Universidade Federal de Ouro Preto

Instituto de Ciências Exatas e Biológicas

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Dissertação

O crivo de Brun para primos gêmeos

Giovanne Drumond Costa

Ouro Preto
2021

UFOP

2021
Giovanne Drumond Costa
DEMAT/UFOP

UNIVERSIDADE FEDERAL DE OURO PRETO

INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS

DEPARTAMENTO DE MATEMÁTICA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Giovanne Drumond Costa

ORIENTADOR:
SÁVIO RIBAS

O CRIVO DE BRUN PARA PRIMOS GÊMEOS

OURO PRETO - MG

FEVEREIRO - 2021

UNIVERSIDADE FEDERAL DE OURO PRETO

INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS

DEPARTAMENTO DE MATEMÁTICA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Giovanne Drumond Costa

O CRIVO DE BRUN PARA PRIMOS GÊMEOS

Dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas e Biológicas da Universidade Federal de Ouro Preto, programa PROFMAT.

Orientador: Sávio Ribas

OURO PRETO - MG

FEVEREIRO - 2021

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

C837c Costa, Giovanne Drumond .
O Crivo de Brun para primos gêmeos . [manuscrito] / Giovanne Drumond Costa. - 2021.
29 f.: il.: , gráf., tab..

Orientador: Prof. Dr. Sávio Ribas.
Dissertação (Mestrado Profissional). Universidade Federal de Ouro Preto. Departamento de Matemática. Programa de Pós-Graduação em Matemática.
Área de Concentração: Matemática com Oferta Nacional.

1. Números primos. 2. Brun, Teorema de . 3. Teoria dos números . I. Ribas, Sávio. II. Universidade Federal de Ouro Preto. III. Título.

CDU 511

Bibliotecário(a) Responsável: Celina Brasil Luiz - CRB6-1589

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
PROGRAMA DE POS-GRADUACAO EM MATEMATICA EM REDE NACIONAL

FOLHA DE APROVAÇÃO

Giovanne Drumond Costa

O Crivo de Brun para Primos Gêmeos

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Mestre em Matemática

Aprovada em 19 de fevereiro de 2021.

Membros da banca

Prof. Dr. Savio Ribas - Orientador Universidade Federal de Ouro Preto
Prof. Dr. Bhavinkumar Kishor Sinh Moriya - Universidade Federal de Viçosa
Prof. Dr. Juliano Soares Amaral Dias - Universidade Federal de Ouro Preto

Prof. Dr. Savio Ribas, orientador do trabalho, aprovou a versão final e autorizou seu depósito no Repositório Institucional da UFOP em 29/03/2021.

Documento assinado eletronicamente por **Savio Ribas**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 29/03/2021, às 12:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0138690** e o código CRC **FB623846**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.001695/2021-77 SEI nº 0138690

Dedico esse trabalho a minha mãe Aparecida Das Graças Drumond, que sempre esteve ao meu lado, dando muito amor, força e motivação. Aos meus filhos João Vitor Paiva Costa e Maria Eduarda Paiva Costa, pois representam a minha melhor parte. Ao meu pai Geraldo Magela Costa, pois me ensina a cada dia a ser grato pela vida e a lutar contra as adversidades. Aos meus irmãos Genner Christhian Drumond Costa e Gabriela Drumond Costa que sempre me apoiam e torcem pelo meu sucesso.

Agradecimentos

Agradeço a Deus, pela minha vida, e por me ajudar a passar por todos obstáculos encontrados nessa caminhada. Aos meus familiares e amigos que me incentivaram em momentos difíceis a continuar seguindo em frente e por compreenderem minha ausência enquanto eu me dedicava à realização deste trabalho. Aos professores, que através dos ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional, em especial ao professor e orientador Savio Ribas, que com muita paciência e competência tanto me ajudou. Aos meus colegas de cursos que sempre foram parceiros e com muita união caminhamos juntos em especial a amiga de curso e companheira de viagem Elaine Veloso Fernandes Pereira. Aos funcionarios e alunos da Escola Estadual Antônio Silva em especial a Diretora Maria de Lurdes de Oliveira Andrade e a vice Raquel Fernanda Alves de Andrade por entenderem as dificuldades e estarem sempre dispostas a ajudar. Ao grupo de amigos inimigos do fim, que me deram suporte emocional, principalmente neste último ano tão difícil. Transformamos dor em alegria.

