

# Teoria Combinatorial dos Números

Thiago Landim

Março 2019

- 1 Apresentação dos Problemas
- 2 Definições e Resultados Básicos
- 3 Parte 1
- 4 Parte 2

# Problemas

- ① **Problemas Extremais.** Qual o maior conjunto  $A \subset \{1, 2, \dots, n\}$  que satisfaz uma propriedade  $\mathcal{P}$  dada?

# Problemas

- ① **Problemas Extremais.** Qual o maior conjunto  $A \subset \{1, 2, \dots, n\}$  que satisfaz uma propriedade  $\mathcal{P}$  dada?
- ② **Problemas de Contagem.** Quantos conjuntos  $A \subset \{1, 2, \dots, n\}$  satisfazem uma propriedade  $\mathcal{P}$  dada?

# Problemas

- ① **Problemas Extremais.** Qual o maior conjunto  $A \subset \{1, 2, \dots, n\}$  que satisfaz uma propriedade  $\mathcal{P}$  dada?
- ② **Problemas de Contagem.** Quantos conjuntos  $A \subset \{1, 2, \dots, n\}$  satisfazem uma propriedade  $\mathcal{P}$  dada?
- ③ **Problemas Probabilísticos.** Dada uma propriedade  $\mathcal{P}$ , qual a probabilidade de um número  $n \in \mathbb{N}$  escolhido aleatoriamente possuir essa propriedade?

# Comportamento Assintótico

Dadas duas funções  $f, g: \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$ , denotamos por

①  $g(n) = O(f(n))$ , se existe  $C$  tal que  $\forall n \in \mathbb{N}, g(n) \leq Cf(n)$ .

②  $g(n) = \Omega(f(n))$ , se existe  $C$  tal que  $\forall n \in \mathbb{N}, g(n) \geq Cf(n)$ .

③  $g(n) = o(f(n))$ , se

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = 0.$$

④  $g(n) \sim f(n)$ , se

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = 1.$$

# Teorema dos Números Primos

Seja  $\pi(n) := \#$  de primos  $p \leq n$  (função de contagem de primos). Então é verdadeiro o seguinte resultado.

Teorema (Teorema dos Números Primos)

$$\pi(n) \sim \frac{n}{\log n}$$

# Probabilidade

Definimos um espaço de probabilidade por uma tripla:

- 1 Um conjunto  $\Omega$  (que será finito) chamado *espaço amostral*;



# Probabilidade

Definimos um espaço de probabilidade por uma tripla:

- 1 Um conjunto  $\Omega$  (que será finito) chamado *espaço amostral*;
- 2 Uma coleção  $E$  de subconjuntos de  $\Omega$  cujos elementos chamaremos de *eventos*;

# Probabilidade

Definimos um espaço de probabilidade por uma tripla:

- 1 Um conjunto  $\Omega$  (que será finito) chamado *espaço amostral*;
- 2 Uma coleção  $E$  de subconjuntos de  $\Omega$  cujos elementos chamaremos de *eventos*;
- 3 Uma função *probabilidade*  $\mathbb{P}: E \rightarrow [0, 1]$  que associa a cada conjunto a chance de ele ocorrer.

# Probabilidade

Definimos um espaço de probabilidade por uma tripla:

- 1 Um conjunto  $\Omega$  (que será finito) chamado *espaço amostral*;
- 2 Uma coleção  $E$  de subconjuntos de  $\Omega$  cujos elementos chamaremos de *eventos*;
- 3 Uma função *probabilidade*  $\mathbb{P}: E \rightarrow [0, 1]$  que associa a cada conjunto a chance de ele ocorrer.

Em geral, tomaremos a distribuição uniforme

$$\mathbb{P}[S] = \frac{|S|}{|\Omega|}.$$

# Probabilidade

Uma *variável aleatória* é uma função  $X: \Omega \rightarrow \mathbb{R}$ . Em particular, a função indicadora

$$\begin{aligned}\mathbb{1}_S : \Omega &\rightarrow \mathbb{R} \\ \mathbb{1}_S(x) &= \begin{cases} 1, & \text{se } x \in S \\ 0, & \text{caso contrário} \end{cases}\end{aligned}$$

é uma variável aleatória. Dado  $F \subset \mathbb{R}$ , definimos

$$\mathbb{P}[X \in F] = \mathbb{P}[\{\omega \in \Omega \mid X(\omega) \in F\}].$$

