ m$ *admite solução se, e somente se,* $d \mid b$ *e neste caso todas as soluções são da forma*

$$x = x_0 - \left(\frac{m}{d}\right)k, \quad com \quad k \in \mathbb{Z}$$

onde x_0 *é uma solução particular.*

Para encerrar essa seção, vamos enunciar alguns resultados clássicos da teoria dos números envolvendo congruências.

Teorema 1.12 (Teorema de Wilson) *Se* p *é primo, então* $(p-1)! \equiv -1 \ mod \ p$.

Teorema 1.13 (Pequeno Teorema de Fermat) *Seja* p *primo. Se* $p \nmid a$ *então* $a^{p-1} \equiv 1 \ mod \ p$.

Se n é um inteiro positivo, a **função ϕ de Euler**, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores ou iguais a n que são relativamente primos com n.

Teorema 1.14 (Euler) *Se* m *é um inteiro positivo e* a *um inteiro com* $mdc(a,m) = 1$, *então* $a^{\phi(m)} \equiv 1 \ mod \ m$.

Teorema 1.15 (Teorema do Resto Chinês) *Se* $mdc(a_i, m_i) = 1$, $mdc(m_i, m_j) = 1$ *para* $i \neq j$ *e* c_i *inteiro, então o sistema*

$$\begin{gathered} a_1 x \equiv c_1 mod m_1 \\ a_2 x \equiv c_2 mod m_2 \\ a_3 x \equiv c_3 mod m_3 \\ \vdots \\ a_r x \equiv c_r mod m_r \end{gathered}$$

possui solução e a solução é única módulo m, *onde* $m = m_1 \cdot m_2 \cdots m_r$.

1.5 Sequências recorrentes lineares

Sequências recorrentes são sequências $x_0, x_1, x_2, \ldots$ em que cada termo é determinado por uma dada função dos termos anteriores. Dado um inteiro positivo k, uma **sequência recorrente de ordem** k é uma sequência em que cada termo é determinado como uma função dos k termos anteriores:

$$x_{n+k} = f(x_{n+k-1}, x_{n+k-2}, \ldots, x_{n+1}, x_n), \quad \forall n \in \mathbb{N}.$$

Uma sequência $(x_n)_{n\in\mathbb{N}}$ é uma **sequência recorrente linear de ordem** k (k é um inteiro positivo) se existem constantes (reais ou complexas) $c_1, c_2, \ldots, c_k$ tais que

$$x_{n+k} = \sum_{j=1}^{k} c_j x_{n+k-j} = c_1 x_{n+k-1} + c_2 x_{n+k-2} + \cdots + c_k x_n, \quad \forall n \in \mathbb{N}.$$

Tais sequências são determinadas pelos seus k primeiros termos $x_0, \cdots, x_{k-1}$.

Exemplo 1.7 *Progressões geométricas:* $x_n = aq^n \Rightarrow x_{n+1} = qx_n, \quad \forall n \in \mathbb{N}$, *em que* (x_n) *é uma sequência recorrente linear de ordem* 1.

Exemplo 1.8 *Se* (x_n) *é uma progressão aritmética, existe uma constante* r *tal que* $x_{n+1} - x_n = r, \quad \forall n \in \mathbb{N}$, *donde* $x_{n+2} - x_{n+1} = x_{n+1} - x_n, \quad \forall n \in \mathbb{N}$, *ou seja,* $x_{n+2} = 2x_{n+1} - x_n, \quad \forall n \in \mathbb{N}$. *Logo,* (x_n) *é uma sequência recorrente linear de ordem* 2.

Exemplo 1.9 *Se* $x_n = P(n)$ *onde* P *é um polinômio de grau* k, *então* (x_n) *satistaz a recorrência linear de ordem* $k+1$ *dada por*

$$x_{n+k+1} = \sum_{j=0}^{k} (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \quad \forall n \in \mathbb{N}.$$

Isso é evidente se $k = 0$ *(isto é, se* P *é constante), pois*

$$\begin{aligned} x_{n+1} &= \sum_{j=0} (-1)^j \binom{0+1}{j+1} x_{n-j}, \quad \forall n \in \mathbb{N} \\ &= (-1)^0 \binom{1}{1} x_{n-0} = 1 \left(\frac{1!}{0!1!}\right) x_n = x_n, \quad \forall n \in \mathbb{N}. \end{aligned}$$

Provando agora o caso geral por indução, suponha o resultado válido para polinômios de grau menor que k. *Se* P *é um polinômio de grau* $k \geq 1$ *então* $Q(x) = P(x+1) - P(x)$ *é um polinômio de grau* $k-1$, *donde, por hipótese de indução,* $y_n = x_{n+1} - x_n = Q(n)$ *satisfaz a recorrência*

$$y_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} y_{n+k-1-j}, \quad \forall n \in \mathbb{N},$$

donde,

$$x_{n+k+1} - x_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} (x_{n+k-j} - x_{n+k-j-1}), \quad \forall n \in \mathbb{N}$$

e logo,

$$x_{n+k+1} = \sum_{j=0}^{k} (-1)^j \left(\binom{k}{j+1} + \binom{k}{j} \right) x_{n+k-j} = \sum_{j=0}^{k} (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \quad \forall n \in \mathbb{N}.$$

Exemplo 1.10 *Seja $x_n = (an+b)q^n$, donde a, b, q são constantes. Temos que*

$$\begin{aligned} x_{n+1} - qx_n &= [a(n+1)+b]q^{n+1} - q(an+b)q^n \\ &= q^{n+1}(an + a + b - an - b) \\ &= aq^{n+1}. \end{aligned}$$

Ou seja,

$$x_{n+1} - qx_n = aq^{n+1}$$

é uma progressão geométrica de razão q, logo

$$x_{n+2} - qx_{n+1} = q(x_{n+1} - qx_n) \Rightarrow x_{n+2} = 2qx_{n+1} - q^2 x_n, \quad \forall n \in \mathbb{N},$$

portanto (x_n) é uma sequência recorrente linear de ordem 2.

O conjunto das sequências que satisfazem uma dada recorrência linear

$$x_{n+k} = \sum_{j=1}^{k} c_j x_{n+k-j}, \quad \forall n \in \mathbb{N}$$

é um espaço vetorial, isto é, dadas duas sequências (y_n) e (z_n) que satisfazem esta recorrência (ou seja, $y_{n+k} = \sum_{j=1}^{k} c_j y_{n+k-j}$ e $z_{n+k} = \sum_{j=1}^{k} c_j z_{n+k-j}, \quad \forall n \in \mathbb{N}$) e uma constante a, a sequência (w_n) dada por $w_n = y_n + az_n$, satisfaz a mesma recorrência: $w_{n+k} = \sum_{j=1}^{k} c_j w_{n+k-j}, \quad \forall n \in \mathbb{N}$.

É bastante usual, dada uma sequência (x_n), estudar a sequência obtida pela soma de seus n primeiros termos $s_n = \sum_{k \le n} x_k$. Se (x_n) é uma sequência recorrente linear, (s_n) também é. De fato,

$$s_{n+1} - s_n = \sum_{k \le n+1} x_k - \sum_{k \le n} x_k = x_{n+1}, \quad n \in \mathbb{N}.$$

Se $x_{n+k} = \sum_{j=1}^{k} c_j x_{n+k-j}$, temos

$$s_{n+k+1} - s_{n+k} = x_{n+k+1} = \sum_{j=1}^{k} c_j x_{n+k+1-j} = \sum_{j=1}^{k} c_j(s_{n+k+1-j} - s_{n+k-j}), \forall n \in \mathbb{N},$$

donde,

$$\begin{aligned}
s_{n+k+1} &= \sum_{j=1}^{k} c_j(s_{n+k+1-j} - s_{n+k-j}) + s_{n+k} \\
&= \sum_{j=1}^{k} c_j(s_{n+k+1-j} - \sum_{j=1}^{k} c_j(s_{n+k-j}) + s_{n+k} \\
&= c_1 s_{n+k} + \sum_{j=2}^{k} c_j s_{n+k+1-j} - c_k s_n - \sum_{j=1}^{k-1} c_j s_{n+k-j} + s_{n+k} \\
&= (1 + c_1)s_{n+k} + \sum_{j=1}^{k-1} c_{j+1} s_{n+k-j} - \sum_{j=1}^{k-1} c_j s_{n+k-j} - c_k s_n
\end{aligned}$$

$$\begin{aligned}
&= (1 + c_1)s_{n+k} + \sum_{j=1}^{k-1} (c_{j+1} s_{n+k-j}) - (c_j s_{n+k-j}) - c_k s_n \\
&= (1 + c_1)s_{n+k} + \sum_{j=1}^{k-1} s_{n+k-j}(c_{j+1} c_j) - c_k s_n \\
&= (1 + c_1)s_{n+k} + \sum_{j=2}^{k} s_{n+k-j+1}(c_j - c_{j-1}) - c_k s_n
\end{aligned}$$

Seja $d_1 = 1 + c_1, d_j = c_j - c_{j-1}$, $\forall\ j = 2, \cdots, k$ e $d_{k+1} = c_j$, daí

$$s_{n+k+1} = d_1 s_{n+k} + \sum_{j=2}^{k} d_j s_{n+k-j+1} + d_{k+1} s_n = \sum_{j=1}^{k+1} d_j s_{n+k-j+1}.$$

1.5.1 A sequência de Fibonacci

A **sequência de Fibonacci** é a sequência numérica proposta pelo matemático Leonardo Pisa, mais conhecido como Fibonacci: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$ Foi a partir de um problema criado por ele que o mesmo detectou a existência de uma regularidade matemática. Trata-se do exemplo clássico dos coelhos, em que Fibonacci descreve o crescimento de uma população desses animais. A sequência é definida pela seguinte recorrência: $F_{n+2} = F_{n+1} + F_n$. A partir dessa sequência, pode ser construído um retângulo, que é chamado de **retângulo de ouro**. Ao desenhar um arco dentro desse retângulo, obtemos a **espiral de Fibonacci**. A verdade é que a sequência de Fibonacci pode ser percebida na natureza. São exemplos disso as folhas das árvores, as pétalas das rosas, os frutos como o abacaxi, as conchas espiraladas dos caracóis ou as galáxias.

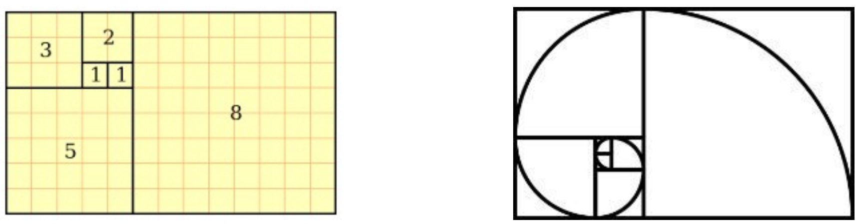


Figura 1.1: Retângulo de ouro e espiral de Fibonacci.

Outro fato interessante, que foi percebido por Fibonacci a respeito da sequência que recebe seu nome, é que o quociente de um número da sequência com o seu antecessor, converge a uma constante com o valor aproximado de 1,618, chamada de **número de ouro**. Ela é aplicada em análises financeiras e na informática e foi utilizada por Da Vinci, que a chamou de *divina proporção*, para fazer desenhos perfeitos. Fibonacci apresentou sua sequência e suas observações a respeito dela no seu livro Liber Abaci (Livro do Ábaco, em português), o qual data de 1202.

Encontrando uma função explícita para F_n

Como dito anteriormente a sequência de Fibonacci é definida por

$$F_0 = 0,\ F_1 = 1 \quad \text{e} \quad F_{n+2} = F_{n+1} + F_n \quad \forall\, n \in \mathbb{N}.$$

Buscamos agora, uma fórmula explícita para F_n em função de n. Para conseguirmos, procuraremos progressões geométricas que satisfazem a mesma recorrência de F_n, ou seja,

$$x_n = aq^n, \quad a, q \neq 0$$

satisfaz

$$x_{n+2} = x_{n+1} + x_n,\ \forall\, n \in \mathbb{N},$$

o que implica que

$$aq^{n+2} = aq^{n+1} + aq^n = aq^n(q+1)$$

em que $q+1=q^2$. Teremos assim dois valores possíveis para q, as duas raízes da equação $q^2-q-1=0$, que são $\frac{1-\sqrt{5}}{2}$ e $\frac{1+\sqrt{5}}{2}$. Logo, sequências da forma $a\left(\frac{1+\sqrt{5}}{2}\right)^n$ e $b\left(\frac{1-\sqrt{5}}{2}\right)^n$ satisfazem a recorrência acima, consequentemente as sequências da forma $y_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$ também satisfazem a recorrência.

Basta agora encontrarmos valores de a e b tais que $y_0 = 0$ e $y_1 = 1$ para que tenhamos $y_n = F_n$ para todo n (de fato, teríamos $y_0 = F_0, y_1 = F_1$, e por indução se $k \geq 2$ e $y_n = F_n$ para todo $n < k$, temos $y_k = y_{k-1} + y_{k-2} = F_{k-1} + F_{k-2} = F_k$). Para isso, devemos ter:

$$\begin{cases} a+b=0 \\ a\left(\frac{1+\sqrt{5}}{2}\right) + b\left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{cases}$$

e portanto $a = \frac{1}{\sqrt{5}}$ e $b = -\frac{1}{\sqrt{5}}$. Mostramos assim que

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right), \quad \forall n \in \mathbb{N}.$$

Proposição 1.4 $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n, \quad \forall\ m, n \in \mathbb{N},\ n \geq 1.$

Demonstração: Sejam $y_m = F_{m+n}$ e $z_m = F_m F_{n-1} + F_{m+1} F_n$. Temos que (y_m) e (z_m) satistazem a recorrência $x_{n+2} = x_{n+1} + x_n, \forall n \in \mathbb{N}$. Note que

$$y_0 = F_n;$$

$$y_1 = F_{n+1};$$

$$z_0 = 0 \times F_{n-1} + 1 \times F_n = F_n = y_0;$$

$$z_1 = 1 \times F_{n-1} + 1 \times F_n = F_{n+1} = y_1,$$

portanto como antes $z_n = y_n$, consequentemente, $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$, $\forall\ m, n \in \mathbb{N},\ n \geq 1$.

■

Teorema 1.16 $mdc(F_m, F_n) = F_{mdc(m,n)}, \quad \forall\ m, n \in \mathbb{N}$

Demonstração: Observe primeiro que $mdc(F_n, F_{n+1}) = 1, \quad \forall n \in \mathbb{N}$. Isto vale para $n = 0$, pois $F_0 = 0$ e $F_1 = 1$ e, por indução

$$mdc(F_{n+1}, F_{n+2}) = mdc(F_{n+1}, F_{n+1} + F_n) = mdc(F_{n+1}, F_n) = 1. \tag{1.8}$$

Agora note que, se $m = 0$, $mdc(F_m, F_n) = mdc(0, F_n) = F_n = F_{mdc(m,n)}, \forall n \in \mathbb{N}$ e se $m = 1$, $mdc(F_m, F_n) = mdc(1, F_n) = 1 = F_1 = F_{mdc(m,n)}, \forall n \in \mathbb{N}$. Fazendo indução sobre

m. Suponha que a afirmação do enunciado seja válida para todo $m < k$ (onde $k \geq 2$ é um inteiro dado) e para todo $n \in \mathbb{N}$, ou seja,

$$mdc(F_m, F_n) = F_{mdc(m,n)}, \quad \text{se} \quad m < k.$$

Queremos provar que, dado $n \in \mathbb{N}$, vale pra $m = k$, isto é, que $mdc(F_k, F_n) = F_{mdc(k,n)}$. Fazendo indução sobre n, temos que se $n = 0$, é claro que

$$mdc(F_k, F_n) = mdc(F_k, F_0) = mdc(F_k, 0) = F_k = F_{mdc(k,0)}.$$

Suponha por hipótese de indução que

$$mdc(F_k, F_r) = F_{mdc(k,r)},$$

para todo $r < n$. Então, dado $n \in \mathbb{N}$, temos dois casos a considerar:
Se $n < k$, $mdc(F_k, F_n) = mdc(F_n, F_k) = F_{mdc(n,k)} = F_{mdc(k,n)}$, pela hipótese de indução sobre m.