Resumo

Um número primo p é dito primo gêmeo se $p+2$ também é primo. Conjectura-se que existem infinitos primos gêmeos. O objetivo dessa dissertação é mostrar que a soma dos inversos dos primos gêmeos converge, enquanto a soma dos inversos de todos os primos diverge (também vamos provar isso usando a função zeta de Riemann). Tal fato pode implicar duas coisas: ou existem finitos primos gêmeos, ou os primos gêmeos são infinitos porém muito escassos na reta real. A técnica utilizada para demonstrar esse resultado é o crivo de Brun, que permite obter uma cota superior para o número de primos gêmeos até x. Para obter tais cotas, é necessário apresentar diversos resultados anteriores, como o princípio da inclusão-exclusão, as funções multiplicativas (em particular, a função de Möbius), as duas primeiras fórmulas de Mertens e o Teorema de Chebyshev. Vamos apresentar também uma caracterização dos primos gêmeos devida a Clement. A cota superior obtida implica diretamente o principal resultado dessa dissertação: a soma dos inversos dos primos gêmeos converge.

Abstract

A prime number p is said to be a twin prime if $p+2$ is also a prime. It's conjectured that there exist infinitely many twin primes. The goal of this master thesis is to show that the sum of the inverses of the twin primes converges, although the sum of the inverses of all the primes diverges (we will also prove the latter using the Riemann zeta function). Such fact can imply two things: either there are finitely many twin primes, or there are infinitely many, however sparse on the real line. The technique used to prove this result is the Brun's sieve, which allows us to obtain an upper bound for the number of twin primes up to x. In order to obtain such bounds, it's required to present several preliminary results, such as inclusion-exclusion principle, the multiplicative functions (in particular, the Möbius function), the first two Merten's formula and the Chebyshev Theorem. We will also present a characterization of twin primes due to Clement. The obtained upper bound directly implies the main result of this thesis: the sum of inverses of twin primes converges.

Sumário

Capítulo 1

Introdução

Por volta de 300 A.C., Euclides, de Alexandria, provou que existem infinitos primos. A demonstração dada por ele é a seguinte: Suponha que o conjunto de números primos é finito, digamos $\{p_1, p_2, p_3, \ldots, p_n\}$. Seja

$$N = p_1 \times p_2 \times \cdots \times p_n + 1.$$

Temos que $N > p_i$ para todo $1 \leq i \leq n$, logo N não pode ser primo. Por outro lado, se N é composto então, pelo Teorema Fundamental da Aritmética, existe um primo p_i que divide N. Como p_i divide N e divide $p_1 \times \cdots \times p_n$, p_i deve dividir a diferença $N - p_1 \times \cdots \times p_n = 1$, o que é um absurdo.

Existem diversas formas de buscar números primos. Por exemplo, na escola aprendemos sobre o Crivo de Eratóstenes (ver, por exemplo, [4, Capítulo 5], que explica o funcionamento desse crivo). De forma elementar, esse crivo consiste em montar uma tabela com os números naturais de 2 até um valor X, circular o número 2 e riscar todos os múltiplos de 2 maiores que 2. Após isso, circulamos o próximo número que ainda não foi riscado (no caso, o 3) e riscamos todos os seus múltiplos maiores que 3. Repetimos o mesmo argumento até que sobram alguns números circulados na tabela. Os números circulados são justamente os números primos. Além disso, vemos que basta testar os números até $\sqrt{X}$, pois se $n \leq X$ é composto então $n = ab$, onde $a \leq \sqrt{X}$ ou $b \leq \sqrt{X}$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Existem diversos outros crivos para buscar diversos números de determinadas formas, como por exemplo:

(i) crivo de Gallagher, que tem como aplicação, por exemplo, mostrar um análogo do Teorema Chinês dos Restos para sistemas de congruências com potências (ao invés de lineares);

(ii) crivo quadrado, utilizado para estimar o número de quadrados perfeitos em um dado conjunto de inteiros;