# Probabilidade

Definimos a *expectativa* ou *valor esperado* de uma variável aleatória  $X$  como a média de  $X$  sobre todos os elementos de  $\Omega$ . Visto matematicamente, temos a fórmula

$$\mathbb{E}[X] = \sum_x x\mathbb{P}[X = x].$$

Em particular,

$$\mathbb{E}[\mathbf{1}_S] = \mathbb{P}[\mathbf{1}_S = 1] = \frac{|S|}{|\Omega|}.$$

Propriedade importante: *A expectativa é linear*

$$\mathbb{E}[c_1X_1 + \cdots + c_nX_n] = c_1\mathbb{E}[X_1] + \cdots + c_n\mathbb{E}[X_n].$$

# Densidade Assintótica

Dado  $A \subset \mathbb{N}$ , definimos sua densidade superior e inferior, respectivamente, por

$$\bar{\sigma}(A) := \limsup_{N \rightarrow \infty} \frac{|A \cap [0, N)|}{N}$$

e

$$\underline{\sigma}(A) := \liminf_{N \rightarrow \infty} \frac{|A \cap [0, N)|}{N}.$$

Se  $\bar{\sigma}(A) = \underline{\sigma}(A)$ , chamamos o limite existente de *Densidade Assintótica* e denotamos por  $\sigma(A)$ .

# Infinitude dos Primos

## Teorema

*Existem infinitos primos.*

## Demonstração de Erdős.

Suponha que haja uma quantidade finita de primos  $p_1, p_2, \dots, p_k$ . Dado  $N \in \mathbb{N}$ , escreva todo  $n \leq N$  na forma  $n = a^2 b$ . Então  $1 \leq a \leq \sqrt{N}$ . Além disso,  $b$  é da forma  $b = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$ , onde  $\varepsilon_i \in \{0, 1\}$ . Então, embora haja  $N$  número entre 1 e  $N$ , há no máximo  $\sqrt{N} \cdot 2^k$  fatorações possíveis de números nesse intervalo, o que é falso para  $N$  suficientemente grande.  $\square$

# Infinitude dos Primos

## Teorema

*Existem infinitos primos.*

## Demonstração de Chernoff.

Iremos contar pontos em um reticulado. Note que se todos os primos são  $p_1, p_2, \dots, p_k$ , então todo número  $n$  pode ser escrito da forma  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Vamos contar quantas fatorações primas temos de 1 a  $N$ . Como  $2^{\alpha_i} \leq p_i^{\alpha_i} \leq N$ , temos  $\left\lfloor \frac{\log N}{\log 2} \right\rfloor + 1$  opções para  $\alpha_i$ . Portanto teríamos que

$$N \leq \left( \left\lfloor \frac{\log N}{\log 2} \right\rfloor + 1 \right)^k,$$

o que é falso para  $N$  grande. □



# Produto de Euler

## Teorema (Produto de Euler)

Se  $s > 1$ , então

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

# Produto de Euler

## Teorema (Produto de Euler)

Se  $s > 1$ , então

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

## Demonstração.

Escolha aleatoriamente um número  $n \in \mathbb{N}$  com probabilidade  $\frac{1/n^s}{\zeta(s)}$ . Então, dado  $p$  primo,  $\mathbb{P}[p \mid n] = \frac{1}{p^s}$ . Assim

$$\zeta(s)^{-1} = \mathbb{P}[1 \text{ foi escolhido}] = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right).$$



# Exemplos de Problemas Extremais

Qual o maior tamanho de um subconjunto  $A \subset \{1, 2, \dots, 2n\}$  tal que:

- ①  $\forall a, b \in A$  tais que  $\text{mdc}(a, b) = 1$ .
- ②  $\nexists a, b \in A$  tais que  $\text{mdc}(a, b) = 1$ .
- ③  $\nexists a, b \in A$  tais que  $a \neq b$  &  $a \mid b$ .
- ④  $\nexists a, b, c \in A$  tais que  $a + b = c$  ( $A$  é chamado livre de somas).

# Números Livres de Quadrados

Um  $n \in \mathbb{N}$  é dito número livre de quadrados se

$$\forall a \in \mathbb{N} \quad a^2 \nmid n,$$

isto é, se ele é o produto de primos distintos.

Pergunta: *Escolhido um número  $n \in \mathbb{N}$  aleatoriamente, qual a probabilidade de ele ser livre de quadrados?*

“Demonstração”.