Se $n \geq k$,

$$F_n = F_{(n-k)+k} \underbrace{=}_{Prop.1.4} F_{n-k}F_{k-1} + F_{n-k+1}F_k,$$

logo

$$\begin{aligned} mdc(F_k, F_n) &= mdc(F_k, F_{n-k}F_{k-1} + F_{n-k+1}F_k) = mdc(F_k, F_{n-k}F_{k-1}) \\ &\underbrace{=}_{(1.8)} mdc(F_k, F_{n-k}) \underbrace{=}_{\text{hip. ind. sobre } n} F_{mdc(k,n-k)} = F_{mdc(k,n)}. \end{aligned}$$

$\blacksquare$

CAPÍTULO 2

PARTIÇÕES DE INTEIROS

Neste capítulo, iremos apresentar o nosso principal objeto de estudo neste trabalho, a teoria das partições. Compreender, ainda que basicamente, a teoria das partições, requer passar pelas duas principais técnicas utilizadas no seu desenvolvimento: as provas bijetivas e as funções geradoras. Na Seção 2.3, veremos como utilizar bijeções na demonstração de resultados envolvendo partições. E na Seção 2.4, apresentaremos e utilizaremos em demonstrações as funções geradoras, o que por alguns estudiosos, foi a maior contribuição para o estudo das partições de inteiros. Tentamos demonstrar, ou pelo menos dar a ideia das provas, da maioria dos resultados aqui apresentados, entretanto, muitos outros resultados foram omitidos, sendo assim, sugerimos, como passo inicial no estudo das partições, o texto apresentado em [4].

Definição 2.1 *Para cada inteiro positivo n, $p(n)$ é o número de maneiras de se representar n como soma de inteiros positivos, chamados partes, na qual a ordem dessas partes não importa. Cada uma dessas somas é chamada de* ***partição*** *de n.*

Exemplo 2.1 *Seguem listadas abaixo as partições de* 3, 4, 5 *e* 6.

3	4	5	6
$2+1$	$3+1$	$4+1$	$5+1$
$1+1+1$	$2+2$	$3+2$	$4+2$
	$2+1+1$	$3+1+1$	$4+1+1$
	$1+1+1+1$	$2+2+1$	$3+3$
		$2+1+1+1$	$3+2+1$
		$1+1+1+1+1$	$3+1+1+1$
			$2+2+2$

$2+2+1+1$ $\qquad$ $2+1+1+1+1$ $\qquad$ $1+1+1+1+1+1$

Do exemplo acima temos que $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ e $p(6) = 11$, além disso, quando falarmos de partições de 0, nós a definiremos como sendo igual a 1, ou seja, $p(0) = 1$, já que o único conjunto que a representaria seria o vazio. Para termos uma noção de quão rápido é o crescimento de $p(n)$ listamos a seguir alguns valores: $p(20) = 627$, $p(100) = 190569292$, $p(200) = 3972999029388$. Note que, pela definição, em uma partição de n nenhuma parte supera n, além disso, a ordem das partes não está sendo considerada.

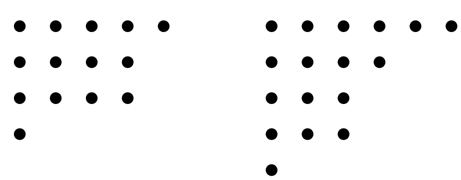
Seja $p_k(n)$, o número de partições de n tendo k como a maior parte. Com ajuda do Exemplo 2.1 temos que $p_2(3) = 1$, $p_3(5) = 2$, $p_4(5) = 1$, $p_5(6) = 1$ e $p_3(6) = 3$. Para um inteiro qualquer, temos: $p_n(n) = 1$ e $p_k(n) = 0$, se $k > n$ e além disso, $\displaystyle\sum_{k=1}^{n} p_k(n) = p(n)$.

2.1 Representações gráficas de partições

As representações gráficas das partições são fundamentais no estudo da teoria. Elas facilitam, por exemplo, a compreensão de diversas demonstrações. No decorrer do trabalho, ficará natural ao falarmos de uma dada partição, associarmos algumas das suas representações gráficas que apresentaremos.

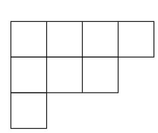
Uma partição de um inteiro n positivo pode ser representada graficamente por meio de um arranjo de n pontos no plano, constituído de s linhas em ordem não crescente. Em cada linha deste arranjo colocamos um número de pontos igual a cada uma de suas partes. Chamamos essa representação de **gráfico de Ferrers** da partição.

Exemplo 2.2 *Os gráficos de Ferrers das partições* $5+4+4+1$ *e* $6+4+3+3+1$ *são, respectivamente*



Uma representação gráfica de uma partição na qual usaremos quadrados em vez de pontos na representação de Ferrers será chamada de **diagrama de Young**.

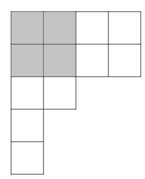
Exemplo 2.3 *A representação da partição* $4+3+1$ *de* 8 *no diagrama de Young é*



Observação 2.1 *Utilizaremos principalmente a representação por pontos, mas ao nos referirmos ao gráfico de Ferrers, podemos também considerar a representação pelos pequenos quadrados.*

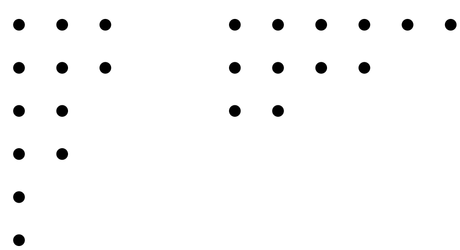
Definição 2.2 *O* ***quadrado de Durfee*** *de uma partição é o maior quadrado que conseguimos colocar "dentro"do gráfico de Ferrers de uma partição, exigindo-se que seu canto superior esquerdo coincida com o canto superior esquerdo do gráfico de Ferrers.*

Exemplo 2.4 *A partição* $4+4+2+1+1$ *tem quadrado de Durfee de lado* 2.

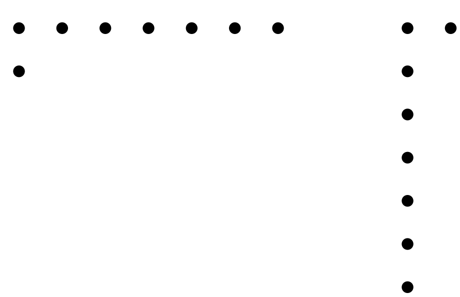


Se no gráfico de Ferrers de uma partição de n trocarmos as linhas pelas colunas, obtemos o gráfico de Ferrers de uma outra partição de n, que chamaremos de **partição conjugada** da partição considerada.

Exemplo 2.5 *Os gráficos de Ferrers das partições* $3+3+2+2+1+1$ *e sua respectiva conjugada* $6+4+2$ *são*



Exemplo 2.6 *Os gráficos de Ferrers das partições* $7+1$ *e sua respectiva conjugada* $2+1+1+1+1+1+1$ *são*



Como veremos nos resultados a seguir, a representação gráfica de uma partição é de grande utilidade em demonstrações. A partir de agora, iremos associar uma partição a sua representação em um gráfico de Ferrers, de modo que quando falarmos da conjugação de uma partição estaremos nos referindo a conjugação de seu gráfico de Ferrers.

Teorema 2.1 *Seja $q_k(n)$ o número de partições de n tendo exatamente k partes. O número $p_k(n)$ de partições de n tendo k como a maior parte é igual ao número $q_k(n)$.*

Demonstração: Usando a operação "conjugação"definida no conjunto das partições de n, teremos que toda partição de n tendo k como maior parte é transformada em uma partição possuindo exatamente k partes e vice-versa. ■

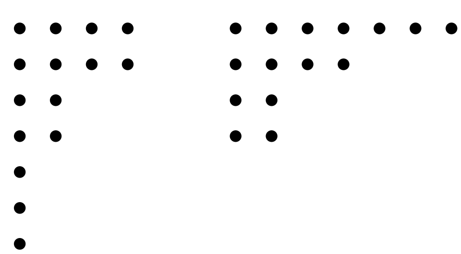
Corolário 2.1 *Seja n um inteiro positivo. O número de partições de n com partes menores ou iguais a k é igual ao número de partições de n com no máximo k partes.*

Demonstração: Da mesma forma, como no teorema anterior, basta usarmos a operação "conjugação". ■

Teorema 2.2 *Seja n um inteiro positivo. O número de partições de n em que cada parte aparece pelo menos duas vezes é igual ao número de partições de n em partes maiores do que 1 e tais que inteiros consecutivos não aparecem como partes.*

Demonstração: Usando novamente a operação conjugação de uma partição de n na qual cada parte aparece ao menos duas vezes, teremos uma partição com partes maiores do que 1 e com inteiros consecutivos não aparecendo como pares e vice-versa. ■

Como exemplo da demonstração acima observemos o gráfico de Ferrers da partição $4+4+2+2+1+1+1$ e de sua conjugada $7+4+2+2$:



Vemos que, pelo fato de cada parte aparecer pelo menos duas vezes, na partição conjugada, a menor parte será pelo menos 2 e que inteiros consecutivos não poderão ocorrer como partes.

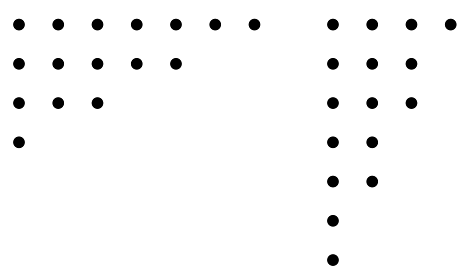
No que segue, utilizaremos a notação $p(n|*)$ quando estivermos falando do número de partições de n satisfazendo a condição $*$.

Exemplo 2.7 *Vamos utilizar a operação de conjugação para provar a seguinte identidade:*

$$p(n \mid \textit{partes são distintas}) = p(n \mid \textit{todo inteiro entre 1 e a maior parte aparece como parte}).$$

Quando fazemos a operação conjugação em uma partição de n qualquer que tenha todas as partes distintas, teremos sempre o 1 *como parte, já que a maior linha se tornará a maior coluna do diagrama de Ferrers da partição conjugada. Se a partição de n tiver apenas uma parte, não há mais o que se fazer, caso contrário, da mesma forma, a segunda linha da partição de n será a segunda coluna do diagrama de Ferrers da partição conjugada e a única com este tamanho, logo, nesta nova partição teremos ao menos uma parte* 2. *Pelo mesmo argumento anterior sempre teremos uma nova coluna menor que a anterior e consequentemente ao menos uma parte uma unidade maior do que a que tínhamos até então no diagrama de Ferrers da partição conjugada. Caso não tenhamos mais outra linha a conjugar da partição, a demonstração termina aqui. Caso contrário, repetiremos o mesmo processo. Feito o processo até que se termine de conjugar todas as linhas da partição de n teremos assim, uma nova partição em que todo inteiro entre 1 e a maior parte aparece como parte.*

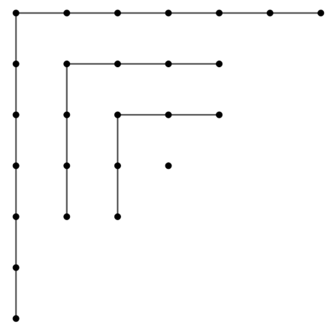
Como exemplo vejamos o gráfico de Ferrers das partições $7+5+3+1$ *e sua conjugada* $4+3+3+2+2+1+1$ *de* 16 *como forma de tornar mais clara a argumentação acima:*



Dizemos que uma partição é **autoconjugada** se ela for igual a sua partição conjugada. Por exemplo, é fácil ver que $3+2+1$ e $5+3+3+1+1$ são autoconjugadas, tal verificação pode ser feita facilmente através de seus respectivos gráficos de Ferrers.

Teorema 2.3 *Seja n um inteiro positivo. Então, o número de partições autoconjugadas de n é igual ao número de partições de n em partes ímpares distintas.*

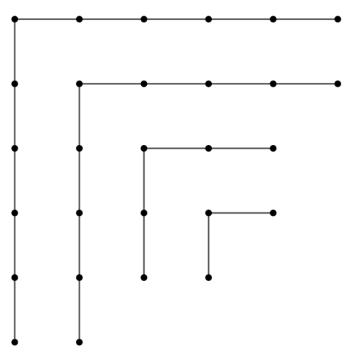
Para termos uma ideia da prova deste teorema e ilustrar tal transformação usaremos como exemplo a partição $7+5+5+4+3+1+1$ de 26. Vemos que, o número de pontos em cada uma das "linhas"em formato de L é ímpar e estes números são necessariamente distintos.



Neste caso, considerando cada parte pelo número de pontos sobre cada "linha"teremos a partição $13 + 7 + 5 + 1$ de 26.

Da mesma forma dando-nos uma partição contendo apenas números ímpares distintos, podemos colocá-los em formato L como mostrado acima e desta forma obtemos o gráfico de Ferrers de uma partição autoconjugada.

Como exemplo usaremos a partição $11 + 9 + 5 + 3$ de 28.



Note que, esta partição é claramente autoconjugada.

Corolário 2.2 *$p(n)$ é ímpar se, e somente se, o número de partições de n cujas partes são ímpares e distintas é ímpar.*

Demonstração: Pelo Teorema 2.3 o número de partições autoconjugadas de n é igual ao número de partições de n em partes ímpares e distintas, daí podemos mostrar então que

$$p(n)\text{é impar} \Leftrightarrow \text{número de partições de} \quad n \quad \text{autoconjugadas é ímpar.}$$

Note que,

$$p(n) = \text{partições autoconjugadas} + \text{partições que não são autoconjugadas} \tag{2.1}$$

Observe que o número de partições de n que não são autoconjugadas é par, já que, quando conjugamos uma dada partição A, teremos como resultado uma nova partição B que é diferente de A e se conjugarmos B resultaremos novamente em A, ou seja, cada partição que não é autoconjugada está associada a uma outra partição. A partir disso e de (2.1) temos que $p(n)$ é ímpar se, e somente se, o número de partições de n autoconjugadas é ímpar. ■

2.2 Um limite superior para *p(n)*

A busca por uma fórmula para a função $p(n)$ foi um fator relevante no desenvolvimento da pesquisa em teoria de partições, uma vez que quanto maior o valor de n, maior era o valor de $p(n)$, que não parecia ter nenhum controle ou padrão de crescimento. Neste trabalho, não temos como foco apresentar resultados relacionados a essa busca por fórmulas, porém achamos interessante falar sobre um limitante para a função. Veremos agora que a função $p(n)$ é limitada pelos números de Fibonacci, apresentados em 1.5.1. Primeiro mostraremos na proposição a seguir que $p(n)$ é uma função crescente.

Proposição 2.1 *Para todo inteiro positivo $n \geq 2$ temos*

$$p(n) > p(n-1).$$

Demonstração: De fato, observe que, de cada partição de $n-1$ obtém-se uma partição de n se adicionarmos uma linha com um único ponto ao seu gráfico de Ferrers. Note também que cada partição de n possuindo em seu diagrama uma linha formada por um único ponto torna-se uma partição de $n-1$ se retirarmos esta linha. Assim temos,

$$p(n) = p(n-1) + p(n \mid \text{não há parte igual a } 1) > p(n-1), \quad \forall n \geq 2 \tag{2.2}$$

e portanto, $p(n)$ é uma função crescente. ■

Observemos agora que

$$p(n-2) = p(n \mid \text{existe ao menos uma parte } 2). \tag{2.3}$$

De fato, acrescentando uma parte 2 em qualquer partição de $n-2$, obtemos partições de n com ao menos uma parte 2. E, inversamente, se removermos uma parte 2 das partições enumeradas por $p(n \mid \text{existe ao menos uma parte } 2)$ obtemos partições de $n-2$.

Proposição 2.2 *Para todo inteiro positivo $n \geq 2$ temos*

$$p(n \mid \textit{não há parte igual a } 1) \leq p(n \mid \textit{existe ao menos uma parte } 2).$$

Demonstração: Dada uma partição contada em $p(n \mid \text{não há parte igual a } 1)$, é claro que as partes dessa partição são maiores que 1. Podemos transformar cada partição com partes maiores que 1 em uma única partição com pelo menos uma parte 2, bastando dividir a menor parte λ (que é maior do que 1) em uma parte 2 e $\lambda - 2$ partes iguais a 1. E portanto, temos provado o resultado. ■

Combinando (2.2) e a Proposição 2.2 temos

$$p(n) \leq p(n-1) + p(n \mid \text{existe ao menos uma parte 2}), \quad \forall n \geq 2 \tag{2.4}$$

Daí, de (2.4) e (2.3) temos

$$p(n) \leq p(n-1) + p(n-2), \quad \forall n \geq 2 \tag{2.5}$$

Mostraremos agora que os números de Fibonacci controlam o crescimento de $p(n)$. Lembramos que os números de Fibonacci são definidos recursivamente da seguinte forma:

$$F_0 = 0,\ F_1 = 1 \quad \text{e} \quad F_{n+2} = F_{n+1} + F_n \quad \forall\, n \in \mathbb{N}.$$

Teorema 2.4 *Para todo inteiro positivo n, temos que $p(n) \leq F_{n+1}$, em que F_{n+1} é o $(n+1)$-ésimo número de Fibonacci.*

Demonstração: Vamos provar o teorema fazendo indução sobre n. Primeiro note que

$$p(0) = 1 = F_1 \quad \text{e} \quad p(1) = F_1 = F_2 = 1,$$

ou seja, o resultado é válido para $n = 1$. Suponha agora, por hipótese de indução, que o resultado seja verdadeiro para todo $k < n$, com $k \geq 2$. De (2.5) temos

$$p(n) \leq p(n-1) + p(n-2).$$

Aplicando a hipótese de indução e a definição dos números de Fibonacci temos

$$p(n) \leq p(n-1) + p(n-2) \leq F_n + F_{n-1} = F_{n+1}.$$

Portanto, o resultado é válido para todo inteiro $n > 0$. ■

2.3 Provas bijetivas

Basicamente se queremos verificar que o número de objetos de um tipo A é igual ao número de objetos de um tipo B não precisamos contar esses elementos. É suficiente fazer pares com um objeto de cada conjunto, mostrando que cada objeto do tipo A faz par com um objeto do tipo B e vice-versa. Essa construção é o que chamamos de bijeção entre os conjuntos A e B.