(iii) crivo usando séries de Dirichilet, utilizado quando temos uma sequência multiplicativa, que possui como aplicações, determinar o número de inteiros que podem ser escritos como soma de dois quadrados, como se comporta a corrida entre primos congruentes a 1 e a 3 módulo 4, entre outras;

(iv) crivo de Turán, utilizado como cota superior para variâncias de determinadas quantidades em diversos problemas da combinatória, como contar torneios em grafos que possuem certa quantidade de ciclos [7], contar coloração de vértices em grafos, contar grafos conexos, contar quadrados latinos, contar geradores de grupos [8], contar polinômios irredutíveis sobre os inteiros ou sobre corpos finitos, entre outros;

(v) crivo de Selberg, utilizado para demonstrar que exisem infinitos pares de primos com diferença muito menor que a média (ver os métodos GPY [5] e Maynard-Tao [9]);

(vi) grande crivo, utilizado para provar o Teorema de Bombieri-Vinogradov, que mostra que a Hipótese de Riemann Generalizada, um resultado sobre o erro na distribuição dos primos em progressão aritmética, vale na média (ver também o método de Zhang [10]).

A ideia geral de todos esses crivos pode ser consultada em [4]. Nessa dissertação, vamos apresentar o Crivo de Brun para os números primos gêmeos.

Definição 1.0.1 (Primos gêmeos)**.** *Dizemos que um número primo p é primo gêmeo se $p+2$ também é primo. Nesse caso, dizemos que o par $(p, p+2)$ é um par de primos gêmeos.*

Exemplo 1.0.2. *Os primeiros pares de primos gêmeos são:* $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, ... *Existem pares de primos gêmeos muito grandes, como* $2.996.863.034.895 \times 2^{1290000} \pm 1$, *que possuem* 388.342 *algarismo na base decimal (esse é o maior par de primos gêmeos conhecido até o momento e foi descoberto em 2016).*

Ao longo dessa dissertação, vamos usar algumas cotas sobre a distribuição dos primos além do resultado que já provamos, sobre a existência de infinitos primos. O segundo resultado, que não será provado por se tratar de uma demonstração longa, é o Teorema dos Números Primos. Mas antes precisamos da seguinte definição.

Definição 1.0.3. *Seja $x > 0$. Definimos $\pi(x) = \#\{p \leq x; p \text{ primo}\}$, isto é, $\pi(x)$ é a função que conta o número de primos menores ou iguais a x.*

Teorema 1.0.4 (dos Números Primos)**.** *É válido que* $\lim_{x\to\infty} \dfrac{\pi(x)}{x/\log x} = 1$.

No Capítulo 2 vamos provar o Teorema de Chebyshev, que é um resultado um pouco mais fraco que o Teorema dos Números Primos, porém fornece corretamente a ordem de crescimento dos números primos. A seguir, vamos demonstrar a existência de infinitos primos de outra forma: usando a Função Zeta de Riemann.

Definição 1.0.5. *Seja* $x > 1$*. A Função Zeta de Riemann é definida como* $\zeta(x) = \sum_{n\geq 1} \dfrac{1}{n^x}$.

Para $x > 1$, esse somatório é convergente e para $x \leq 1$ esse somatório é divergente. Em particular, a série harmônica diverge, isto é, $\lim_{x\to 1^+} \zeta(x) = \infty$. Isso implica que existem infinitos números primos, como veremos a seguir, sendo uma versão mais fraca do que o Teorema dos Números Primos e mais forte que o Teorema de Euclides. A partir de agora, a letra p denotará sempre um número primo.

Proposição 1.0.6 (Fórmula de Euler)**.** *Seja* $x > 1$*. Então vale*

$$\zeta(x) = \prod_{p} \left(1 - \frac{1}{p^x}\right)^{-1}.$$

Demonstração. Seja $\delta > 1$ fixo. Se $x \geq \delta$ então $\zeta(x)$ converge uniformemente. De fato,

$$\zeta(x) = \sum_{n\geq 1} \frac{1}{n^x} \leq \sum_{n\geq 1} \frac{1}{n^\delta},$$

que converge. Seja

$$P(t) = \prod_{p\leq t} \left(1 + \frac{1}{p^x} + \frac{1}{p^{2x}} + \dots\right) = \prod_{p\leq t} \left(1 - \frac{1}{p^x}\right)^{-1}.$$