Dado  $p$  primo, um número  $n \in \mathbb{N}$  escolhido aleatoriamente tem probabilidade  $\frac{1}{p^2}$  de ser múltiplo de  $p^2$ . Assim, a probabilidade de ele não ser múltiplo de nenhum primo ao quadrado é

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}.$$



# Números Coprimos

## Teorema

*A probabilidade de dois números naturais escolhidos aleatoriamente serem coprimos é  $\frac{6}{\pi^2}$ . Mais geralmente, a probabilidade de  $k$  números  $a_1, \dots, a_k \in \mathbb{N}$  serem coprimos é  $\frac{1}{\zeta(k)}$ .*

## “Demonstração”.

A probabilidade de que um primo  $p$  divida todos os  $k$  números é  $\frac{1}{p^k}$ , então a probabilidade de que ele não divida pelo menos um deles é  $1 - \frac{1}{p^k}$ . Tomando o produto sobre todos os primos e usando o produto de Euler, temos o resultado.



# Números Coprimos

Uma outra pergunta que Cameron e Erdős se interessaram foi a quantidade de subconjuntos  $A \subset \{1, 2, \dots, n\}$  tais que  $\forall a, b \in A, \text{mdc}(a, b) = 1$ .

# Números Coprimos

Uma outra pergunta que Cameron e Erdős se interessaram foi a quantidade de subconjuntos  $A \subset \{1, 2, \dots, n\}$  tais que  $\forall a, b \in A, \text{mdc}(a, b) = 1$ .

## Teorema (Cameron-Erdős, 1990)

Se  $f(n)$  é o número de conjuntos  $A \subset \{1, 2, \dots, n\}$  tais que  $\text{mdc}(a, b) = 1 \forall a \neq b \in A$ , então

$$e^{(\frac{1}{2}+o(1))\sqrt{n}}2^{\pi(n)} \leq f(n) \leq e^{(2+o(1))\sqrt{n}}2^{\pi(n)}.$$

# Números Coprimos

Posteriormente, N. Calkin e A. Granville demonstraram um resultado mais forte.

## Teorema (Calkin-Granville, 1996)

Se  $f(n)$  é o número de conjuntos  $A \subset \{1, 2, \dots, n\}$  tais que  $\text{mdc}(a, b) = 1 \ \forall a \neq b \in A$ , então

$$f(n) = 2^{\pi(n)} e^{\sqrt{n}(1+O(\log \log n / \log n))}.$$



# Conjuntos Livres de Coprimos

Outro problema estudado por Cameron e Erdős foi a quantidade de subconjuntos de  $\{1, 2, \dots, n\}$  livre de coprimos.

Teorema (Cameron-Erdős, 1990)

Se  $g(n)$  é o número de subconjuntos de  $\{1, 2, \dots, n\}$  livres de coprimos.

$$2^{\lfloor n/2 \rfloor} \leq g(n) \leq n2^{\lfloor n/2 \rfloor}.$$

# Números Coprimos

No mesmo artigo, N. Calkin e A. Granville também melhoraram essa cota.

## Teorema (Calkin-Granville, 1996)

A quantidade de conjuntos  $A \subset \{1, 2, \dots, n\}$  tais que  $\text{mdc}(a, b) = 1 \ \forall a \neq b \in A$  é

$$2^{\lfloor n/2 \rfloor} + 2^{\lfloor n/2 \rfloor - K} + O\left(2^{\lfloor n/2 \rfloor - K} \exp\left(-C \frac{n}{(\log n)^2 \log \log n}\right)\right)$$

para alguma constante  $C > 0$ , onde  $K$  satisfaz

$$K = (e^{-\gamma} + o(1)) \frac{n}{\log \log n}$$

# Função $\varphi$ de Euler

## Teorema

Se  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ , então

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

## Demonstração.

A probabilidade de que um número entre 1 e  $n$  seja coprimo com  $n$  é, por definição,  $\frac{\varphi(n)}{n}$ . Por outro lado, a probabilidade de que um número escolhido aleatoriamente seja múltiplo de  $p_i$  é  $\frac{1}{p_i}$ . Assim probabilidade de que ele seja coprimo com  $n$  também pode ser calculada por

$$\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right),$$

de onde segue o teorema. □

# Função $\varphi$ de Euler

Um outro resultado interessante a respeito da função  $\varphi$  é o seguinte.

$$\sum_{d|n} \varphi(d) = n.$$

Uma demonstração de tal resultado consiste em contar as frações  $\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, 1\}$ . Obviamente, temos  $n$  frações dessa forma, mas quantas frações reduzidas temos?