Na teoria de partições, afirmações como "o número de partições de n do tipo A é igual o número de partições de n do tipo B"são chamadas de **identidades em partições**. E uma **prova bijetiva** para uma identidade em partições consiste em se obter uma bijeção entre o conjunto de partições do tipo A e o conjunto de partições do tipo B. Já vimos alguns exemplos de provas deste tipo nos teoremas 2.1 e 2.2. Nesta seção veremos mais detalhadamente a importância e utilidade de tais provas.

Teorema 2.5 (Euler) *Para qualquer inteiro positivo n,*

$$p(n \mid \textit{partes são ímpares}) = p(n \mid \textit{partes são distintas}).$$

Demonstração: Operação 1 - De partes ímpares para partes distintas: dada uma partição de n em partes ímpares, se a partição não possuir partes iguais, não há o que fazer, caso contrário, se tal partição possuir ao menos duas partes iguais, somaremos duas a duas essas partes iguais e repetiremos esse procedimento até que todas as partes sejam distintas, ou até que sobre apenas uma parte.

Operação 2 - De partes distintas para partes ímpares: dada uma partição de n em partes distintas, caso todas as partes distintas sejam ímpares não temos nada a fazer, caso contrário, pegaremos cada parte par e a dividiremos por dois, originando duas novas partes iguais e repetiremos esse procedimento até que todas as partes restantes sejam ímpares.

Denotando por A e B os conjuntos formados pelas partições de n em partes ímpares e partes distintas, respectivamente, temos que $f : A \longrightarrow B$ definida por $f(\lambda) = \mu$, em que μ é a partição obtida a partir de $\lambda \in A$ pela operação 1, é uma bijeção, e devido a Operação 2, $f^{-1}(\mu) = \lambda$. Com isso temos a prova bijetiva do teorema. ■

Observação 2.2 *Quando usarmos no texto a expressão "somar"estaremos nos referindo a Operação 1 da demonstração do Teorema de Euler e quando utilizarmos a expressão "dividir"estaremos nos referindo a Operação 2 desta mesma demonstração.*

Exemplo 2.8 *Para um inteiro par $n > 2$, vamos encontrar uma prova bijetiva para as identidades abaixo:*

(i) $p(n \mid \textit{partes são pares}) = p\left(\frac{n}{2}\right)$.

(ii) $p(n \mid \textit{partes aparecem um número par de vezes}) = p\left(\frac{n}{2}\right)$.

Solução:

(i) Dada uma partição de n em que todas suas partes são pares, dividimos cada parte desta partição por 2 e assim teremos uma partição de $\frac{n}{2}$. Reciprocamente, dada uma partição de $\frac{n}{2}$ multiplicando cada parte desta partição por 2 teremos uma partição de n. Com isso temos uma prova bijetiva para a identidade.

(ii) Dada um partição de n em que as partes aparecem um número par de vezes, somamos cada par de partes iguais e posteriormente dividimos estes resultados por 2, logo teremos uma partição de $\frac{n}{2}$. Reciprocamente, dada uma partição de $\frac{n}{2}$ multiplicamos cada parte dessa partição de $\frac{n}{2}$ por 2 e posteriormente abrimos cada produto em uma soma de dois termos iguais, logo teremos uma partição de n tal que as partes aparecem um número par de vezes. Com isso temos uma prova bijetiva para a identidade.

Teorema 2.6 *Seja n um inteiro positivo. Então,*

$$p(n \mid \textit{partes} \in \{1\}) = p(n \mid \textit{partes são potências distintas de } 2)$$

Demonstração: É claro que $p(n \mid \text{partes} \in \{1\}) = 1$, já que existe apenas uma partição de n formada somente por partes iguais a 1. Usando a operação "somar" transformamos pares de números 1 em partes 2, na sequência os pares de 2 em partes 4 e assim sucessivamente, logo o conjunto de partições obtidas tem partes distintas e estas partes estão no conjunto formado pelas potências de 2, ou seja, o conjunto $\{1, 2, 4, ...\}$.

Reciprocamente, cada potência de 2, digamos 2^k, é dividida em um par de potências de 2, $2^{k-1} + 2^{k-1}$. Como a única potência de 2 que é ímpar é $2^0 = 1$, a operação "dividir" será executada em cada potência de 2 até restarem apenas partes iguais a 1. Com isso, temos que a igualdade do enunciado é de fato verdadeira. ■

Os conjuntos para os quais é possível obter uma bijeção através das operações "somar" e "dividir" são chamados de **pares de Euler**. Note que é fácil obtermos novos pares de Euler a partir de antigos, através da multiplicação de cada parte por um mesmo inteiro positivo. Como exemplo, multiplicando a identidade anterior por 3, obtemos a identidade:

$$p(n \mid \text{partes} \in \{3\}) = p(n \mid \text{partes distintas} \in \{3, 6, 12, 24, ...\})$$

Seja $N \subset \mathbb{N}$ um conjunto de partes. Através da operação "somar", pares de partes iguais são somados em cada passo do processo até que restem apenas partes distintas. Tal processo pode ser invertido, ou desfeito, de maneira única se dividirmos partes pares em duas novas partes iguais, através da operação "dividir", desde que saibamos quando parar de dividir, ou seja, quando as partes estiverem no conjunto N. Mas, como exemplo, na identidade acima, se $3 \in N$ e $6 \in N$ como saberíamos se o correto seria pararmos ao obter partes iguais a 6 ou partes iguais a 3, pois:

$$6 + 6 = 12 \quad \text{e} \quad 3 + 3 + 3 + 3 = 6 + 6 = 12.$$

Este problema ocorre, se e somente se, existirem em N dois elementos tais que um é uma potência de 2 vezes o outro. Assim, as operações "somar" e "dividir" provam o teorema a seguir.

Teorema 2.7
$$p(n \mid partes \in N) = p(n \mid partes\ distintas \in M),$$
em que N é o conjunto formado por inteiros positivos tais que nenhum de seus elementos é igual a uma potência de 2 vezes algum outro elemento, e M é o conjunto formado pelos elementos de N juntamente com produtos de elementos de N por potências de 2, ou seja, $M = N \cup \bigcup_{k\in\mathbb{N}} 2^k N$.

Teorema 2.8
$$p(n \mid a\ maior\ parte\ é \quad r) = p(n - r \mid cada\ parte\ é \leq r),$$
em que n e r são inteiros positivos, com $n \geq r$.

Demonstração: Dada uma partição $\lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_s$ de n, com $r = \lambda_1 \geq \ldots \geq \lambda_s$, ao removermos a maior parte, λ_1, ficaremos com uma partição $\lambda_2 + \lambda_3 + \ldots + \lambda_s$ de $n - r$ tal que cada parte é menor do que ou igual a r. Claramente este processo é invertível bastando acrescentar uma parte r a qualquer partição de $n - r$ com partes menores do que ou iguais a r. Com isso temos estabelecido uma prova bijetiva. ■

Vamos denotar por $A_k(n)$ o número de partições de n em partes ímpares, não necessariamente distintas, possuindo exatamente k partes diferentes.

Exemplo 2.9 $A_3(14) = 7$, *pois as partições contadas por* $A_3(14)$ *são*

$$\begin{aligned}
&9+3+1+1\\
&7+5+1+1\\
&7+3+3+1\\
&7+3+1+1+1+1\\
&5+5+3+1\\
&5+3+3+1+1+1\\
&5+3+1+1+1+1+1+1.
\end{aligned}$$

Vamos denotar por $B_k(n)$ o número de partições de n nas quais cada partição é formada por k sequências de um ou mais inteiros consecutivos, tais que essas sequências não podem ser consecutivas.

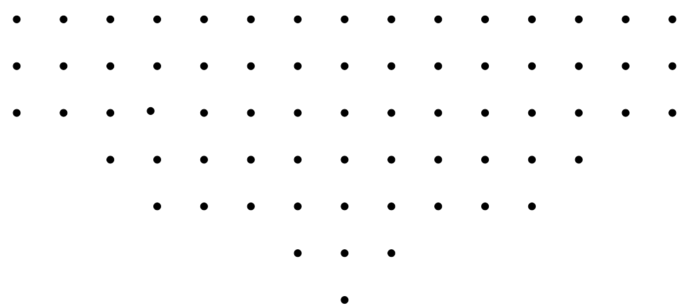
Exemplo 2.10 $B_3(14) = 7$, *pois as partições contadas por* $B_3(14)$ *são*

$$10+3+1, 9+4+1, 8+4+2, 8+5+1, 7+5+2, 7+4+2+1 \quad e \quad 6+4+3+1.$$

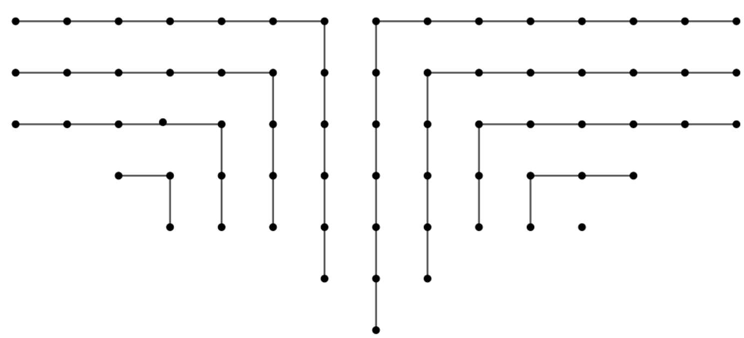
Observe, por exemplo, que a partição $8+3+2+1$ apesar de ser formada por 3 sequências de inteiros, não é contada em $B_3(14)$, pois as segunda e terceira sequências são consecutivas.

Teorema 2.9 (Sylvester) *$A_k(n) = B_k(n)$, para quaisquer inteiros positivos k e n.*

Para este teorema, iremos apenas ilustrar a demonstração através de um exemplo. Para obtermos uma bijeção iremos fazer uma variação no gráfico de Ferrers das partições em partes ímpares. Na representação gráfica de uma partição as linhas são alinhadas a esquerda, o que iremos fazer agora será alinhá-las ao centro. Como exemplo podemos representar a partição $15 + 15 + 15 + 11 + 9 + 3 + 1$, uma das partições contadas em $A_5(69)$ por:



Agora, neste novo diagrama, conectamos os pontos em L da seguinte maneira:



Cada parte da nova partição será obtida contando o numero de pontos sobre cada linha em L, o que resulta na partição $14+12+11+9+8+7+4+3+1$. Observe que esta nova partição possui partes distintas e exatamente cinco sequências separadas: $14, 12+11, 9+8+7, 4+3$ e 1, isto é, trata-se de uma partição contada em $B_5(69)$.

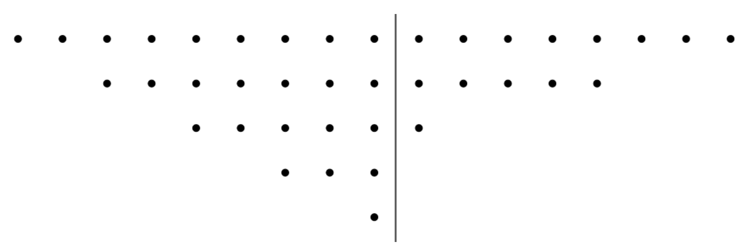
Teorema 2.10 *Dados a, b, c inteiros positivos com $a > b > 1$ e $a > c > 1$ então*

$$p(a-c|b-1 \quad \textit{partes, cada parte} \quad \leq c) = p(a-b|c-1 \quad \textit{partes, cada parte} \quad \leq b)$$

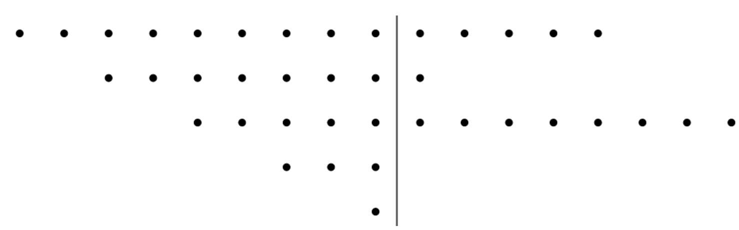
Demonstração: Considere o gráfico de Ferrers de uma partição enumerada pelo lado esquerdo da igualdade. Vamos transformar essa partição da seguinte maneira: primeiro acrescentaremos uma nova parte igual a c, obtendo uma partição de a com b partes, todas menores do que ou iguais a c. Em seguida, subtrairemos 1 de cada parte da nova partição e obteremos uma partição de $a - b$, com no máximo b partes e todas menores que c, sendo que a maior parte é $c-1$. Por último conjugaremos a mesma e obteremos uma partição de $a-b$ em $c-1$ partes e cada parte é no máximo b. Não é difícil se convencer de que esta composição de transformações fornece uma bijeção que prova a identidade do enunciado. ■

Teorema 2.11 *O número de partições de um inteiro positivo n cuja diferença entre quaisquer duas partes é ≥ 2 é igual ao número de partições de n em partes distintas, onde cada parte par é maior que duas vezes o número de partes ímpares.*

Vamos descrever brevemente o processo para demonstrar este teorema através de um exemplo. Considere o gráfico de Ferrers de uma partição contada por $p(n \mid \text{diferença entre quaisquer duas partes é} \geq 2)$. Ajustaremos as linhas deste gráfico da seguinte maneira: deslocaremos a segunda linha para a direita de forma que o primeiro ponto desta linha fique na mesma direção do terceiro ponto da primeira linha e faremos este mesmo processo sucessivamente para todas as outras linhas de forma que o primeiro ponto de cada linha coincida sempre com o terceiro ponto da linha anterior. Traçaremos agora um linha vertical neste diagrama de forma que fique apenas um ponto na última linha à esquerda desta linha vertical. Por exemplo, para $17+12+6+3+1$, o diagrama modificado é:



À direita da linha vertical no diagrama acima temos um gráfico de Ferrers de uma partição e agora vamos reordenar suas linhas colocando as partes ímpares em ordem não-crescente e, depois, as partes pares em ordem não-crescente:



Agora, ignorando a linha vertical no meio do diagrama e considerando cada linha como uma parte da nova partição, temos que $14+8+13+3+1$ será esta nova partição em partes distintas e tal que cada parte par é maior do que duas vezes o número de partes ímpares. Este procedimento fornece uma prova bijetiva para o teorema.

Relação de recorrência para $q_k(n)$

Relembremos do Teorema 2.1 que $q_k(n)$ é o número de partições de n tendo exatamente k partes se $0 < k \leq n$. Vamos agora obter, por meio de bijeções, a relação de recorrência

$$q_k(n) = q_{k-1}(n-1) + q_k(n-k),$$

onde estamos assumindo

$$q_k(n) = \begin{cases} 0, & \text{se} \quad k = 0 \quad \text{e} \quad n > 0 \quad \text{ou} \quad k > n \quad \text{ou} \quad k < 0, \\ 1, & \text{se} \quad k = 0 = n. \end{cases}$$

Seja $Q_j(i)$ o conjunto formado pelas partições de i com exatamente j partes. Então, o número de elementos de $Q_j(i)$ é $|Q_j(i)| = q_j(i)$. Temos que o conjunto $Q_k(n)$ é a união disjunta dos seguintes conjuntos

$$S = \{(\lambda_1, \ldots, \lambda_k) \in Q_k(n) | \lambda_k = 1\},$$

$$T = \{(\lambda_1, \ldots, \lambda_k) \in Q_k(n) | \lambda_k > 1\}.$$

A função $f : S \longrightarrow Q_{k-1}(n-1)$, dada por

$$f((\lambda_1, \ldots, \lambda_k)) = (\lambda_1, \ldots, \lambda_{k-1}),$$

é uma bijeção cuja inversa satisfaz $f^{-1}((\mu_1, \ldots, \mu_{k-1})) = (\mu_1, \ldots, \mu_{k-1}, 1)$. Logo, $|S| = |Q_{k-1}(n-1)| = q_{k-1}(n-1)$. Por outro lado, a função $g : T \longrightarrow Q_k(n-k)$, dada por

$$g((\lambda_1, \ldots, \lambda_k)) = (\lambda_1 - 1, \ldots, \lambda_k - 1),$$

é uma bijeção cuja inversa satisfaz $g^{-1}((\mu_1, \ldots, \mu_k)) = (\mu_1 + 1, \ldots, \mu_k + 1)$. Logo, $|T| = |Q_k(n-k)| = q_k(n-k)$. Portanto,

$$q_k(n) = |Q_k(n)| = |S| + |T| = q_{k-1}(n-1) + q_k(n-k).$$

2.3.1 Algumas identidades

Vimos que identidades em partições é algo amplamente estudado e com diversos resultados. E de fato, esse é um tópico que motiva diversos pesquisadores na teoria. No início do século XX, Ramanujan apresentou suas identidades, que até hoje impulsionam diversas pesquisas na área. Essas identidades intrigaram bastante o mundo matemático, pois eram resultados relacionados aos primos 5, 7 e 11, mas que porém não possuíam resultados análogos para outros primos. Veremos a seguir, ainda que superficialmente, alguns exemplos de identidades famosas dentro da teoria.