Expandindo o produto, temos

$$P(t) = \sum_{n\in A_t} \frac{1}{n^x},$$

onde A_t é o conjunto dos números naturais que são escritos como produtos de primos menores ou iguais a t. Assim, temos

$$0 \leq \zeta(x) - P(t) = \sum_{n\notin A_t} \frac{1}{n^x} \leq \sum_{n>t} \frac{1}{n^x} \to 0$$

quando $t \to \infty$. Logo, se $x \geq \delta$ então temos a seguinte convergência uniforme:

$$\lim_{t\to\infty} P(t) = \zeta(x).$$

□

Teorema 1.0.7. $\sum_p \frac{1}{p}$ *diverge. Em particular existem infinitos números primos.*

Demonstração. Tomando logaritmos na fórmula de Euler, temos

$$\log \zeta(x) = -\sum_p \log(1 - 1/p^x)$$

Expandindo o último termo em série de potências, obtemos

$$\log \zeta(x) = \sum_p \sum_{n\geq 1} \frac{1}{np^{nx}} = \sum_p \frac{1}{p^x} + \sum_p \sum_{n\geq 2} \frac{1}{np^{nx}}.$$

Vamos mostrar que $\sum_p \sum_{n\geq 2} \frac{1}{np^{nx}}$ converge. Temos

$$\sum_p \sum_{n\geq 2} \frac{1}{np^{nx}} < \sum_p \sum_{n\geq 2} \frac{1}{p^n} = \sum_p \frac{1/p^2}{1 - 1/p} = \sum_p \frac{1}{p(p-1)} < \sum_n \frac{1}{n(n-1)} = 1.$$

Dessa forma, tomando $x \to 1^+$ teremos $\log \zeta(x) \to \infty$ e portanto $\sum_p \frac{1}{p}$ diverge.

□

O teorema anterior garante que a série dos inversos dos primos diverge. O objetivo dessa dissertação é mostrar que a soma dos inversos dos primos gêmeos converge, e isso pode implicar duas coisas: ou existem finitos pares de primos gêmeos, ou os primos gêmeos são infinitos, porém muito espaçados na reta real. A técnica utilizada para demonstrar esse resultado é o crivo de Brun, que será introduzido no Capítulo 3. No Capítulo 2, vamos apresentar o Princípio da Inclusão-Exclusão e algumas funções multiplicativas como a função de Möbius, além de determinar diversas fórmulas envolvendo primos, como as fórmulas de Mertens e o Teorema de Chebyshev. Vamos apresentar também uma caracterização dos primos gêmeos devida a Clement. No Capítulo 3, vamos descrever o crivo de Brun, que permite obter cotas superiores para o número de primos gêmeos até x, e com isso vamos obter o principal resultado dessa dissertação: a soma dos inversos dos primos gêmeos converge.

Capítulo 2

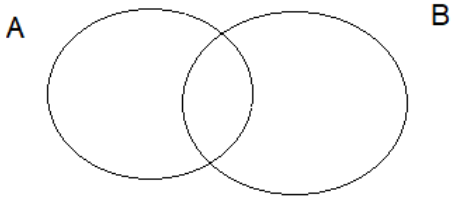
Preliminares

2.1 Princípio da Inclusão-Exclusão

Seja X um conjunto qualquer. Denotamos por $\#X$ ou $|X|$ o número de elementos de X. Observando o diagrama a seguir com os conjuntos A e B, podemos deduzir que

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{2.1}$$

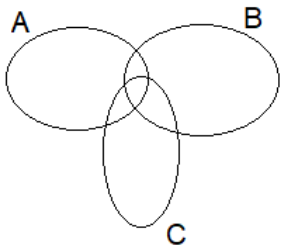
uma vez que a intersecção é contada duas vezes quando somamos $|A|$ com $|B|$. Portanto, deve ser descontada uma vez



Para três conjuntos A, B e C, temos um resultado análogo; a saber

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

uma vez que cada intersecção dois a dois entre os conjuntos é contada duas vezes na soma $|A| + |B| + |C|$ e a intersecção entre os três conjuntos é somada três vezes em $|A| + |B| + |C|$ e subtraída três vezes em $|A \cup B| + |A \cup C| + |B \cup C|$, sendo necessário somar uma vez mais.