A fração  $k/n$  será reduzida da forma  $k'/d$  se, e somente se,  $\text{mdc}(k, n) = d$ . Ou seja, se e somente se  $\text{mdc}(k, n/d) = 1$ . Logo isso ocorre  $n/d$  vezes para cada divisor. Somando sobre todos os divisores, temos o resultado.

# Pequeno Teorema de Fermat

## Teorema

Se  $p$  é um primo, então

$$p \mid a^p - a.$$

## Demonstração.

Desejamos contar de quantas formas é possível colorir um colar de  $p$  pérolas com  $a$  cores de modo que haja pelo menos 2 cores. Temos  $a^p - a$  colares com pelo menos 2 cores, mas cada uma delas é gerada  $p$  vezes (cada rotação), portanto

$$\frac{a^p - a}{p}$$

é um inteiro. □

# Um Exemplo Olímpico

(IMO 1968) Para todo  $n$  natural, calcule a soma

$$\sum_{k=0}^{\infty} \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor = \left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \cdots + \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor + \cdots$$

# Solução

Vamos contar quantos números  $\leq n$  existem da forma  $r = 2^k(2m - 1)$ .

$$2^k \leq 2^k(2m - 1) \leq n$$

$$1 \leq 2m - 1 \leq \frac{n}{2^k}$$

$$2 \leq 2m \leq \frac{n + 2^k}{2^k}$$

$$1 \leq m \leq \left\lfloor \frac{n + 2^k}{2^{k+1}} \right\rfloor$$

Assim, como todo número pode ser escrito dessa forma ao variarmos o  $k$ , a soma vale  $n$ .

# Problemas com Divisibilidade

Iremos estudar conjuntos  $A \subset \{1, 2, \dots, n\}$  tais que

$$\forall a, b \in A, a \neq b \implies a \nmid b.$$

Seja  $f(n)$  a quantidade de conjuntos dessa forma. Então  $2^{n/2} \leq f(n)$ .

Cameron e Erdős conjecturaram em 1990 que existe  $c$  tal que  $f(n) = (c + o(1))^n$ , ou seja,  $\lim_n f(n)^{1/n} = c$ , e encontraram as seguintes cotas.

**Teorema (Cameron-Erdős, 1990)**

*Para  $n$  suficientemente grande,*

$$c_1^n \leq f(n) \leq c_2^n$$

*para  $c_1 = 1.55967\dots$  e  $c_2 = 1.59\dots$*



# Problemas com Divisibilidade

Esse problema foi resolvido em 2018 pelo brasileiro Rodrigo Angelo.

Teorema (Angelo, 2018)

*Seja  $f(n)$  definido como anteriormente. Então o limite*

$$\lim_{n \rightarrow \infty} f(n)^{1/n}$$

*existe.*

Infelizmente, sua demonstração não dá indícios de qual o valor desse limite.

# Conjuntos Livres de Somas

## Teorema (Erdős, 1965)

Seja  $A \subset \mathbb{Z}$  finito com elementos não nulos. Então existe um  $B \subset A$  livre de somas e satisfazendo  $|B| > |A|/3$ .

## Demonstração.

Considere  $A$  imerso em algum  $\mathbb{Z}_p$  com  $p$  grande, e  $p = 3k + 2$ . Note que o conjunto  $S = \{k + 1, \dots, 2k + 1\}$  é um conjunto livre de somas e tal que  $|S|/|\mathbb{Z}_p^\times| = \frac{k+1}{3k+1} > \frac{1}{3}$ . Considere a variável aleatória

$X(x) = \#$  de números da forma  $xa$  em  $S$ ,  $a \in A$ .

Então

$$\mathbb{E}[X] = |A|\mathbb{P}[y \in S] > \frac{|A|}{3}$$



# Conjuntos Livres de Somas

Seja  $f(n)$  = tamanho do maior conjunto  $B \subset \{1, 2, \dots, n\}$  livre de somas.

Teorema (Erdős, 1965)

$$\frac{n}{3} \leq f(n) \leq \frac{3}{7}n$$

Teorema (Alon-Kleitman, 1990)

$$\frac{n+1}{3} \leq f(n) \leq \frac{12}{29}n$$

Teorema (Bourgain, 1997)

$$\frac{n+2}{3} \leq f(n)$$

# Conjuntos Livres de Somas

Seja  $f(n)$  = tamanho do maior conjunto  $B \subset \{1, 2, \dots, n\}$  livre de somas.