Muitas das identidades que vimos até agora tem a forma

$$p(n \mid [\text{alguma condição}]) = p(n \mid \text{partes em N}), \forall n > 0. \tag{2.6}$$

É o caso, por exemplo, de

$$p(n \mid \text{partes distintas em M}) = p(n \mid \text{partes em N}),$$

em que (M, N) é um par de Euler. Ou ainda,

$$p(n \mid \text{no máximo} \quad k \quad \text{partes}) = p(n \mid \text{partes} \leq k).$$

Dizemos que uma partição tem partes ***d*-distintas** se a diferença entre estas partes é de pelo menos d. Veja por exemplo na Tabela 2.1 as partições em partes 2-distintas dos 11 primeiros inteiros positivos.

n	Quantidade	Partições em partes 2-distintas
1	1	1
2	1	2
3	1	3
4	2	4, 3+1
5	2	5, 4+1
6	3	6, 5+1, 4+2
7	3	7, 6+1, 5+2
8	4	8, 7+1, 6+2, 5+3
9	5	9, 8+1, 7+2, 6+3, 5+3+1
10	6	10, 9+1, 8+2, 7+3, 6+4, 6+3+1
11	7	11, 10+1, 9+2, 8+3, 7+4, 7+3+1, 6+4+1

Tabela 2.1: Partições em partes 2-distintas

Com base na tabela acima iremos construir um conjunto N tal que

$$p(n \mid \text{partes em} \quad N) = p(n \mid \text{partes} \quad \text{2-distintas}),$$

ou seja, queremos encontrar uma identidade de partição da forma (2.6) envolvendo partições em partes 2-distintas. Começamos com $N = \emptyset$ e então:

- Deve existir uma partição de 1. Com partes em $N = \emptyset$ não teremos uma partição de 1, logo devemos ter $1 \in N$.

- Deve existir uma partição de 2. Como temos uma partição de 2 com partes em $N = \{1\}, 1 + 1$, segue que $2 \notin N$.

- Deve existir uma partição de 3. Como temos uma partição de 3 com partes em $N = \{1\}, 1+1+1$, segue que $3 \notin N$.

- Devem existir duas partições de 4. Com partes em $N = \{1\}$ temos apenas uma partição de $4, 1+1+1+1$, logo devemos ter $4 \in N$.

- Devem existir duas partições de 5. Com partes em $N = \{1, 4\}$, temos duas partições de $5 : 4+1, 1+1+1+1+1$, logo $5 \notin N$.

- Devem existir três partições de 6. Com partes em $N = \{1, 4\}$ temos duas partições de $6 : 4+1+1, 1+1+1+1+1+1$, logo devemos ter $6 \in N$.

- Devem existir três partições de 7. Com partes em $N = \{1, 4, 6\}$ temos três partições de $7 : 6+1, 4+1+1+1, 1+1+1+1+1+1+1$, logo $7 \notin N$.

- Devem existir quarto partições de 8. Com partes em $N = \{1, 4, 6\}$ temos quatro partições de $8 : 6+1+1, 4+4, 4+1+1+1+1, 1+1+1+1+1+1+1+1$, logo $8 \notin N$.

- Devem existir cinco partições de 9. Com partes em $N = \{1, 4, 6\}$ temos 4 partições de $9 : 6+1+1+1, 4+4+1, 4+1+1+1+1+1, 1+1+1+1+1+1+1+1+1$, logo $9 \in N$.

- Devem existir seis partições de 10. Com partes em $N = \{1, 4, 6, 9\}$ temos 6 partições de $10 : 9+1, 6+4, 4+4+1+1, 4+1+1+1+1+1+1, 6+1+1+1+1, 1+1+1+1+1+1+1+1+1+1$, logo $10 \notin N$.

- Devem existir sete partições de 11. Com partes em $N = \{1, 4, 6, 9\}$ temos partições de $11 : 9+1+1, 6+4+1, 4+4+1+1+1, 6+1+1+1+1+1, 4+1+1+1+1+1+1+1, 1+1+1+1+1+1+1+1+1+1+1$, logo $11 \in N$.

Até aqui obtivemos $N = \{1, 4, 6, 9, 11\}$. Prosseguindo com a argumentação acima, pode-se verificar que $N = \{1, 4, 6, 9, 11, 14, 16, 19, 21, 24, \ldots\}$. Observe que os elementos em N são inteiros que deixam resto 1 ou 4 quando divididos por 5, ou seja, pela Definição 1.2, os elementos de N são todos os inteiros congruentes a 1 ou 4 módulo 5. Com base na investigação que fizemos acima, podemos conjecturar a seguinte identidade

$$p(n \mid \text{partes} \equiv 1 \quad \text{ou} \quad 4 \mod 5) = p(n \mid \text{partes são} \quad \text{2-distintas}),$$

chamada de **primeira identidade de Rogers-Ramanujan**. Note que não provamos esta identidade, apenas temos evidências, com base em alguns poucos exemplos, de que ela possa ser verdadeira. Para tal identidade cabe-se uma demonstração analítica.

O mesmo método citado anteriormente pode ser empregado para descobrir a **segunda identidade de Rogers-Ramanujan**:

$$p(n \mid \text{partes} \equiv 2 \quad \text{ou} \quad 3 \quad \text{mod} \quad 5) = p(n \mid \text{partes são} \quad \text{2-distintas e } > 1).$$

Investigaremos brevemente a segunda identidade de Rogers-Ramanujan. Para começar, construimos uma tabela com todas as partições com partes 2-distintas e > 1 para $n = 1, 2, ...12$.

n	Quantidade	Partições em partes 2-distintas e > 1
1	0	
2	1	2
3	1	3
4	1	4
5	1	5
6	2	6, 4+2
7	2	7, 5+2
8	3	8, 6+2, 5+3
9	3	9, 7+2, 6+3
10	4	10, 8+2, 7+3, 6+4
11	4	11, 9+2, 8+3, 7+4
12	6	12, 10+2, 9+3, 8+4, 7+5, 6+4+2

Tabela 2.2: Partições em partes 2-distintas e > 1

Utilizando os dados da Tabela 2.2, vamos procurar um conjunto M tal que as partes das partições de n pertençam a M e satisfaçam a seguinte identidade:

$$p(n|\text{partes sejam 2-distintas e} > 1) = p(n|\text{partes em} \quad M).$$

Inicialmente consideramos o conjunto $\emptyset$ e vamos construindo o conjunto M:

- Para $n = 1$, não há partição em partes 2-distintas e > 1. Assim, $p(1 \mid \text{partes em } M)$ deve ser zero. Portanto, o número 1 não pertence a M.

- Para $n = 2$, há uma partição em partes 2-distintas e > 1. Assim, $p(2 \mid \text{partes em } M)$ deve ser um. Portanto, o número 2 pertence a M. Agora $M \supseteq \{2\}$.

- Para $n = 3$, há uma partição em partes 2-distintas e > 1. Assim, $p(3 \mid \text{partes em } M)$ deve ser um. Portanto, o número 3 pertence a M. Agora $M \supseteq \{2, 3\}$.

- Para $n = 4$, há uma partição em partes 2-distintas e > 1. Assim, $p(4 \mid \text{partes em } M)$ deve ser um. Como $M \supseteq \{2, 3\}$, temos a partição $2 + 2$. Portanto, o número 4 não pertence a M.

- Para $n = 5$, há uma partição em partes 2-distintas e > 1. Assim, $p(5 \mid \text{partes em } M)$ deve ser um. Como $M \supseteq \{2, 3\}$, temos a partição $2 + 3$. Portanto, o número 5 não pertence a M.

- Para $n = 6$, há duas partições em partes 2-distintas e > 1. Assim, $p(6 \mid \text{partes em } M)$ deve ser dois. Como $M \supseteq \{2, 3\}$, temos as partições $3 + 3$ e $2 + 2 + 2$. Portanto, o número 6 não pertence a M.

- Para $n = 7$, há duas partições em partes 2-distintas e > 1. Assim, $p(7 \mid \text{partes em } M)$ deve ser dois. Como $M \supseteq \{2, 3\}$, temos a partição $3+2+2$. Logo, precisamos de mais uma partição. Portanto, o número 7 pertence a M. Agora $M \supseteq \{2, 3, 7\}$.

- Para $n = 8$, há três partições em partes 2-distintas e > 1. Assim, $p(8 \mid \text{partes em } M)$ deve ser três. Como $M \supseteq \{2, 3, 7\}$, temos as partições $3 + 3 + 2$ e $2 + 2 + 2 + 2$. Logo, precisamos de mais uma partição. Portanto, o número 8 pertence a M. Agora $M \supseteq \{2, 3, 7, 8\}$.

- Para $n = 9$, há três partições em partes 2-distintas e > 1. Assim, $p(9 \mid \text{partes em } M)$ deve ser três. Como $M \supseteq \{2, 3, 7, 8\}$, temos as partições $7+2, 3+3+3$ e $3+2+2+2$. Portanto, o número 9 não pertence a M.

- Para $n = 10$, há quatro partições em partes 2-distintas e > 1. Assim, $p(10 \mid \text{partes em } M)$ deve ser quatro. Como $M \supseteq \{2, 3, 7, 8\}$ temos as partições $8+2, 7+3, 3+3+2+2$ e $2 + 2 + 2 + 2 + 2$. Portanto, o número 10 não pertence a M.

- Para $n = 11$, há quatro partições em partes 2-distintas e > 1. Assim, $p(11 \mid \text{partes em } M)$ deve ser quatro. Como $M \supseteq \{2, 3, 7, 8\}$, temos as partições $8+3, 7+2+2, 3+3+3+2$ e $3 + 2 + 2 + 2 + 2$. Portanto, o número 11 não pertence a M.

- Para $n = 12$, há seis partições em partes 2-distintas e > 1. Assim, $p(12 \mid \text{partes em } M)$ deve ser seis. Como $M \supseteq \{2, 3, 7, 8\}$, temos as partições $8 + 2 + 2, 7 + 3 + 2, 3 + 3 + 3 + 3, 3 + 3 + 2 + 2 + 2$ e $2 + 2 + 2 + 2 + 2 + 2$. Logo, precisamos de mais uma partição. Portanto, o número 12 pertence a M. Agora $M \supseteq \{2, 3, 7, 8, 12\}$.

Assim, $M \supseteq \{2, 3, 7, 8, 12\}$ e se continuarmos com o mesmo argumento, podemos verificar que M contém $\{13, 17, 18, 22, 23, 27, 28, \ldots\}$. Note que obtemos os dois próximos números do conjunto M adicionando 5 nos dois últimos números da sequência. Este conjunto de números pode ser descrito como o conjunto dos inteiros positivos que, quando divididos por 5, deixam restos iguais a 2 ou 3. Portanto,

$$p(n \mid \text{partes} \equiv 2 \quad \text{ou} \quad 3 \mod 5) = p(n \mid \text{partes são} \quad \text{2-distintas e } > 1).$$

O argumento acima não prova a identidade para todo n, apenas verifica que é verdadeira para alguns valores de n e encaminha a construção de M. É importante mencionar também que até hoje não se obteve uma prova bijetiva simples e direta para as identidades de Rogers-Ramanujan.

Utilizaremos o método utilizado para redescobrir as identidades de Rogers-Ramanujan, para descobrir uma outra identidade conhecida na teoria das partições, a **identidade de Schur**. Trata-se de uma identidade sobre partições em partes 3-distintas e não possuindo partes consecutivas divisíveis por 3. Primeiro faremos uma tabela na qual listaremos todas as partições, para $n = 1, 2, 3, \ldots, 13$, com partes 3-distintas e não possuindo partes consecutivas divisíveis por 3:

n	Quantidade	Partições em partes 3-distintas e não possuindo partes consecutivas divisíveis por 3
1	1	1
2	1	2
3	1	3
4	1	4
5	2	5, 4+1
6	2	6, 5+1
7	3	7, 6+1, 5+2
8	3	8, 7+1, 6+2
9	3	9, 8+1, 7+2
10	4	10, 9+1, 8+2, 7+3
11	5	11, 10+1, 9+2, 8+3, 7+4
12	6	12, 11+1, 10+2, 9+3, 8+4, 7+4+1
13	7	13, 12+1, 11+2, 10+3, 9+4, 8+5, 8+4+1

Tabela 2.3: Partições em partes 3-distintas e não possuindo partes consecutivas divisíveis por 3

Agora, com base na tabela acima, vamos construir um conjunto S tal que $p(n \mid \text{partes em } S) = p(n \mid \text{partes 3-distintas e não possui partes consecutivas divisíveis por 3})$. Começaremos com $N = \emptyset$ e então:

- Deve existir uma partição de 1. Com partes em $S = \emptyset$ não teremos uma partição de 1, logo, devemos ter $1 \in S$.

- Deve existir uma partição de 2. Como temos uma partição de 2 em $S = \{1\}, 1 + 1$, segue que $2 \notin S$.

- Deve existir uma partição de 3. Como temos uma partição de 3 em $S = \{1\}, 1 + 1 + 1$, segue que $3 \notin S$.

- Deve existir uma partição de 4. Como temos uma partição de 4 em $S = \{1\}, 1{+}1{+}1{+}1$, segue que $4 \notin S$.

- Devem existir duas partições de 5. Com partes em $S = \{1\}$, temos apenas uma partição de $5 : 1+1+1+1+1$. Assim devemos ter $5 \in S$.

- Devem existir duas partições de 6. Como temos duas partição de 6 em $S = \{1,5\}$, $1+1+1+1+1+1$ e $5+1$, segue que $6 \notin S$.

- Devem existir três partições de 7. Com partes em $S = \{1,5\}$, temos apenas duas partições de $7 : 1+1+1+1+1+1+1$ e $5+1+1$. Assim devemos ter $7 \in S$.

- Devem existir três partições de 8. Como temos três partições de 8 em $S = \{1,5,7\}$, $1+1+1+1+1+1+1+1, 7+1$ e $5+1+1+1$, segue que $8 \notin S$.

- Devem existir três partições de 9. Como temos três partições de 9 em $S = \{1,5,7\}$, $1+1+1+1+1+1+1+1+1, 7+1+1$ e $5+1+1+1+1$, segue que $9 \notin S$.

- Devem existir quatro partições de 10. Como temos quatro partições de 10 em $S = \{1,5,7\}$, $1+1+1+1+1+1+1+1+1+1, 7+1+1+1, 5+5$ e $5+1+1+1+1+1$ segue que $10 \notin S$.

- Devem existir cinco partições de 11. Com partes em $S = \{1,5,7\}$, temos apenas quatro partições de $11 : 1+1+1+1+1+1+1+1+1+1+1, 7+1+1+1+1, 5+5+1$ e $5+1+1+1+1+1+1$. Assim devemos ter $11 \in S$.

- Devem existir seis partições de 12. Com partes em $S = \{1,5,7,11\}$, temos seis partições de $12 : 1+1+1+1+1+1+1+1+1+1+1+1, 7+1+1+1+1+1, 5+5+1+1$, $5+1+1+1+1+1+1+1$, $11+1$ e $7+5$. Assim devemos ter $12 \notin S$.

- Devem existir sete partições de 13. Com partes em $S = \{1,5,7,11\}$, temos apenas quatro partições de $13 : 1+1+1+1+1+1+1+1+1+1+1+1+1, 7+1+1+1+1+1+1, 5+5+1+1+1$, $5+1+1+1+1+1+1+1+1$, $11+1+1$ e $7+5+1$. Assim devemos ter $13 \in S$.

Até aqui obtivemos $S = \{1,5,7,11,13\}$. Prosseguindo com a argumentação acima, pode-se verificar que $S = \{1,5,7,11,13,17,19,23,25,29,\ldots\}$. Observe que os inteiros em S são congruentes a ± 1 mod 6 e com isso podemos conjecturar que:

$$p(n \mid \text{partes} \equiv \pm 1 \bmod 6) = p(n \mid \text{partes 3-distintas e sem partes múltiplas consecutivas de } 3),$$

que é conhecida como a identidade de Schur.