No caso de mais conjuntos temos um resultado análogo, sempre removendo os termos contados a mais, e adicionando os termos contados a menos.

Proposição 2.1.1 (Princípio da Inclusão-Exclusão)**.** *Sejam $A_1, A_2, \ldots, A_n$ conjuntos, onde $n \geq 2$, é válido que*

$$\begin{aligned}|\bigcup_{i=1}^{n} A_i| &= \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j\leq n} |A_i \cap A_j \cap A_l| - \cdots + (-1)^{n+1}|A_1 \cap \cdots \cap A_n| \\ &= \sum_{i=1}^{n} (-1)^{i+1} \sum_{1\leq j_1<\cdots<j_i\leq n} |A_{j_1} \cap \cdots \cap A_{j_i}|.\end{aligned}$$

Demonstração. A demonstração é feita por indução em n. A base da indução ($n = 2$) já foi feita anteriormente na Equação (2.1). Suponha que a proposição é válida para todo k com $2 \leq k \leq n$. Vamos provar que também é válida para $n + 1$ termos:

$$\begin{aligned}&|A_1 \cup \cdots \cup A_n \cup A_{n+1}| = |(A_1 \cup \cdots \cup A_n) \cup A_{n+1}| \\ &= |(A_1 \cup \cdots \cup A_n)| + |A_{n+1}| - |(A_1 \cup \cdots \cup A_n) \cap A_{n+1}| \\ &= \left(\sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \ldots\right) + |A_{n+1}| - |\bigcup_{i=1}^{n}(A_i \cap A_{n+1})| \\ &= \sum_{i=1}^{n+1} |A_i| - \left(\sum_{i=1}^{n} |A_i \cap A_j| - \ldots\right) - \left(\sum_{i=1}^{n} |A_i \cap A_{n+1}| - \sum_{1\leq i<j\leq n} |A_i \cap A_j \cap A_{n+1}| + \ldots\right) \\ &= \sum_{i=1}^{n+1} |A_i| - \sum_{1\leq i<j\leq n+1} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n+1} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n+2}|A_i \cap \cdots \cap A_{n+1}|,\end{aligned}$$

o que prova a proposição. □

2.2 Funções multiplicativas e a função de Möbius

Definição 2.2.1. *Seja $f : \mathbb{N} \to \mathbb{R}$. Dizemos que f é multiplicativa se $f(mn) = f(m)f(n)$ para todo par de inteiros (m, n) tais que $mdc(m, n) = 1$. Além disso, dizemos que f é totalmente multiplicativa se $f(mn) = f(m)f(n)$ para todo par de inteiros (m, n).*

Teorema 2.2.2. *Seja f uma função multiplicativa. Então a função*

$$F(n) = \sum_{d|n} f(d)$$

também é multiplicativa.

Demonstração. Sejam a e b inteiros tais que $mdc(a, b) = 1$. Notemos que se $d \mid ab$ então

$d = d_1 d_2$, onde $d_1 \mid a$, $d_2 \mid b$ e $mdc(d_1, d_2) = 1$. Logo

$$F(ab) = \sum_{d|ab} f(d) = \sum_{\substack{d_1|a \\ d_2|b}} f(d_1 d_2) = \sum_{d_1|a} \sum_{d_2|b} f(d_1) f(d_2) = \sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2) = F(a)F(b).$$

Daí, segue que F é multiplicativa. □

Proposição 2.2.3. *Seja $f : \mathbb{N} \to \mathbb{R}$ multiplicativa e limitada e seja $x > 1$. Então vale*

$$\sum_{n\geq 1} \frac{f(n)}{n^x} = \prod_p \left(\sum_{k\geq 0} \frac{f(p^k)}{p^{kx}} \right).$$

Se, além disso, f é totalmente multiplicativa então

$$\sum_{n\geq 1} \frac{f(n)}{n^x} = \prod_p \left(1 - \frac{f(p)}{p^x} \right)^{-1}.$$