Teorema (Erdős, 1965)

$$\frac{n}{3} \leq f(n) \leq \frac{3}{7}n$$

Teorema (Alon-Kleitman, 1990)

$$\frac{n+1}{3} \leq f(n) \leq \frac{12}{29}n$$

Teorema (Bourgain, 1997)

$$\frac{n+2}{3} \leq f(n)$$

**Problema.** É possível substituir  $\frac{n}{3}$  por  $\frac{n}{3} + 10$ ?

# Conjuntos Livres de Somas

Um desenvolvimento recente da teoria foi feito por Eberhard, Green e Manners.

Teorema (Eberhard-Green-Manners, 2014)

$$f(n) \leq \left( \frac{1}{3} + o(1) \right) n$$

Mostrando que a constante  $\frac{1}{3}$  é ótima.

# Conjectura de Cameron-Erdős

**Quantos conjuntos livre de somas há?**

Teorema (Erdős-Granville-Calkin-Alon, 1990)

*A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  é  $2^{(\frac{1}{2} + o(1))n}$ .*

# Conjectura de Cameron-Erdős

## Quantos conjuntos livre de somas há?

Teorema (Erdős-Granville-Calkin-Alon, 1990)

A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  é  $2^{(\frac{1}{2}+o(1))n}$ .

Teorema (Green-Sapozhenko, 2003)

A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  é  $O(2^{n/2})$ .

# Conjectura de Cameron-Erdős

## Quantos conjuntos livre de somas há?

Teorema (Erdős-Granville-Calkin-Alon, 1990)

A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  é  $2^{(\frac{1}{2}+o(1))n}$ .

Teorema (Green-Sapozhenko, 2003)

A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  é  $O(2^{n/2})$ .

Uma generalização desse resultado foi recentemente demonstrada.

Teorema (Alon-Balogh-Morris-Samotij, 2012)

A quantidade de conjuntos livre de somas  $A \subset \{1, 2, \dots, n\}$  de tamanho  $m$  é  $2^{O(n/m)} \binom{\lfloor n/2 \rfloor}{m}$  e esse resultado é preciso salvo pela constante implícita no  $O(\cdot)$ .



# Conjuntos Livres de Somas Maximais

Uma outra conjectura de Cameron e Erdős é se a quantidade de conjuntos livres de soma maximais é bem menor que a quantidade de conjuntos livres de soma. Eles deram a cota inferior  $2^{\lfloor n/4 \rfloor}$ .

O seguinte resultado resolve o problema.

**Teorema (Balogh-Liu-Sharifzadeh-Treglown, 2015)**

*Para  $1 \leq i \leq 4$ , existem  $C_i$  tais que se  $n \equiv i \pmod{4}$ , então  $\{1, 2, \dots, n\}$  contém  $(C_i + o(1))2^{\lfloor n/4 \rfloor}$  conjuntos livres de somas maximais.*

# Somas Distintas

Um conjunto de inteiros positivos  $A = \{a_1, a_2, \dots, a_k\}$  é dito ter somas distintas se as  $2^k - 1$  somas dos elementos de subconjuntos de  $A$  são distintas dois a dois.

Seja  $f(n)$  o maior  $k$  para o qual existe um conjunto

$$\{a_1, \dots, a_k\} \subset \{1, 2, \dots, n\}$$

com somas distintas.

O exemplo mais simples de um conjunto livre de somas é

$$\{2^i : 0 \leq i \leq \lfloor \log_2 n \rfloor\}.$$

Portanto

$$f(n) \geq 1 + \lfloor \log_2 n \rfloor.$$

# Somas Distintas

Para encontrar uma cota superior, uma contagem simples dá conta. Como as  $2^k - 1$  somas são distintas e inferiores a  $kn$ , sabemos que  $2^k \leq kn$ , de onde segue que  $f(n) \leq \log_2 n + \log_2 \log_2 n + O(1)$ .

# Somas Distintas

Erdős ofereceu \$300 para quem conseguisse provar ou desprovar

$$f(n) \leq \lfloor \log_2 n \rfloor + C.$$

# Somas Distintas

Outro problema que Cameron e Erdős resolveram, foi calcular a quantidade de conjuntos em  $\{1, 2, \dots, n\}$  com somas distintas.