2.4 Funções geradoras

As funções geradoras estão entre as principais ferramentas utilizadas na solução de problemas de contagem. Essa técnica teve origem em trabalhos de A. De Moivre (1667 - 1754) e quem começou a empregá-la na teoria aditiva dos números foi Euler. Veremos nessa seção como utilizar as funções geradoras no estudo das partições.

Uma **série de potências** é uma soma infinita da forma $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$, em que a_i, para $i = 1, 2, 3, \ldots$, são números reais e x é uma variável. Dada uma sequência $(a_r)_{r\in\mathbb{N}}$, a **função geradora ordinária** para esta sequência é definida como a série de potências

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots .$$

Exemplo 2.11 *Pela definição de função geradora ordinária acima, vemos que a função dada por*

$$f(x) = 1 + x + x^2 + x^3 + x^4 + \ldots,$$

é a função geradora para a sequência $a_r = 1$, para $r = 0, 1, 2, 3, \ldots$.

Sabemos que, para $|x| < 1$,

$$f(x) = \frac{1}{1-x}.$$

Quando consideramos expressões como $f(x) = 1+x+x^2+x^3+x^4+\ldots$, sabemos do cálculo que estamos interessados na função definida por esta expressão e, portanto, nos importa o problema de sua convergência, isto é, quando $f(x)$ é finito. Desta forma não nos interessará os valores de x com $|x| \geq 1$. No nosso contexto de funções geradoras estamos interessados nos coeficientes e raramente iremos atribuir valores para x, sendo assim vamos manipular essas séries sem nos preocuparmos com convergência. Implicitamente, estaremos sempre considerando $|x| < 1$.

Teorema 2.12 *Sendo $f(x)$ e $g(x)$ as funções geradoras das sequências $(a_r)_{r\in\mathbb{N}}$ e $(b_r)_{r\in\mathbb{N}}$, respectivamente, temos:*

(i) $Af(x) + Bg(x)$ *é uma função geradora para a sequência* $(Aa_r + Bb_r)_{r\in\mathbb{N}}$*;*

(ii) $f(x)g(x) = \displaystyle\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(a_k b_{n-k})\right)x^n$*;*

(iii) A função geradora para $(a_0 + a_1 + \cdots + a_r)_{r\in\mathbb{N}}$ *é igual a* $(1 + x + x^2 + \cdots)f(x)$*;*

(iv) A função geradora para $(ra_r)_{r\in\mathbb{N}}$ *é igual a* $xf'(x)$*, em que* $f'(x)$ *é a derivada de* f *com respeito a* x*;*

(v) $\displaystyle\int f(x)dx = \sum_{n=0}^{\infty}\frac{a_n}{n+1}x^{n+1}.$

Exemplo 2.12 *Vamos encontrar a função geradora ordinária para a sequência $a_r = r$.*

Pelo Exemplo 2.11, a função geradora para a sequência $(1, 1, 1, 1, \ldots)$ é

$$f(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^r + \cdots .$$

Usando o item iv) do teorema acima, a função geradora ordinária procurada é $xf'(x)$. E como

$$f'(x) = \frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \cdots + rx^{r-1} + \cdots ,$$

logo

$$xf'(x) = \frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + 4x^4 + \cdots + rx^r + \cdots .$$

Teorema 2.13 *Para $|x| < 1$ temos:*

$$(1+x)^u = 1 + ux + \frac{u(u-1)}{2}x^2 + \frac{u(u-1)\cdots(u-r+1)}{r!}x^r + \cdots .$$

Denotando por

$$\binom{u}{r} = \begin{cases} \dfrac{u(u-1)\cdots(u-r+1)}{r!}, & se \quad r > 0, \\ 1, & se \quad r = 0, \end{cases}$$

temos

$$(1+x)^u = \sum_{r=0}^{\infty} \binom{u}{r} x^r.$$

O número $\binom{u}{r}$, definido acima, é chamado de **coeficiente binomial generalizado**.

Teorema 2.14 *O coeficiente de x^p na expansão de*

$$(1 + x + x^2 + x^3 + \cdots)^n$$

é igual a $\binom{n+p-1}{p}$.

Exemplo 2.13 *Sendo $(1+x)^{\frac{1}{4}}$ a função geradora ordinária para a sequência $(a_r)_{r\in\mathbb{N}}$, vamos encontrar a_2.*

Solução: *Basta tomarmos o coeficiente de x^2 na expansão de $(1+x)^{\frac{1}{4}}$:*

$$(1+x)^{\frac{1}{4}} = \sum_{r=0}^{\infty} \binom{\frac{1}{4}}{r} x^r = 1 + \frac{1}{4}x + \frac{\frac{1}{4}\left(\frac{1}{4}-1\right)}{2!}x^2 + \cdots .$$

Logo,

$$a_2 = \frac{\frac{1}{4}\left(\frac{1}{4}-1\right)}{2} = -\frac{3}{32}.$$

Definição 2.3 *A série de potências*

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = a_0 + a_1\frac{x}{1!} + a_2\frac{x^2}{2!} + a_3\frac{x^3}{3!} + a_4\frac{x^4}{4!} + \cdots$$

é a ***função geradora exponencial*** *para a sequência* $(a_r)_{r\in\mathbb{N}}$.

Observação 2.3 *Utilizamos a função geradora exponencial quando a ordem dos objetos retirados deve ser considerada. Caso contrário, utilizamos, como vimos anteriormente, a função geradora ordinária.*

Exemplo 2.14 *Vamos determinar a função geradora exponencial para se encontrar o número de sequências de k letras ($k \leq 6$) formadas pelas letras a, b, c, em que a letra a ocorre no máximo uma vez, a letra b no máximo duas vezes e a letra c no máximo três vezes.*

Para tal, devemos considerar o produto dos três polinômios abaixo em que cada um "controla" a presença das letras a, b, c, respectivamente:

$$(1+x)\left(1+x+\frac{x^2}{2!}\right)\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}\right) = 1+3x+4x^2+\frac{19}{6}x^3+\frac{10}{3}x^4+\frac{1}{2}x^5+\frac{1}{6}x^6.$$

Como estamos interessados na sequência dos coeficientes de $\frac{x^r}{r!}$, devemos reescrever este polinômio na forma

$$1+3\frac{x}{1!}+8\frac{x^2}{2!}+19\frac{x^3}{3!}+80\frac{x^4}{4!}+60\frac{x^5}{5!}+120\frac{x^6}{6!}.$$

2.4.1 Exemplos

Vamos utilizar a breve introdução sobre funções geradoras vista acima para determinar tais funções associadas a algumas partições e a partir daí compreender como esse tópico se insere na teoria de partições dos inteiros. Conheceremos, a seguir, uma série de exemplos de funções geradoras para contar alguns exemplos de partições restritas, isto é, aquelas em que as partes possuem alguma propriedade especial, e partições irrestritas.

Função geradora para as partições de n em partes ímpares e distintas

Tomando o produto $(1+x)(1+x^3)(1+x^5)(1+x^7)\cdots(1+x^{2k+1})\cdots$, podemos ver que o coeficiente de x^6 é igual a 1, que é o total de maneiras de se escrever 6 como soma de ímpares distintos. É fácil ver que a potência x^6 aparece como o produto de $x^5 \cdot x^1$. Note também que 11 só pode ser escrito como soma de ímpares distintos através do próprio número 11 e da soma $7+3+1$, por isso o coeficiente de x^{11} no produto acima é 2. Já o coeficiente de x^{14} é 3, pois obteremos x^{14} apenas quando se multiplica $x \cdot x^{13}$, $x^3 \cdot x^{11}$ e $x^5 \cdot x^9$. Desta forma vemos que

$$\prod_{k=0}^{\infty}(1+x^{2k+1}) = \sum_{n=1}^{\infty} d_i(n)x^n,$$

em que $d_i(n)$ é o número de partições de n em partes ímpares distintas, ou seja,

$$\prod_{k=0}^{\infty}(1+x^{2k+1})$$

é a função geradora para $d_i(n)$.

Função geradora para partições de n em partes distintas

Tome o produto

$$(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots(1+x^n)\cdots.$$

Tome agora como exemplo um número inteiro positivo que seja menor ou igual a 5. É claro que nenhuma parte deste número pode ser maior ou igual a 5 e se tomarmos então o produto $(1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)$ e considerarmos apenas as potências de $x \leq 5$ temos a função geradora para as partições de todos os números menores do que ou iguais a 5 em partes distintas. Como o produto acima é igual a $1+x+x^2+2x^3+2x^4+3x^5+\cdots$ podemos observar, por exemplo, que, como 3 é o coeficiente da potência x^5, existem 3 partições de 5 em partes distintas, que são: $5, 4+1, 3+2$. É fácil ver que os termos do tipo $(1+x^{n+1}), (1+x^{n+2}), \cdots$ não contribuem para as partições de n, com isso, para se encontrar o total de partições de n em partes distintas, basta considerarmos o produto finito $(1+x)(1+x^2)(1+x^3)\cdots(1+x^n)$. Pela argumentação acima, podemos concluir que a função geradora para as partições de n em partes distintas é dada pelo produto infinito

$$\prod_{k=1}^{\infty}(1+x^k). \tag{2.7}$$

Função geradora para partições de n em partes pares e distintas

Se estivermos interessados na função geradora das partições de n em partes pares e distintas devemos tomar o produto $(1+x^2)(1+x^4)(1+x^6)(1+x^8)(1+x^{10})\cdots(1+x^{2k})\cdots$. Como na partição de um número menor do que ou igual a oito nunca teremos partes maiores do que 8, se tomarmos o produto

$$(1+x^2)(1+x^4)(1+x^6)(1+x^8)$$

e considerarmos apenas as potências de $x \leq 8$ teremos a função geradora para a partição de todos os números menores do que ou iguais a 8 em partes pares e distintas. É fácil ver que o produto acima é igual a

$$1 + x^2 + x^4 + 2x^6 + 2x^8 + \cdots$$

e como exemplo podemos observar que o coeficiente de x^6 é 2 que representa a quantidade de partições de 6 em partes pares e distintas que são: 6 e $4 + 2$.

A partir desta argumentação e da função geradora (2.7) é fácil ver que a função geradora para partições de n em partes pares e distintas é

$$\prod_{k=1}^{\infty}(1 + x^{2k}).$$

Função geradora para partições de n em partes que são quadrados distintos

Se estivermos interessados na função geradora das partições de n em quadrados distintos devemos tomar o produto

$$(1 + x)(1 + x^4)(1 + x^8)(1 + x^{16})\ldots = 1 + x + x^4 + x^5 + x^9 + x^{10} + x^{13} + x^{14} + x^{16} + \ldots.$$

Desta forma por exemplo, podemos ver que entre os números de 1 a 16, somente oito possuem partições cujas partes são quadrados perfeitos.

A partir da mesma argumentação para a função geradora (2.7) e no que foi dito acima, vemos que, a função geradora para partições de n em partes que são quadrados distintos é

$$\prod_{k=1}^{\infty}(1 + x^{k^2}).$$

Função geradora para $p(n)$

Note que

$$\begin{aligned}
\frac{1}{1-x} &= 1 + x + x^2 + x^3 + x^4 + \cdots \\
\frac{1}{1-x^2} &= 1 + x^2 + x^4 + x^6 + x^8 + \cdots \\
&\vdots \\
\frac{1}{1-x^m} &= 1 + x^m + x^{2m} + x^{3m} + x^{4m} + \cdots,
\end{aligned}$$

daí,

$$\prod_{k=1}^{\infty}\frac{1}{1-x^k} = (1+x+x^2+x^3+x^4+\cdots)(1+x^2+x^4+x^6+x^8+\cdots)(1+x^3+x^6+x^9+x^{12}+\cdots)\cdots,$$

e com isso concluimos que as contribuições para os coeficientes de x^n vêm de um termo x^{a_1} da primeira série, de x^{2a_2} da segunda série, de x^{3a_3} da terceira, ..., de x^{ma_m} da m-ésima série, em que $a_i \geq 0$, para todo i. Como o produto destes termos resulta em x^n, temos que

$$a_1 + 2a_2 + 3a_3 + \cdots + ma_m = n.$$

Cada a_i deve ser representado como a soma de is que aparecem na partição de n, isto é, podemos expressar n da seguinte forma

$$n = 1 + \cdots + 1 + 2 + \cdots + 2 + \cdots + m + \cdots + m,$$

em que o número 1 aparece a_1 vezes, o número 2 aparece a_2 vezes e assim sucessivamente. Desta forma, cada partição de n vai contribuir com uma unidade para o coeficiente de x^n nesta expansão.

Como exemplo do que acabamos de expor, suponha que em cada uma das quatro primeiras séries, tenhamos tomado, respectivamente as seguintes potências de $x : x^4, x^6, x^6, x^{12}$. Escrevamos estas potências da seguinte forma

$$\begin{aligned} x^4 &= x^{1+1+1+1} \\ x^6 &= x^{2+2+2} \\ x^6 &= x^{3+3} \\ x^{12} &= x^{4+4+4}. \end{aligned}$$

Note que o produto das potências x acima resultam em x^{28} e com isso temos a seguite partição de 28 :

$$4 + 4 + 4 + 3 + 3 + 2 + 2 + 2 + 1 + 1 + 1 + 1.$$

Observe que o termo x^6 representa três 2 na segunda série e dois 3 na terceira série. Assim, as séries acima estão sendo vistas como

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k} = (1+x^1+x^{1+1}+x^{1+1+1}+\ldots)(1+x^2+x^{2+2}+x^{2+2+2}+\ldots)(1+x^3+x^{3+3}+x^{3+3+3}+\ldots)\ldots$$

A função $\frac{1}{1-x}$ "controla", portanto, a presença dos 1s, $\frac{1}{1-x^2}$ a presença dos 2s, $\frac{1}{1-x^3}$ a presença dos 3s,... , $\frac{1}{1-x^m}$ a presença dos ms. Isto prova, portanto, que

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k}$$

é a função geradora para partições irrestritas. Se estivermos interessados na função geradora para as partições de n em que nenhuma parte supera m, basta tomarmos:

$$\prod_{k=1}^{m} \frac{1}{1-x^k}.$$

Função geradora de partições de n em partes ímpares

Mostraremos a seguir que a função geradora de partições de n em partes ímpares é dada por:

$$\prod_{k=0}^{\infty} \frac{1}{1-x^{2k+1}}$$

Primeiro note que

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Substituindo x por x^3 e posteriormente por x^5 na equação acima temos, respectivamente,

$$\frac{1}{1-x^3} = 1 + x^3 + x^6 + x^9 + \cdots$$
$$\frac{1}{1-x^5} = 1 + x^5 + x^{10} + x^{15} + \cdots .$$

A partir disto podemos escrever

$$\prod_{k=0}^{\infty} \frac{1}{1-x^{2k+1}} = (1+x+x^2+x^3+x^4+\ldots)(1+x^3+x^6+x^9+\ldots)(1+x^5+x^{10}+x^{15}+\ldots)\ldots .$$

Sabemos que o expoente n de x será obtido a partir da soma de um expoente da primeira série, outro da segunda e assim sucessivamente, sendo que na primeira série o expoente será um múltiplo de 1, na segunda um múltiplo de 3, na terceira um múltiplo de 5 e assim sucessivamente, daí

$$a_1 + 3a_2 + 5a_3 + 7a_4 + \cdots + (2m-1)a_m = n,$$

que por sua vez podemos escrever

$$n = \underbrace{1 + \cdots + 1}_{a_1} + \underbrace{3 + \cdots + 3}_{a_2} + \cdots + \underbrace{2m-1 + \cdots + 2m-1}_{a_m}.$$

Assim, a série $\displaystyle\prod_{k=0}^{\infty} \frac{1}{1-x^{2k+1}}$ está sendo vista da seguinte maneira

$$\prod_{k=0}^{\infty} \frac{1}{1-x^{2k+1}} = (1 + x + x^{1+1} + \cdots)(1 + x^3 + x^{3+3} + \cdots)(1 + x^5 + x^{5+5} + \cdots)\cdots$$

em que a função $\frac{1}{1-x}$ "controla", portanto, a presença dos 1s, $\frac{1}{1-x^3}$ a presença dos 3s, $\frac{1}{1-x^5}$ a presença dos 5s,... , $\frac{1}{1-x^m}$ a presença dos ms, sendo m um número ímpar.

Portanto, a partição de n será dada a partir apenas de partes ímpares, já que o produto de x que resultará em x^n será formado apenas por potências de x com expoentes que são múltiplos de ímpares.