Demonstração. Sendo f limitada, a série

$$\sum_{n\geq 1} \frac{f(n)}{n^x}$$

converge uniformemente para $x \geq \delta$ para todo $\delta > 1$. De fato, seja $M > 0$ tal que $f(n) \leq M$ para todo $n \in \mathbb{N}$. Temos

$$\left| \sum_{n\geq 1} \frac{f(n)}{n^x} \right| \leq M \sum_{n\geq 1} \frac{1}{n^\delta} < \infty,$$

logo a série $\sum_{n\geq 1} \frac{f(n)}{n^x}$ converge uniformemente em $x \geq \delta > 1$. Sejam

$$S = \sum_{n\geq 1} \frac{f(n)}{n^x}$$

e

$$P(a) = \prod_{p\leq a} \left(1 + \frac{f(p)}{p^x} + \frac{f(p^2)}{p^{2x}} + \cdots \right).$$

Como $P(a)$ é o produto de séries absolutamente convergentes podemos reescrever $P(a) = \sum_{n\in N_a} \frac{f(n)}{n^x}$, onde N_a é o conjunto dos inteiros positivos cujos fatores primos são menores ou iguais a a. Sabendo que os inteiros entre 1 e a estão em N_a, temos

$$|S - P(a)| = \left| \sum_{n\in\mathbb{N}\setminus N_a} \frac{f(x)}{n^x} \right| \leq \sum_{n\in\mathbb{N}\setminus N_a} \frac{|f(x)|}{n^x} \leq M \sum_{n>a} \frac{1}{n^x} \to 0,$$

quando $a \to \infty$. Daí segue que $\lim_{a\to\infty} P(a) = S$. De fato, se $x \geq \delta > 1$, a convergência

uniforme de S implica que $P(a)$ converge uniformemente a S neste domínio. Logo vale que

$$\sum_{n\geq 1}\frac{f(n)}{n^x}=\prod_p\left(\sum_{k\geq 0}\frac{f(p^k)}{p^{kx}}\right).$$

Com f estritamente multiplicativa teremos $f(p^m)=(f(p))^m$, daí usando soma de progressão geométrica, obtemos

$$\sum_{m\geq 0}f(p^m)p^{-mx}=\sum_{m\geq 0}(f(p)p^{-x})^m=\frac{1}{1-f(p)p^{-x}},$$

logo vale

$$\sum_{n\geq 1}\frac{f(n)}{n^x}=\prod_p\left(1-\frac{f(p)}{p^x}\right)^{-1}.$$

□

Definição 2.2.4. *A função de Möbius $\mu:\mathbb{N}\to\mathbb{R}$ é definida como*

$$\mu(n)=\begin{cases}1 & \text{se } n=1,\\ (-1)^k & \text{se } n=p_1\dots p_k, \text{ onde os primos } p_i \text{ são distintos},\\ 0 & \text{se } p^2\mid n \text{ para algum } p \text{ primo.}\end{cases}$$

Proposição 2.2.5. *A função μ de Möbius é multiplicativa.*

Demonstração. Sejam a e b naturais primos entre si. Se p^2 divide a ou divide b para algum p primo, então $\mu(a)=0$ ou $\mu(b)=0$ e também p^2 divide ab, ou seja $\mu(a)\mu(b)=0=\mu(ab)$. Então vamos supor que $a=p_1\dots p_r$ e $b=q_1\dots q_s$ (onde $r=0$ se $a=1$ e $s=0$ se $b=1$), são livres de quadrados. Como a e b são primos entre si, os primos p_i são distintos dos primos q_j. Logo ab também é livre de quadrados, e vale $\mu(ab)=(-1)^{r+s}=(-1)^r\cdot(-1)^s=\mu(a)\mu(b)$. □

Lema 2.2.6. *Para todo inteiro positivo n, vale que*

$$\sum_{d\mid n}\mu(d)=\begin{cases}1 & \text{se } n=1,\\ 0 & \text{se } n>1.\end{cases}$$