Como vimos, o tamanho máximo de um conjunto dessa forma é  $(1 + o(1)) \log_2 n$ , portanto temos a cota superior

$$f(n) \leq n^{(1+o(1)) \log n / \log 2}.$$

# Somas Distintas

Além disso, se escolhermos os números em ordem, para garantir que possamos adicionar  $a_{i+1}$ , basta que ele seja diferente de todas as somas da forma  $\sum_{j < i} \delta_j a_j$  ( $\delta_j \in \{-1, 0, 1\}$ ).

Então temos no máximo  $\frac{3^i - 1}{2}$  números proibidos, assim, enquanto  $n > \frac{3^i - 1}{2}$ , podemos adicionar um número a sequência, de modo que podemos fazer pelo menos  $\lfloor \log_3 n \rfloor$  escolhas e obtemos pelo menos  $n^{(1+o(1)) \log n / \log 3}$  sequências.

# Funções Aritméticas

Algumas definições de funções aritméticas que serão usadas posteriormente.

Se  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ , então

$$d(n) := \# \text{ de divisores de } n$$

$$\omega(n) := r$$

$$\Omega(n) := \alpha_1 + \cdots + \alpha_r$$

# Alguns Resultados Assintóticos

## Série Harmônica

$$\sum_{k=1}^n \frac{1}{k} = \log n + \gamma + O\left(\frac{1}{n}\right)$$

## Teoremas de Mertens

$$\sum_p \frac{\log p}{p} = \log n + O(1)$$

$$\sum_p \frac{1}{p} = \log \log n + M + O\left(\frac{1}{\log n}\right)$$

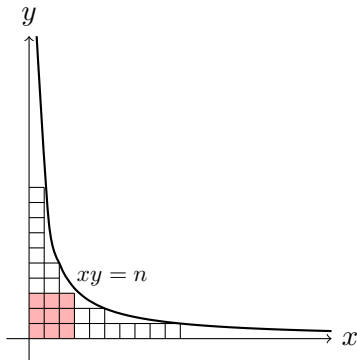
$$\lim_{n \rightarrow \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma}$$



# A Ordem Média de $d(n)$

## Teorema

$$\sum_{k=1}^n d(k) = n \log n + (2\gamma - 1)n + O\left(\frac{1}{\sqrt{n}}\right)$$



# A Ordem Normal de $\omega(n)$ e de $\Omega(n)$

Teorema (Hardy-Ramanujan, 1917; Turán, 1934)

A ordem normal de  $\omega(n)$  e de  $\Omega(n)$  é  $\log \log n$ . Isto é,  $\forall \varepsilon > 0$ ,

$$|\{n \leq N \mid |\omega(n) - \log \log n| > (\log \log n)^{\frac{1}{2} + \varepsilon}\}| = o(n)$$

e o mesmo é válido para  $\Omega(n)$ .

Demonstração.

Mostraremos que a soma

$$\sum_{n \leq N} |\omega(n) - \log \log n|^2 = O(N \log \log N).$$

Assim, se ocorresse de a quantidade do problema não ser  $o(n)$ , isto é, ser  $\Omega(n)$ , então essa soma seria  $\Omega(N(\log \log N)^{1+2\varepsilon})$ . Absurdo.



# A Ordem Normal de $\log d(n)$

Note que  $\forall n \in \mathbb{N}$ ,

$$2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)}.$$

Portanto a ordem normal de  $\log d(n)$  é  $\log 2 \log \log n$ .

Note que, nesse caso, a ordem normal é diferente da ordem média, pois a série é dominada por alguns poucos termos grandes.

# Aplicação Interessante

Defina  $f(n)$  a quantidade de elementos de 1 a  $n^2$  que podem ser escritos como produto de dois números de 1 a  $n$ , isto é,

$$f(n) := |\{1 \leq z \leq n^2 : \exists a, b \leq n, z = ab\}|.$$

Então

$$\lim_{n \rightarrow \infty} \frac{f(n)}{n^2} = 0$$

# O Teorema de Erdős-Kac

No Teorema de Hardy-Ramanujan, dissemos que a quantidade de ponto para os quais  $\omega(n)$  está longe de  $\log \log n$  a uma medida maior que  $\sqrt{\log \log n}$  tende a 0. Desejamos saber como essa diferença se comporta quando estes números estão próximos.