Função geradora de partições de n em partes pares

Mostraremos a seguir que a função geradora de partições de n em partes pares é dada por:

$$\prod_{k=1}^{\infty} \frac{1}{1-x^{2k}}$$

Primeiro note que

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Substituindo x por x^2, depois por x^4 e posteriormente por x^6 na equação acima temos, respectivamente,

$$\begin{aligned} \frac{1}{1-x^2} &= 1 + x^2 + x^4 + x^6 + \cdots \\ \frac{1}{1-x^4} &= 1 + x^4 + x^8 + x^{12} + \cdots \\ \frac{1}{1-x^6} &= 1 + x^6 + x^{12} + x^{18} + \cdots \end{aligned}$$

A partir disto, podemos escrever

$$\prod_{k=1}^{\infty} \frac{1}{1+x^{2k}} = (1 + x^2 + x^4 + x^6 + \cdots)(1 + x^4 + x^8 + x^{12} + \cdots)(1 + x^6 + x^{12} + x^{18} + \cdots)\cdots .$$

Sabemos que o expoente n de x será obtido a partir da soma de um expoente da primeira série, outro da segunda e assim sucessivamente, sendo que na primeira série o expoente será um múltiplo de 2, na segunda um múltiplo de 4, na terceira um múltiplo de 6 e assim sucessivamente, daí

$$2a_1 + 4a_2 + 6a_3 + \cdots + (2m)a_m = n$$

que por sua vez escrevemos

$$n = \underbrace{2 + \cdots + 2}_{a_1} + \underbrace{4 + \cdots + 4}_{a_2} + \cdots + \underbrace{2m + \cdots + 2m}_{a_m}.$$

Assim, a série $\displaystyle\prod_{k=1}^{\infty} \frac{1}{1-x^{2k}}$ está sendo vista da seguinte maneira

$$\prod_{k=1}^{\infty} \frac{1}{1-x^{2k}} = (1 + x^2 + x^{2+2} + \cdots)(1 + x^4 + x^{4+4} + \cdots)(1 + x^6 + x^{6+6} + \cdots)\cdots$$

em que a função $\frac{1}{1-x^2}$ "controla", portanto, a presença dos 2s, $\frac{1}{1-x^4}$ a presença dos 4s, $\frac{1}{1-x^6}$ a presença dos 6s,... , $\frac{1}{1-x^m}$ a presença dos ms, sendo m um número par.

Portanto, a partição de n será dada apenas por partes pares, já que o produto de x que resultará em x^n será formado apenas por potências de x com expoentes múltiplos de pares.

Função geradora de partições de n em partes que são cubos

Mostraremos a seguir que a função geradora de partições de n em partes que são cubos é dada por:

$$\prod_{k=1}^{\infty} \frac{1}{1-x^{k^3}}$$

Primeiro note que

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Substituindo x por x^8 e posteriormente por x^{27} na equação acima temos, respectivamente:

$$\frac{1}{1-x^8} = 1 + x^8 + x^{16} + x^{24} + \cdots$$
$$\frac{1}{1-x^{27}} = 1 + x^{27} + x^{54} + x^{81} + \cdots$$

A partir disto, sabemos que

$$\prod_{k=1}^{\infty} \frac{1}{1-x^{k^3}} = (1+x+x^2+x^3+x^4+\cdots)(1+x^8+x^{16}+x^{24}+\cdots)(1+x^{27}+x^{54}+x^{81}+\cdots)\cdots.$$

Sabemos que o expoente n de x será obtido a partir da soma de um expoente da primeira série, outro da segunda e assim sucessivamente, sendo que na primeira série o expoente será um múltiplo de 1^3, na segunda um múltiplo de 2^3, na terceira um múltiplo de 3^3 e assim sucessivamente, daí

$$a_1 + 8a_2 + 27a_3 + \cdots + (m^3)a_m = n$$

que por sua vez escrevemos

$$n = \underbrace{1+\cdots+1}_{a_1} + \underbrace{2^3+\cdots+2^3}_{a_2} + \cdots + \underbrace{m^3+\cdots+m^3}_{a_m}.$$

Assim a série $\prod_{k=1}^{\infty} \frac{1}{1-x^{k^3}}$ está sendo vista da seguinte maneira:

$$\prod_{k=1}^{\infty} \frac{1}{1-x^{k^3}} = (1 + x^1 + x^{1+1} + x^{1+1+1} + \cdots)(1 + x^{2^3} + x^{2^3+2^3} + x^{2^3+2^3+2^3} + \cdots)\cdots$$

em que a função $\frac{1}{1-x}$ "controla", portanto, a presença dos 1s, $\frac{1}{1-x^8}$ a presença dos 2^3s, $\frac{1}{1-x^{27}}$ a presença dos 3^3s,... , $\frac{1}{1-x^m}$ a presença dos ms, onde m é um cubo.

Portanto, a partição de n será dada apenas de partes que são cubos, já que o produto de x que resultará em x^n será formado apenas por potências de x com expoentes que são múltiplos de cubos.

Função geradora de partições de n em partes $2, 3, 4$ com ao menos uma parte 3

Mostraremos a seguir, que a função geradora de partições de n em partes $2, 3$ ou 4 com ao menos uma parte 3 é dada por

$$\frac{x^3}{(1-x^2)(1-x^3)(1-x^4)}$$

Primeiro note que

$$\begin{aligned}\frac{1}{1-x^2} &= 1 + x^2 + x^4 + x^6 + \cdots\,,\\ \frac{1}{1-x^3} &= 1 + x^3 + x^6 + x^9 + \cdots\,,\\ \frac{1}{1-x^4} &= 1 + x^4 + x^8 + x^{12} + \cdots\,.\end{aligned}$$

Logo, podemos escrever:

$$\begin{aligned}\frac{x^3}{(1-x^2)(1-x^3)(1-x^4)} &= x^3(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots)(1 + x^4 + x^8 + \cdots)\\ &= x^3(1 + x^2 + x^{2+2} + \cdots)(1 + x^3 + x^{3+3} + \cdots)(1 + x^4 + x^{4+4} + \cdots).\end{aligned}$$

Observe que o termo x^3 que aparece na frente do produto dos parênteses garante que o produto de potências de x sempre tenha ao menos um número 3 no expoente, mesmo quando o expoente de x nos demais parênteses seja zero, ou seja, $x^0 = 1$.

Portanto a função geradora de partições de n em partes $2, 3$ ou 4 com ao menos uma parte 3 é dada por

$$\frac{x^3}{(1-x^2)(1-x^3)(1-x^4)}. \tag{2.8}$$

2.4.2 Funções geradores e partições

Vejamos agora como as funções geradoras podem nos auxiliar na demonstração de resultados dentro da teoria das partições. Vimos uma série de exemplos onde associamos uma função geradora a partições com partes possuindo características específicas. Enquanto na Seção 2.3 utilizamos bijeções para mostrar que o número de partições de uma dada característica A era igual ao número de partições de uma dada característica B, aqui a nossa ferramenta será mostrar que as funções geradoras dos dois tipos de partições que estaremos comparando são iguais e consequentemente a quantidade dessas partições coincidirão.

Na Seção 2.3 enunciamos e provamos uma das várias contribuições de Euler para a teoria das partições, o Teorema 2.5. Nossa demonstração foi através de bijeção. Apresentaremos agora o mesmo teorema, porém com uma demonstração utilizando funções geradoras.

Teorema 2.15 *O número de partições de n em partes distintas é igual ao número de partições de n em partes ímpares.*

Demonstração: Sabemos que a função geradora para partições em partes distintas é dada por

$$\prod_{k=1}^{\infty}(1+x^k)$$

e que a função geradora para partições em partes ímpares é igual a

$$\prod_{k=1}^{\infty}\frac{1}{1-x^{2k-1}}.$$

Daí, basta que mostremos que ambas as expressões são idênticas. Temos,

$$\begin{aligned}
\prod_{k=1}^{\infty}(1+x^k) &= \prod_{k=1}^{\infty}\frac{(1+x^k)(1-x^k)}{1-x^k} \\
&= \prod_{k=1}^{\infty}\frac{1-x^{2k}}{1-x^k} \\
&= \frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots} \\
&= \frac{1}{(1-x)(1-x^3)(1-x^5)(1-x^7)\cdots} \\
&= \prod_{k=1}^{\infty}\frac{1}{1-x^{2k-1}}.
\end{aligned}$$

■

Vejamos mais alguns exemplos dessa utilização das funções geradoras.

Exemplo 2.15 *Todo inteiro positivo pode ser expresso de maneira única como soma de potências distintas de* 2.

De fato, pelos argumentos apresentados nesta seção, a função geradora para partições de n em potências distintas de 2 é dada por

$$(1+x)(1+x^2)(1+x^4)(1+x^8)\cdots(1+x^{2^k})\cdots$$

e o coeficiente de x^n da expanção deste produto nos fornece o número de maneiras de escrever n como soma de potências distintas de 2. Logo basta mostrarmos que o coeficiente de x^n é igual a 1 para todo n.

Sabemos que

$$\frac{1}{1-x} = 1 + x + x^{+}x^{3} + x^{4} + \cdots$$

logo nos resta provar que

$$\frac{1}{1-x} = (1+x)(1+x^2)(1+x^4)(1+x^8)\cdots(1+x^{2^k})\cdots .$$

Temos,

$$\begin{aligned}(1-x)(1+x)(1+x^2)(1+x^4)(1+x^8)\cdots &= (1-x^2)(1+x^2)(1+x^4)(1+x^8)\cdots\\ &= (1-x^4)(1+x^4)(1+x^8)(1+x^{16})\cdots\\ &= (1-x^8)(1+x^8)(1+x^{16})(1+x^{32})\cdots\\ &= (1-x^{16})(1+x^{16})(1+x^{32})(1+x^{64})\cdots\\ &= 1,\end{aligned}$$

já que $|x| < 1$ *e conforme o exponente de* x *cresce seu valor se aproxima de* 0.

Uma prova bijetiva para o exemplo acima foi apresentada no Teorema 2.6.

Exemplo 2.16 *Mostremos agora que o número de partições de* n *em partes distintas, nenhuma sendo múltipla de* 3, *é igual ao número de partições de* n *em partes da forma* $6j-1$ *ou* $6j-5$.

Das nossas discussões anteriores e dos exemplos apresentados podemos concluir que

$$\prod_{j=1}^{\infty}(1+x^{3j-2})(1+x^{3j-1})$$

e

$$\prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-1})(1-x^{6j-5})}$$

são as funções geradoras para partições de n *em partes distintas e não divisíveis por* 3 *e, para partições de* n *em partes da forma* $(6j-1)$ *ou* $(6j-5)$, *respectivamente. Logo devemos* *mostrar que tais funções geradoras são idênticas. De fato,*

$$
\begin{aligned}
\prod_{j=1}^{\infty}(1+x^{3j-2})(1+x^{3j-1}) &= \prod_{j=1}^{\infty}\frac{(1+x^{3j-2})(1+x^{3j-1})(1-x^{3j-2})(1-x^{3j-1})}{(1-x^{3j-2})(1-x^{3j-1})}\\
&= \prod_{j=1}^{\infty}\frac{(1-x^{6j-4})(1-x^{6j-2})}{(1-x^{3j-2})(1-x^{3j-1})}\\
&= \prod_{j=1}^{\infty}(1-x^{6j-4})(1-x^{6j-2})\prod_{j=1}^{\infty}\frac{1}{(1-x^{3j-2})(1-x^{3j-1})}\\
&= \prod_{j=1}^{\infty}(1-x^{6j-4})(1-x^{6j-2})\prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-4})(1-x^{6j-1})(1-x^{6j-5})(1-x^{6j-2})}\\
&= \prod_{j=1}^{\infty}\frac{1}{(1-x^{6j-1})(1-x^{6j-5})}.
\end{aligned}
$$

Exemplo 2.17 *Mostremos que o número de partições de n cujas partes não são divisíveis por 3 é igual ao número de partições de n nas quais cada parte aparece, no máximo, duas vezes.*

De fato, sabemos que a função geradora das patições de n cujas partes não são divisíveis por 3 é

$$\prod_{j=1}^{\infty}\frac{1}{(1-x^{3j-1})(1-x^{3j-2})},$$

e das nossas discussões anteriores, temos que a função geradora das partições de n nas quais cada parte aparece no máximo duas vezes é

$$\prod_{j=1}^{\infty}(1+x^{j}+x^{2j}).$$

Logo, devemos mostrar que tais funções geradoras são idênticas. Temos,

$$\begin{aligned}
\prod_{j=1}^{\infty}\frac{1}{(1-x^{3j-1})(1-x^{3j-2})} &= \frac{1}{(1-x)(1-x^2)(1-x^4)(1-x^5)(1-x^7)(1-x^8)\cdots}\\
&= \frac{(1-x^3)(1-x^6)(1-x^9)(1-x^{12})\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)\cdots}\\
&= \prod_{j=1}^{\infty}\frac{1-x^{3j}}{1-x^j}\\
&= \prod_{j=1}^{\infty}\frac{(1-x^j)(1+x^j+x^{2j})}{1-x^j}\\
&= \prod_{j=1}^{\infty}(1+x^j+x^{2j}).
\end{aligned}$$

Operador $\Omega_{\geq}$

Considere o seguinte problema: qual é a forma fechada para a função geradora $\sum_{n=0}^{\infty} p_m(n)q^n$, sendo $p_m(n)$ o número de partições de n em, no máximo, m partes?

Podemos escrever esta função geradora da seguinte forma:

$$\sum_{n=0}^{\infty} p_m(n)q^n = \sum_{n_1\geq n_2\geq\cdots\geq n_m\geq 0} q^{n_1+n_2+\cdots+n_m}.$$

A exigência $n_1 \geq n_2 \geq \cdots \geq n_m \geq 0$ ocorre já que a ordem das partes de uma partição não importam. Sejam λ_i novas variáveis e consideremos agora a seguinte soma

$$\sum_{n_1,n_2,\ldots,n_m\geq 0} q^{n_1+n_2+\cdots+n_m}\lambda_1^{n_1-n_2}\lambda_2^{n_2-n_3}\cdots\lambda_{m-1}^{n_{m-1}-n_m}. \tag{2.9}$$

Se selecionarmos apenas termos com expoentes não negativos em λ, então o expoente correspondente de q será uma partição de n em no máximo m partes. Por exemplo, se fixarmos $m = 2$ teremos

$$\sum_{n=0}^{\infty} p_2(n)q^n = q^0\lambda_1^0+q^1\lambda_1^1+q^2\lambda_1^2+q^{1+1}\lambda_1^0\lambda_2^1+q^3\lambda_1^3+q^{2+1}\lambda_1^1\lambda_2^1+q^4\lambda_1^4+q^{3+1}\lambda_1^2\lambda_2^1+q^{2+2}\lambda_1^0\lambda_2^2+\cdots$$

Note, utilizando a soma acima, que os expoentes de λ que restam são 0 para $n = 0$, 1 para $n = 1$, 2 e $1 + 1$ para $n = 2$ e assim sucessivamente, que são partições de n em no máximo 2 partes.

Definamos agora um operador linear $\Omega_{\geq}$ que assim como no exemplo acima, ele age nas variáveis λ anulando os termos tendo expoentes negativos e além disso, ele substitui as demais variáveis λ por 1.

Lema 2.1

$$\Omega_{\geq}\frac{1}{(1-\lambda x)\left(1-\frac{y}{\lambda}\right)}=\frac{1}{(1-x)(1-xy)}.$$

Demonstração: Note que

$$\begin{aligned}\Omega_{\geq}\frac{1}{(1-\lambda x)\left(1-\frac{y}{\lambda}\right)} &= \Omega_{\geq}\sum_{n,m\geq 0}(\lambda x)^n\left(\frac{y}{\lambda}\right)^m\\ &= \Omega_{\geq}\sum_{n,m\geq 0}\lambda^n x^n\frac{y^m}{\lambda^m}\\ &= \Omega_{\geq}\sum_{n,m\geq 0}\frac{\lambda^n}{\lambda^m}x^n y^m\\ &= \Omega_{\geq}\sum_{n,m\geq 0}\lambda^{n-m}x^n y^m\\ &= \Omega_{\geq}\sum_{n,m\geq 0}\lambda^{n-m}x^n y^m\\ &= \sum_{n\geq m\geq 0}x^n y^m.\end{aligned}$$

Fazendo $k=n-m$, temos

$$\sum_{k,m\geq 0}x^{m+k}y^m=\sum_{k\geq 0}x^k\sum_{m\geq 0}(xy)^m=\frac{1}{(1-x)(1-xy)}.$$

■

Antes de aplicarmos efetivamente o operador $\Omega_{\geq}$ em (2.9), vamos reescrever a igualdade de uma maneira mais simples de utilizarmos o Lema 2.1.

$$
\begin{aligned}
\sum_{n=0}^{\infty} p_m(n)q^n &= \Omega_{\geq} \sum_{n_1,n_2,\cdots,n_m\geq 0} q^{n_1+n_2+\cdots+n_m} \lambda_1^{n_1-n_2}\lambda_2^{n_2-n_3}\cdots\lambda_{m-1}^{n_{m-1}-n_m} \\
&= \Omega_{\geq} \sum_{n_1,n_2,\ldots,n_m\geq 0} q^{n_1}q^{n_2}\cdots q^{n_m} \frac{\lambda_1^{n_1}}{\lambda_1^{n_2}}\frac{\lambda_2^{n_2}}{\lambda_2^{n_3}}\cdots\frac{\lambda_{m-1}^{n_{m-1}}}{\lambda_{m-1}^{n_m}} \\
&= \Omega_{\geq} \sum_{n_1,n_2,\ldots,n_m\geq 0} (q\lambda_1)^{n_1}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\cdots\left(\frac{q}{\lambda_{m-1}}\right)^{n_m} \\
&= \Omega_{\geq} \sum_{n_1\geq 0}(q\lambda_1)^{n_1}\sum_{n_2\geq 0}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\cdots\sum_{n_m\geq 0}\left(\frac{q}{\lambda_{m-1}}\right)^{n_m} \\
&= \Omega_{\geq} \frac{1}{(1-q\lambda_1)\left(1-\frac{q\lambda_2}{\lambda_1}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)}.
\end{aligned}
$$

Se aplicarmos o Lema 2.1 sucessivas vezes obteremos a forma fechada para a função geradora de $p_m(n)$. Com uma aplicação temos

$$\sum_{n=0}^{\infty} p_m(n)q^n = \Omega_{\geq} \frac{1}{(1-q)\left(1-q^2\lambda_2\right)\left(1-\frac{q\lambda_3}{\lambda_2}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)}.$$

Com uma segunda aplicação resultamos em

$$\sum_{n=0}^{\infty} p_m(n)q^n = \Omega_{\geq} \frac{1}{(1-q)\left(1-q^2\right)\left(1-q^3\lambda_3\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)}.$$

Continuando, obtemos finalmente,

$$\sum_{n=0}^{\infty} p_m(n)q^n = \frac{1}{(1-q)(1-q^2)(1-q^3)\cdots(1-q^m)}.$$

Apresentaremos a seguir, um exemplo para ilustrar o método descrito acima. Para isso será necessário o uso do lema que segue abaixo, que é uma versão estendida do lema anterior, cuja demonstração é bem semelhante a do Lema 2.1.