A resposta é que se comportam como a Distribuição Gaussiana.

## Teorema (Erdős-Kac, 1940)

*Dados  $a < b$  reais, seja*

$$\Phi(a, b) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

*Então,*

$$\lim_{N \rightarrow +\infty} \frac{1}{N} \left| n \leq N : a \leq \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq b \right| = \Phi(a, b).$$

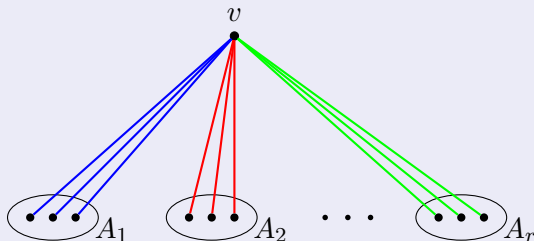
# Teorema de Ramsey Infinito

## Teorema (Teorema de Ramsey)

Dado  $r \in \mathbb{N}$ . Para toda coloração  $c: \binom{\mathbb{N}}{2} \rightarrow \{1, 2, \dots, r\}$ , existe um subconjunto infinito  $S \subset \mathbb{N}$  monocromático.

## Demonstração.

Escolha um ponto qualquer, escolha a vizinhança monocromática dele infinita e continue esse processo.



# Um resultado interessante

## Teorema

*Existe um subconjunto infinito  $S \subset \mathbb{N}$  tal que a soma de quaisquer dois elementos de  $S$  possui uma quantidade par de divisores primos distintos.*

# Propriedade Multiplicativa

Se chamarmos  $f(n)$  a quantidade de conjuntos

$A = \{a_1, \dots, a_t\} \subset \{1, 2, \dots, n\}$  tais que nenhum termo divide o produto dos outros, trivialmente temos a vota inferior  $2^{\pi(n)}$ , mas podemos melhorá-la para.

**Teorema (Cameron-Erdős, 1990)**

*Se  $f(n)$  é definido como acima,*

$$2^{(c+o(1))\pi(n)} \leq f(n)$$

*onde*

$$c = \frac{1}{\log 2} \sum_{r \geq 1} \frac{\log(r+1)}{r(r+1)} \approx 1.1814...$$



# Demonstração

Para cada  $\sqrt{n} \leq p \leq n$ , podemos adicionar no máximo um  $pt$  para  $0 \leq t \leq n/p$ . Assim, temos pelo menos

$$\prod_{r \leq \sqrt{n}} (r + 1)^{\pi(n/r) - \pi(n/(r+1))}.$$

Usando o Teorema dos Números primos, o resultado segue.

# Conjuntos Sidon Multiplicativos

Um conjunto  $A = \{a_1, a_2, \dots, a_m\} \subset \mathbb{N}$  é dito Sidon se

$$a_i + a_j = a_k + a_l \implies \{i, j\} = \{k, l\}$$

e chamado Sidon multiplicativo se

$$a_i a_j = a_k a_l \implies \{i, j\} = \{k, l\}.$$

# Conjuntos Sidon Multiplicativos

Um conjunto  $A = \{a_1, a_2, \dots, a_m\} \subset \mathbb{N}$  é dito Sidon se  
 $a_i + a_j = a_k + a_l \implies \{i, j\} = \{k, l\}$  e chamado Sidon multiplicativo se  
 $a_i a_j = a_k a_l \implies \{i, j\} = \{k, l\}$ .

## Teorema (Erdős, 1938)

*Um conjunto Sidon multiplicativo  $A \subset \{1, 2, \dots, n\}$  tem tamanho no máximo  $\pi(n) + 2n^{2/3}$ .*

# Conjuntos Sidon Multiplicativos

## Teorema (Cameron-Erdős, 1990)

Se  $f(n)$  é a quantidade de conjuntos Sidon multiplicativos em  $\{1, 2, \dots, n\}$ , então

$$2^{(c+o(1))\pi(n)} \leq f(n)$$

onde

$$c = \frac{1}{\log 2} \sum_{r \geq 1} \frac{\log(r+1)}{r(r+1)} \approx 1.1814...$$

# Teorema de Schur

Enquanto estudava o Último Teorema de Fermat, Schur demonstrou o seguinte resultado.

## Teorema (Schur, 1916)

*Para qualquer  $r$ -coloração dos números naturais, existem  $x, y, z$  monocromáticos tais que  $x + y = z$ .*

Que tem como corolário o seguinte teorema.