Lema 2.2 *Se α é um inteiro não-negativo,*

$$\Omega_{\geq} \frac{\lambda^{-\alpha}}{(1-\lambda x)\left(1-\frac{y}{\lambda}\right)} = \frac{x^{\alpha}}{(1-x)(1-xy)}.$$

Para nosso exemplo, seja n um inteiro positivo e $\Delta(n)$ o número de triângulos não-congruentes de perímetro n e lados inteiros. Vamos procurar uma interpretação para $\displaystyle\sum_{n=0}^{\infty} \Delta(n)q^n$.

Suponha que n_1, n_2, n_3 sejam os lados do triângulo em ordem não crescente. Pela desigualdade triangular, devemos ter $n_2 + n_3 \geq n_1 + 1$. Assim,

$$\begin{aligned}
\sum_{n=0}^{\infty} \Delta(n)q^n &= \Omega_{\geq} \sum_{n_1,n_2,n_3\geq 0} q^{n_1+n_2+n_3} \lambda_1^{n_1-n_2} \lambda_2^{n_2-n_3} \lambda_3^{n_2+n_3-n_1-1} \\
&= \Omega_{\geq} \sum_{n_1,n_2,n_3\geq 0} q^{n_1} q^{n_2} q^{n_3} \frac{\lambda_1^{n_1}}{\lambda_1^{n_2}} \frac{\lambda_2^{n_2}}{\lambda_2^{n_3}} \frac{\lambda_3^{n_2}\lambda_3^{n_3}}{\lambda_3^{n_1}\lambda_3} \\
&= \Omega_{\geq} \sum_{n_1,n_2,n_3\geq 0} \left(\frac{q\lambda_1}{\lambda_3}\right)^{n_1} \left(\frac{q\lambda_2\lambda_3}{\lambda_1}\right)^{n_2} \left(\frac{q\lambda_3}{\lambda_2}\right)^{n_3} \lambda_3^{-1} \\
&= \Omega_{\geq} \frac{\lambda_3^{-1}}{\left(1 - \frac{q\lambda_1}{\lambda_3}\right)\left(1 - \frac{q\lambda_2\lambda_3}{\lambda_1}\right)\left(1 - \frac{q\lambda_3}{\lambda_2}\right)} \\
&= \Omega_{\geq} \frac{\lambda_3^{-1}}{\left(1 - \frac{q}{\lambda_3}\right)(1 - q^2\lambda_2)\left(1 - \frac{q\lambda_3}{\lambda_2}\right)} \\
&= \Omega_{\geq} \frac{\lambda_3^{-1}}{\left(1 - \frac{q}{\lambda_3}\right)(1 - q^2)(1 - q^3\lambda_3)} \\
&= \frac{q^3}{(1-q^2)(1-q^3)(1-q^4)}.
\end{aligned}$$

Note que, a expressão resultante no desenvolvimento acima coincide com a expressão obtida em (2.8). Portanto, $\Delta(n)$ é o número de partições de n em partes $2, 3$ ou 4, com, ao menos, uma parte 3.

Teorema 2.16 *Seja $t_m(n)$ o número de partições de n em exatamente m partes distintas. Então,*

$$\sum_{n=0}^{\infty} t_m(n)q^n = \frac{q^{\frac{m(m+1)}{2}}}{(1-q)(1-q^2)\cdots(1-q^m)}.$$

Demonstração: Se $n_1 + n_2 + \cdots n_m$ é uma partição de n em partes distintas, então $n_1 \geq$

$n_2+1, n_2 \geq n_3+1, \ldots, n_m \geq 1$. Daí,

$$\begin{aligned}\sum_{n=0}^{\infty} t_m(n)q^n &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} q^{n_1+n_2+\cdots n_m}\lambda_1^{n_1-n_2-1}\lambda_2^{n_2-n_3-1}\cdots\lambda_{m-1}^{n_{m-1}-n_m-1}\lambda_m^{n_m-1}\\ &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} (q\lambda_1)^{n_1}\lambda_1^{-1}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\lambda_2^{-1}\cdots\left(\frac{q\lambda_m}{\lambda_{m-1}}\right)^{n_m}\lambda_m^{-1}\\ &= \Omega_{\geq}\frac{\lambda_1^{-1}\lambda_2^{-1}\cdots\lambda_m^{-1}}{(1-\lambda_1 q)\left(1-\frac{q\lambda_2}{\lambda_1}\right)\cdots\left(1-\frac{q\lambda_m}{\lambda_{m-1}}\right)}.\end{aligned}$$

Aplicando agora o Lema 2.2 sucessivas vezes, obtemos

$$\begin{aligned}\sum_{n=0}^{\infty} t_m(n)q^n &= \Omega_{\geq}\frac{q\lambda_2^{-1}\cdots\lambda_m^{-1}}{(1-q)(1-\lambda_2q^2)\left(1-\frac{q\lambda 3}{\lambda_2}\right)\cdots\left(1-\frac{q\lambda_m}{\lambda_{m-1}}\right)}\\ &= \Omega_{\geq}\frac{q\cdot q^2\lambda_3^{-1}\cdots\lambda_m^-1}{(1-q)(1-q^2)\left(1-\frac{q\lambda_3}{\lambda_2}\right)\cdots\left(1-\frac{q\lambda_m}{\lambda_{m-1}}\right)}\\ &= \frac{q\cdot q^2\cdots q^m}{(1-q)(1-q^2)\cdots(1-q^m)},\end{aligned}$$

que conclui a demonstração. ■

Iremos agora provar um teorema no qual, $t_m^{(k,l)}(n)$ é o número de partições de n tendo exatamente m partes, a diferença entre duas partes é $\geq k$ e a menor parte é $\geq l$.

Teorema 2.17

$$\sum_{n=0}^{\infty} t_m^{(k,l)}(n)q^n = \frac{q^{\frac{m(k(m-1)+2l)}{2}}}{(1-q)(1-q^2)\cdots(1-q^m)}.$$

Demonstração: Note que

$$\begin{aligned}\sum_{n=0}^{\infty} t_m^{(k,l)}(n)q^n &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} q^{n_1+n_2+\cdots+n_m}\lambda_1^{n_1-n_2-k}\cdots\lambda_{m-1}^{n_{m-1}-n_m-k}\lambda_m^{n_m-l}\\ &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} (q\lambda_1)^{n_1}\lambda_1^{-k}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\lambda_2^{-k}\cdots\left(\frac{q\lambda_m}{\lambda_{m-1}}\right)^{n_m}\lambda_m^{-l}\\ &= \Omega_{\geq}\frac{\lambda_1^{-k}\lambda_2^{-k}\cdots\lambda_{m-1}^{-k}\lambda_m^{-l}}{(1-q\lambda_1)\left(1-\frac{q\lambda_2}{\lambda_1}\right)\cdots\left(1-\frac{q\lambda_m}{\lambda_{m-1}}\right)}.\end{aligned}$$

E aplicando sucessivas vezes o Lema 2.2, temos

$$\frac{q^{\frac{m(k(m-1)+2l)}{2}}}{(1-q)(1-q^2)\cdots(1-q^m)}.$$

A única diferença em relação à demonstração anterior é que, nas primeiras $m-1$ aplicações de $\Omega_{\geq}$, $\alpha = k$ e, na última aplicação, $\alpha = l$ e $y = 0$ no Lema 2.2. ■

Função geradora em duas variáveis

Muitas das vezes precisamos de uma função geradora que controle não apenas o número que está sendo particionado. Por exemplo se estivermos interessados em saber o número de partes de cada partição gerada não é difícil perceber que na função

$$(1+zq^{n_1})(1+zq^{n_2})(1+zq^{n_3}) = 1+zq^{n_1}+zq^{n_2}+zq^{n_3}+z^2q^{n_1+n_2}+z^2q^{n_1+n_3}z^2q^{n_2+n_3}+z^3q^{n_1+n_2+n_3}$$

o expoente da variável z controla o número de partes de cada partição gerada.

Com o mesmo raciocínio empregado no exemplo acima podemos deduzir outras funções geradoras em duas variáveis, por exemplo

$$\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} p(n \mid m \quad \text{partes distintas, cada parte} \in S)z^m q^n = \prod_{k\in S}(1+zq^k);$$

$$\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} p(n \mid m \quad \text{partes, cada parte} \in S)z^m q^n = \prod_{k\in S}\frac{1}{(1-zq^k)};$$

$$\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} p(n \mid m \quad \text{partes, cada parte} \in S \quad \text{e aparece, no máximo} \quad d \quad \text{vezes})z^m q^n = f(z,q),$$

onde $f(z,q) = \prod_{k\in S}\frac{(1-z^{d+1}q^{(d+1)k})}{(1-zq^k)}$.

Caso S seja um conjunto infinito, devemos ter $|q| < 1$ para as três funções citadas acima. Para a segunda função, devemos adicionar a exigência $|z| < \frac{1}{q}$.

Exemplo 2.18 *Com raciocínio semelhante ao que foi empregado nas funções geradoras citadas acima, podemos observar que*

$$\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} p(n \mid \textit{tendo} \quad m \quad \textit{partes pares})z^m q^n = \prod_{k=0}^{m}\frac{1}{1-zq^{2k}},$$

em que $m, n \in \mathbb{Z}_+^*$ *e* $|q| < 1$.

Teorema 2.18 *Seja* $b_m(j,n)$ *(respectivamente,* $t_m(j,n)$*) o número de partições de* n *em no máximo* m *partes (respectivamente, exatamente* m *partes distintas) com maior parte* j*. Então,*

$$\sum_{j,n\geq 0} b_m(j,n)z^j q^n = \frac{1}{(1-zq)(1-zq^2)\cdots(1-zq^m)}$$

e

$$\sum_{j,n\geq 0} t_m(j,n)z^jq^n = \frac{z^m q^{\frac{m(m+1)}{2}}}{(1-zq)(1-zq^2)\cdots(1-zq^m)}.$$

Demonstração: Pela definição de $b_m(j,n)$, temos

$$\begin{aligned}
\sum_{j,n\geq 0} b_m(j,n)z^jq^n &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} z^{n_1}q^{n_1+n_2+\cdots+n_m}\lambda_1^{n_1-n_2}\lambda_2^{n_2-n_3}\cdots\lambda_{m-1}^{n_{m-1}-n_m} \\
&= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} (zq\lambda_1)^{n_1}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\cdots\left(\frac{q}{\lambda_{m-1}}\right)^{n_m} \\
&= \Omega_{\geq} \frac{1}{(1-zq\lambda_1)\left(1-\frac{q\lambda_2}{\lambda_1}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)}
\end{aligned}$$

Com aplicações sucecivas do Lema 2.1 temos

$$\begin{aligned}
\sum_{j,n\geq 0} b_m(j,n)z^jq^n &= \Omega_{\geq} \frac{1}{(1-zq)(1-zq^2\lambda_2)\left(1-\frac{q\lambda_3}{\lambda_2}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)} \\
&= \Omega_{\geq} \frac{1}{(1-zq)(1-zq^2)(1-zq^3\lambda_3)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)} \\
&= \frac{1}{(1-zq)(1-zq^2)\cdots(1-zq^m)}.
\end{aligned}$$

A demonstração da outra identidade segue

$$\begin{aligned}
\sum_{j,n\geq 0} t_m(j,n)z^jq^n &= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} z^{n_1}q^{n_1+n_2+\cdots+n_m}\lambda_1^{n_1-n_2-1}\lambda_2^{n_2-n_3-1}\cdots\lambda_{m-1}^{n_{m-1}-n_m-1}\lambda_m^{n_m-1} \\
&= \Omega_{\geq} \sum_{n_1,\ldots,n_m\geq 0} (zq\lambda_1)^{n_1}\lambda_1^{-1}\left(\frac{q\lambda_2}{\lambda_1}\right)^{n_2}\lambda_2^{-1}\cdots\left(\frac{q}{\lambda_{m-1}}\right)^{n_m}\lambda_m^{-1} \\
&= \Omega_{\geq} = \frac{\lambda_1^{-1}\lambda_2^{-1}\cdots\lambda_m^{-1}}{(1-zq\lambda_1)\left(1-\frac{q\lambda_2}{\lambda_1}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)}
\end{aligned}$$

Agora, aplicando sucessivas vezes o Lema 2.1 temos

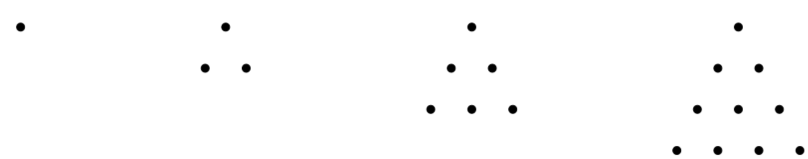
$$\begin{aligned}
\sum_{j,n\geq 0} t_m(j,n)z^jq^n &= \Omega_{\geq} \frac{zq\lambda_2^{-1}\cdots\lambda_m^{-1}}{(1-zq)(1-zq^2\lambda_2)\left(1-\frac{q\lambda_3}{\lambda_2}\right)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)} \\
&= \Omega_{\geq} \frac{zq\cdot zq^2\lambda_3^{-1}\cdots\lambda_m^{-1}}{(1-zq)(1-zq^2)(1-zq^3\lambda_3)\cdots\left(1-\frac{q}{\lambda_{m-1}}\right)} \\
&= \frac{z^m q^{\frac{m(m+1)}{2}}}{(1-zq)(1-zq^2)\cdots(1-zq^m)}.
\end{aligned}$$

■

2.5 Números triangulares e números pentagonais

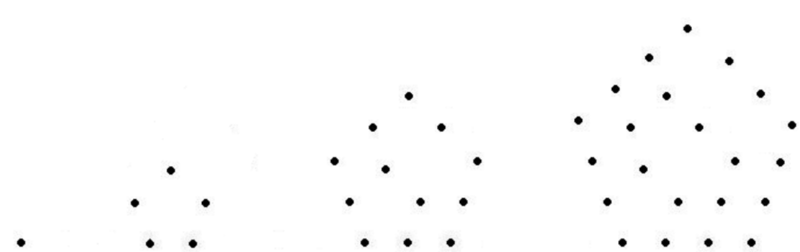
Elaborados pelos pitagóricos, os *números figurados* são números expressos como reunião de pontos numa determinada configuração geométrica, ou seja, um número é representado por uma quantidade de pontos que são agrupados em formas sugestivas. Deste números, os mais estudados têm sido os números poligonais, dos quais destacamos os triangulares e os pentagonais. A seguir, encerraremos nosso trabalho apresentando dois importantes teoremas da teoria de partições de inteiros que envolvem estes números, entre eles o *Teorema dos Números Pentagonais de Euler*. Apresentaremos apenas a versão combinatória deste teorema, e com as ferramentas que desenvolvemos neste trabalho, será possível apresentarmos uma demonstração do mesmo.