## Teorema (Schur, 1916)

*Para todo  $n \in \mathbb{N}$ , a equação*

$$x^n + y^n \equiv z^n \pmod{p}$$

*tem solução não trivial para todo  $p$  primo suficientemente grande.*

# Uma Resultado Recente

Uma generalização do Teorema de Schur é tentar tomar combinações não lineares de  $x$  e  $y$ . Um problema em aberto recentemente solucionado é que é possível sempre encontrar um par  $\{x + y, xy\}$  monocromático. Na verdade, temos um resultado mais forte.

# Uma Resultado Recente

Uma generalização do Teorema de Schur é tentar tomar combinações não lineares de  $x$  e  $y$ . Um problema em aberto recentemente solucionado é que é possível sempre encontrar um par  $\{x + y, xy\}$  monocromático. Na verdade, temos um resultado mais forte.

**Teorema (J. Moreira, 2016)**

*Se  $\mathbb{N}$  é  $r$ -colorido, então existem infinitos  $x, y$  tais que  $\{x, x + y, xy\}$  é monocromático.*

# Teorema de Van der Waerden

## Teorema (Van der Waerden, 1927)

*Toda coloração dos números inteiros possui progressões aritméticas monocromáticas de tamanho arbitrário.*



# Densidade de um Conjunto

Erdős e Turán em 1938 conjecturaram que o Teorema de Schur era consequência de um resultado mais profundo. Uma das partições deve ser grande, e esse resultado só seria suficiente para demonstrar o resultado. Considere a seguinte definição.

Dado  $A \subset \mathbb{N}$ , definimos sua densidade superior por

$$\bar{\sigma}(A) := \limsup_{N \rightarrow \infty} \frac{|A \cap [0, N)|}{N}$$

# Teorema de Szemerédi

## Teorema (Roth, 1953)

*Seja  $A \subset \mathbb{N}$ . Se  $\bar{\sigma}(A) > 0$ , então existem progressões aritméticas de tamanho arbitrário em  $A$ .*

# Teorema de Szemerédi

## Teorema (Roth, 1953)

*Seja  $A \subset \mathbb{N}$ . Se  $\bar{\sigma}(A) > 0$ , então existem progressões aritméticas de tamanho arbitrário em  $A$ .*

## Teorema (Szemerédi, 1969-1975)

*Seja  $A \subset \mathbb{N}$ . Se  $\bar{\sigma}(A) > 0$ , então existem progressões aritméticas de tamanho arbitrário em  $A$ .*

# Teorema de Szemerédi

## Teorema (Roth, 1953)

*Seja  $A \subset \mathbb{N}$ . Se  $\bar{\sigma}(A) > 0$ , então existem progressões aritméticas de tamanho arbitrário em  $A$ .*

## Teorema (Szemerédi, 1969-1975)

*Seja  $A \subset \mathbb{N}$ . Se  $\bar{\sigma}(A) > 0$ , então existem progressões aritméticas de tamanho arbitrário em  $A$ .*

Posteriormente, H. Furstenberg (1982) demonstrou utilizando Teoria Ergódica e T. Gowers (2001) demonstrou usando Análise Harmônica.

# Conjectura de Erdős

## Teorema

*Para todo  $A \subset \mathbb{N}$  com densidade superior positiva, existem subconjuntos infinitos  $B, C \subset \mathbb{N}$  tais que  $B + C \subset A$ .*





# Conjectura de Erdős

## Teorema

*Para todo  $A \subset \mathbb{N}$  com densidade superior positiva, existem subconjuntos infinitos  $B, C \subset \mathbb{N}$  tais que  $B + C \subset A$ .*

Demonstrado por *Joel Moreira, Florian Karl Richter, Donald Robertson* em 2018.

# Bibliografia

-  G. H. Hardy, E. M. Wright; An Introduction to the Theory of Numbers, 6th Edition, OUP, 2008.
-  N. Alon, J. Spencer; The Probabilistic Method, 4th Edition, Wiley, 2015.
-  T. Tao, V. Vu; Additive Combinatorics, CUP, 2006.
-  R. Morris; Extremal and Probabilistic Combinatorics, [http://w3.impa.br/~rob/Extremal\\_and\\_probabilistic\\_combinatorics.pdf](http://w3.impa.br/~rob/Extremal_and_probabilistic_combinatorics.pdf), 2012.