Definição 2.4 *Os* ***números triangulares*** *são* $1, 3, 6, 10, \ldots$, *referentes ao número de pontos nos triângulos em ordem crescente:*

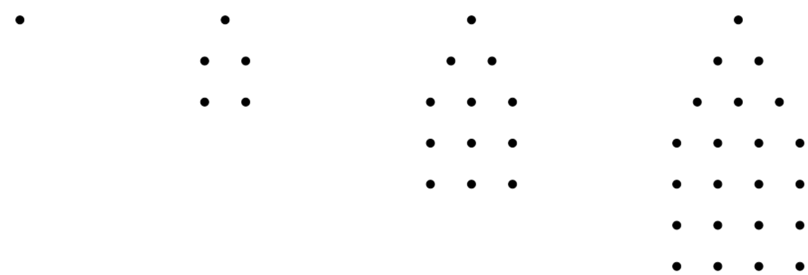


O j-ésimo número triangular é dado por $1+2+3+\cdots+j = \dfrac{j(j+1)}{2}$. De maneira análoga, podemos definir os números pentagonais.

Definição 2.5 *Os números pentagonais são* $1, 5, 12, 22, \ldots$, *referentes ao número de pontos nos pentágonos abaixo:*



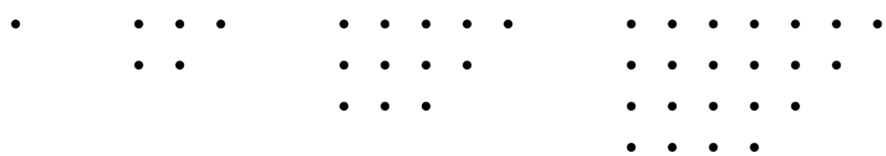
Vamos agora representar os números pentagonais da seguinte forma:



Desta forma, vemos que o j-ésimo número pentagonal consiste em um triângulo equilátero de lado j sobre um retângulo de lados j e $j-1$, com isso, o j-ésimo número pentagonal é

$$\frac{j(j+1)}{2} + j(j-1) = \frac{j(3j-1)}{2}.$$

A partir da representação gráfica dos números pentagonais acima podemos obter gráficos de Ferrers de partições rotacionando os diagramas e alinhando suas linhas à esquerda:



Teorema 2.19 (Teorema dos Números Pentagonais de Euler)

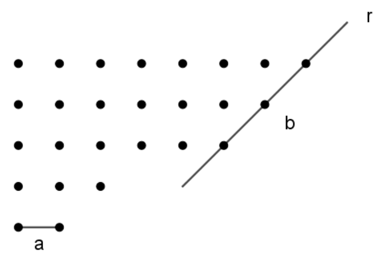
$$p(n \mid \textit{número par de partes distintas}) = p(n \mid \textit{número ímpar de partes distintas}) + e(n),$$

em que

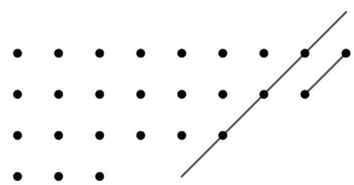
$$e(n) = \begin{cases} (-1)^j, & \textit{se} \quad n = \dfrac{j(3j \pm 1)}{2} \\ 0, & \textit{caso contrário.} \end{cases}$$

Demonstração: Iremos agora construir uma bijeção entre as partições de n em um número par de partes distintas e as partições de n em um número ímpar de partes distintas. Essa prova bijetiva foi obtida por F. Flanklin em 1881.

Considere um Gráfico de Ferrers de uma partição de n em partes distintas. Vamos chamar de a a menor parte e de b, o número de pontos sobre a linha r mostrada na figura a seguir:

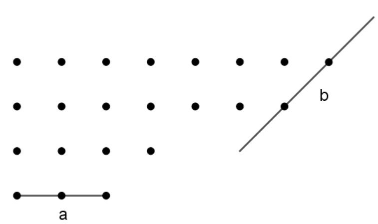


Se $a \leq b$, como na figura acima, removeremos os a pontos e os colocaremos paralelos a reta r de forma que ocupem as primeiras linhas do gráfico de Ferrers:

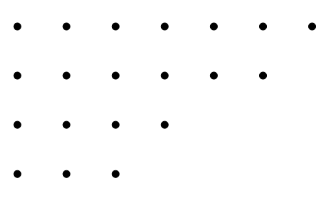


Feita tal mudança podemos observar que temos uma nova partição de n, possuindo partes distintas e representadas em ordem decrescente e com paridade diferente da anterior, ou seja, se o total de partes era par, agora é ímpar e se era ímpar, agora é par. Note também que, ainda que tivéssemos $a = b$ a mudança acima ainda teria sido possível.

Vejamos agora, um caso em que $a > b$. Considere o gráfico de Ferrers abaixo:

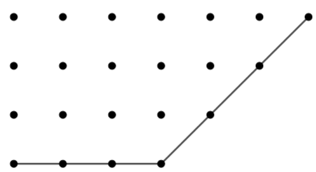


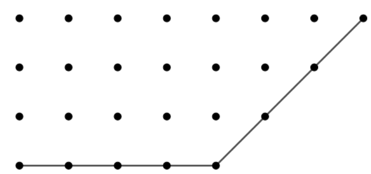
Neste caso podemos tomar os b pontos da linha r e colocá-los abaixo da parte de tamanho a, desta forma teremos uma nova partição com diferente pariedade. Feita tal alteração na partição continuaremos com uma partição em partes distintas e colocadas em ordem decrescente em seu gráfico de Ferrers.



Vemos que quando uma das transformações acima puder ser feita, teremos uma correspndência entre as partições de n em um número par de partes distintas e as partições de n em um número ímpar de partes distintas. Porém, as duas transformações mostradas acima nem sempre podem ser feitas. Existem dois casos em que a linha r passa do último ponto da menor parte. Isso ocorre quando $a = b$ ou $a = b + 1$

Com ajuda dos gráficos abaixo fica fácil ver que não podemos fazer nenhuma das transformações descritas até então, já que sempre que executada uma destas transformações, devemos ter partes distintas e dispostas em ordem decrescente.


a = b


a = b + 1

Nas figuras acima temos

$$n = a + (a+1) + (a+2) + \cdots + (a + (b-1)) = \frac{b(2a+b-1)}{2}.$$

Daí, no caso $a = b + 1$ temos $n = \dfrac{b(3b+1)}{2}$, logo, se b que é o número de partes, for par, teremos

$$p(n \mid \text{número par de partes distintas}) - p(n \mid \text{número ímpar de partes distintas}) = 1$$

e se b for ímpar

$$p(n \mid \text{número par de partes distintas}) - p(n \mid \text{número ímpar de partes distintas}) = -1,$$

ou seja, teremos exatamente uma partição contendo um número par (ímpar) de partes distintas excedendo aquelas com um número ímpar (par) de partes distintas.

No caso em que $a = b$, teremos

$$n = \frac{b(3b-1)}{2}$$

e a mesma análise acima pode ser feita, ou seja,

$$p(n \mid \text{número par de partes distintas}) - p(n \mid \text{número ímpar de partes distintas}) = (-1)^b,$$

o que conclui a demonstração do teorema. ■

Vejamos agora um teorema envolvendo a função geradora para os números triangulares, que possui uma prova bijetiva semelhante à do Teorema dos Números Pentagonais dada por F. Flanklin.

Teorema 2.20 *Para* $|q| < 1$

$$1 + q + \sum_{n=1}^{\infty} \frac{(1-q^2)(1-q^4)\cdots(1-q^{2n})}{(1-q^3)(1-q^5)\cdots(1-q^{2n+1})} q^{2n+1} = \sum_{n=0}^{\infty} q^{\frac{n(n+1)}{2}}. \tag{2.10}$$

Observe que, a soma do lado esquerdo da equação acima gera partições em que as partes são maiores do que 1, as partes pares são distintas, a maior parte é ímpar e tendo um peso associado dado por $(-1)^m$ em que m é o número de partes pares. Além disso, é facil ver que os expoentes do lado direito da equação acima são os números triangulares. Note que a equação abaixo é equivalente a Equação (2.10)

$$\sum_{n=1}^{\infty} \frac{(1-q^2)(1-q^4)\cdots(1-q^{2n})}{(1-q^3)(1-q^5)\cdots(1-q^{2n+1})} q^{2n+1} = \sum_{n=2}^{\infty} q^{\frac{n(n+1)}{2}}. \tag{2.11}$$

Temos como objetivo para provarmos a equação acima, mostrar que os coeficientes de q^n do lado esquerdo são iguais a 1 se n é um número triangular e 0, caso contrário. Em outras palavras, é equivalente mostrar que, se $p_e(n)(p_o(n))$ denota o número de partições de n geradas pelo lado esquerdo de (2.11) tendo um número par (ímpar) de partes pares, então devemos mostrar que

$$p_e(n) - p_o(n) = \begin{cases} 1, \text{se} \quad n \quad \text{é um número triangular} \\ 0, \text{caso contrário.} \end{cases} \tag{2.12}$$

De fato, se $P(n)$ denota o conjunto das partições de n em partes maiores do que 1, tendo todas as partes pares distintas e a maior parte ímpar, então

$$|P(n)| = p_e(n) + p_o(n).$$

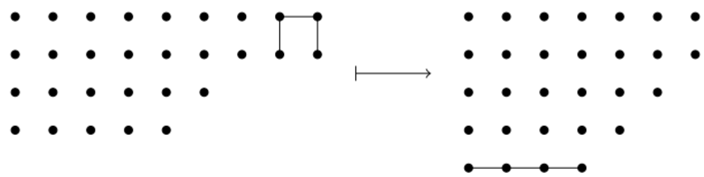
A ideia utilizada na demonstração a seguir é mostrar que, dada uma partição de n contada em $p_e(n)$ obtemos uma correspondente contada em $p_o(n)$ e vice-versa, para todos os valores de n exceto se n for um número triangular.

Se n não é um número triangular, existe uma bijeção entre o conjunto de partições contado por $p_e(n)$ e o conjunto de partições de n contado por $p_o(n)$, daí $p_e(n) - p_o(n) = 0$.

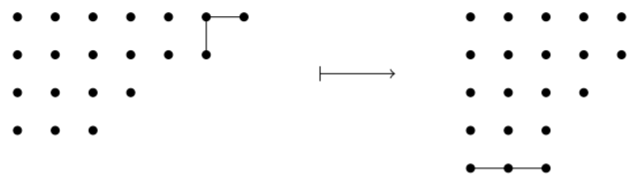
No caso de n ser um número triangular, existe uma partição contada em $p_e(n)$ que não tem correspondente contada por $p_o(n)$, daí, $p_e(n) - p_o(n) = 1$.

Demonstração: Definamos em $P(n)$ a seguinte transformação: dada uma partição $\lambda = \lambda_1 + \cdots + \lambda_s \in P(n)$ consideramos seu gráfico de Ferrers e removamos as duas últimas colunas para formarmos uma nova parte λ_{s+1}. Com isso ficamos com uma partição $\lambda' = \lambda'_1 + \cdots + \lambda'_s$ de $n - \lambda_{s+1}$.

Posteriormente, inserimos esta nova parte abaixo da menor parte de λ' quando $\lambda_{s+1} \leq \lambda'_s$ e λ'_s é ímpar ou $\lambda_{s+1} < \lambda'_s$ e λ'_s é par, resultando na partição $\lambda'' = \lambda'_1 + \cdots + \lambda'_s + \lambda_{s+1} \in P(n)$. Como exemplo:



e



Se por acaso $\lambda_{s+1} > \lambda'_s$ ou $\lambda_{s+1} = \lambda'_s$ e λ'_s é par não podemos realizar a operação acima a fim de termos uma nova partição em $P(n)$. Quando isso acontece, removemos a menor parte λ_s de λ para formarmos duas colunas para adicionarmos ao gráfico de Ferrers da partição $\lambda_1 + \cdots + \lambda_{s-1}$, em que serão iguais quando λ_s é par ou que diferem por 1 quando λ_s é ímpar. Podemos observar que a nova partição formada a partir desta operação está em $P(n)$, já que todas suas partes continuarão sendo maiores do que 1, pois a menor parte retirada é maior que 1 e o gráfico de Ferrers tem suas partes dispostas em ordem não crescente, todas as partes pares são distintas já que eram distintas antes e agora foram somadas mais duas unidades quando λ_s é par ou então se torna uma parte ímpar se for somada apenas uma unidade e a maior parte continua ímpar ja que resultará da soma de uma parte ímpar com uma parte 2. Como exemplo:

e

Observe que, quando n é um número triangular, ou seja, tem forma $n = \frac{k(k+1)}{2}$, nenhuma das duas operações definidas acima podem ser aplicadas aquela partição em $P(n)$ tendo $\frac{k}{2}$

partes $k+1$, quando k é par ou $\frac{k+1}{2}$, se k é ímpar.

De fato, se removermos as duas últimas colunas da partição que tem $\frac{k}{2}$ partes $k+1$, quando k é par, a nova parte terá tamanho $2\frac{k}{2} = k$ e, consequentemente, não podemos colocá-la abaixo da menor parte $k+1-2 = k-1$. Inversamente, removendo a menor parte, cujo tamanho é $k+1$, não podemos colocar as duas novas colunas obtidas, uma tendo tamanho $\frac{k}{2}+1$ e a outra $\frac{k}{2}$, em frete a última coluna, que tem tamanho $\frac{k}{2}-1$, da partição com a menor parte removida.

Se removermos as duas últimas colunas da partição que tem $\frac{k+1}{2}$ partes k, quando k é ímpar, a nova parte terá tamanho $2\frac{k+1}{2} = k+1$ e , consequentemente, não podemos colocá-la abaixo da menor parte $k-2$. Inversamente, removendo a menor parte, cujo tamanho é k, não podemos colocar as duas novas colunas obtidas, a maior tendo tamanho $\frac{k+1}{2}$, em frente a última coluna, que tem tamanho $\frac{k-1}{2}$ da partição com a menor parte removida.

Por exemplo, não podemos aplicar nenhuma das duas operações nas partições de 6 em que $k = 3$ e 10 em que $k = 4$ abaixo:

$$\begin{array}{ccc} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{array} \qquad\qquad \begin{array}{ccccc} \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \end{array}$$

Para concluirmos a demonstração, basta mostrarmos que as transformações descritas acima, quando aplicadas, mudam a paridade do número de partes pares. Feito isso, teremos mostrado que (2.12) é valida.

Para aquelas partições em $P(n)$ nas quais podemos remover as duas últimas colunas do gráfico de Ferrers, temos duas possibilidades: se as colunas têm o mesmo tamanho, não modificamos o número de partes ímpares e a nova parte terá tamanho par, o que modifica a paridade do número de partes pares; se as colunas diferem por 1 perdemos uma parte par e obtemos uma parte ímpar como nova parte modificando a paridade do número de partes pares. Estes argumentos podem ser facilmente invertidos para mostrar que a outra transformação também modifica a paridade do número de partes pares.

$\blacksquare$

CONSIDERAÇÕES FINAIS

Com a realização deste trabalho foi possível revisar alguns importantes conceitos da teoria dos números, além de nos aprofundarmos em conceitos mais avançados e resultados ou conjecturas, propostas por grandes nomes da matemática, como Euler e Ramanujan, sobre partições de inteiros.

É interessante ver como a matemática está ligada a inúmeros momentos da nossa vida e traz explicações para tantos feitos ou ocorrências, como por exemplo, a sequência de Fibonacci e suas diversas aparições em padrões na natureza.

Chama a atenção o fato de que, para muitas das demonstrações sobre partições de inteiros uma importante técnica utilizada, baseia-se em conceitos simples de matemática básica, como o de função bijetora, mas que por muitas vezes não era tão simples encontarmos essa tal bijeção entre dois conjuntos. Outro ponto, é o fato de como o recurso visual, a partir dos gráficos de Ferres, nos permitem fazer com que as demonstrações analíticas se tornem menos extensas e de caráter mais didático para o leitor.

Até aqui ficou evidente a importância dos estudos de nomes como Euler, Ramanujan e Hardy para o desenvolvimento da área. Entretanto, também ficou claro o quanto ela ainda deve ser desenvolvida, haja visto que muitos problemas ainda estão sem respostas, como por exemplo a obtenção de uma prova bijetiva para as identidades de Rogers-Ramanujan. Um caminho natural para prosseguimento do trabalho é analisar mais detalhadamente as novas representações de partições que vêm surgindo, em especial, a representação matricial. E tentar utilizar essa representação em provas bijetivas e/ou usando funções geradoras para obter novas identidades dentro da teoria.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] A. Vidigal, et al., *Fundamentos de Álgebra*, Editora UFMG, Belo Horizonte, MG, 2005.

[2] E. Tengan, et al., *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, 5. edição, Projeto Euclides, IMPA, Rio de Janeiro, RJ, 2018.

[3] J. P. O. Santos, *Introdução à Teoria dos Números*, 3. edição, Coleção Matemática Universitária, IMPA, Rio de Janeiro, RJ, 2018.

[4] J. P. O. Santos, R. Silva, *Aspectos Combinatórios da Teoria Aditiva dos Números*, 1. Colóquio de Matemática da Região Sul, UFSM, Santa Maria, RS, 2010.