Demonstração. O caso $n=1$ trivial. Vamos supor que $n>1$. Como a μ é multiplicativa, o Teorema 2.2.2 garante que $\sum_{d\mid n}\mu(d)$ também multiplicativa. Sendo assim, basta provar o lema para as potências de primos . De fato:

$$\sum_{d\mid p^k}\mu(d)=\sum_{j=0}^{k}\mu(p^j)=1-1+0+0+\dots=0.$$

□

Teorema 2.2.7 (Fórmula de Inversão de Möbius)**.** *Sejam f uma função multiplicativa e $F(n) = \sum_{d|n} f(d)$. Então para todo natural n vale*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Demonstração. Vejamos que

$$\begin{aligned}\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d_1|\frac{n}{d}} f(d_1) = \sum_{d|n} \sum_{d_1|\frac{n}{d}} \mu(d) f(d_1) \\ &= \sum_{d_1|n} \sum_{d|\frac{n}{d_1}} \mu(d) f(d_1) = \sum_{d_1|n} f(d_1) \sum_{d|\frac{n}{d_1}} \mu(d) = f(n)\mu(1) = f(n).\end{aligned}$$

□

A ideia do crivo de Eratóstenes é identificar os números primos até um certo valor. A função de Möbius permite captar números livres de quadrados, isto é, numéros naturais n tais que $p^2 \nmid n$ para todo p primo. Além disso, a função de Möbius permite uma ideia análoga ao Princípio da Inclusão-Exclusão. De fato, $\mu(p_1) = -1$, $\mu(p_1p_2) = 1$, $\mu(p_1p_2p_3) = -1$, ..., onde os p_i são primos distintos. Isso gera os sinais alternados da expressão do Princípio da Inclusão-Exclusão. Ao truncar o número de fatores primos de um número livre de quadrados, ganhamos uma desigualdade superior ou inferior, a depender da paridade do número de fatores primos. Essa é a principal motivação do crivo de Brun que veremos nessa dissertação.

2.3 O Teorema de Chebyshev e as Fórmulas de Mertens

Lema 2.3.1. *Sejam n um número natural e p um número primo. Defina γ_p como sendo o único inteiro positivo tal que $p^{\gamma_p} < 2n < p^{\gamma_p+1}$. Então o expoente da maior potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!^2}$ é menor ou igual a γ_p. Em particular, se $p > \sqrt{2n}$ então o expoente desta máxima potência de p é menor ou igual a 1. Com isso, se $\frac{2}{3}n < p < n$ então p não divide $\binom{2n}{n.}$*

Demonstração. Defina α e β como os máximos expoentes das potências de p que dividem $(2n)!$ e $n!$, respectivamente. Por [1, Proposição 1.22], temos

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \dots \quad \text{e} \quad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Isso implica que o expoente da máxima potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!^2}$ é:

$$\alpha - 2\beta = \sum_{i=1}^{\gamma_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right).$$

Daí segue que

$$\frac{2n}{p^i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1$$

e

$$-2\left(\frac{n}{p^i} - 1\right) > -2\left\lfloor \frac{n}{p^i} \right\rfloor \geq -2\frac{n}{p^i}.$$

Somando as duas inequações acima obtemos

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor > -1.$$

Com isso, temos que $\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor$ pertence a $\{0, 1\}$, o que implica que $\alpha - 2\beta \leq \sum_{i=1}^{\gamma_p} 1 = \gamma_p$. Suponha agora que $2n/3 < p < n$. Temos $2 < n/p < 3$ e também $1 < n/p < 3/2$, donde concluímos que $\alpha = 2$ e $\beta = 1$, logo $\alpha - 2\beta = 0$. □

Definição 2.3.2. *Seja g uma função que toma valores positivos. Escrevemos $f(x) = O(g(x))$ se existir $C > 0$ tal que $f(x) \leq C \cdot g(x)$ para todo $x > 0$.*

Teorema 2.3.3 (Chebyshev)**.** *Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x. Existem constantes positivas $0 < c < 1 < C$ tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}.$$

Demonstração. Notemos que

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

e como existem $\pi(2n) - \pi(n)$ primos entre n e $2n$, temos que

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p<2n} p \leq \binom{2n}{n} < 2^{2n},$$

onde na 2° desigualdade usamos que $p \mid \binom{2n}{n}$ para todo $n < p \leq 2n$, logo $\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}$. Vamos mostrar que $\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}$. Para $1 \leq k \leq 5$, vamos testar manualmente:

(a) para $k = 1$, temos $2 = \pi(2^{1+1}) = \pi(4) \leq \frac{5 \cdot 2^1}{1} = 10$,

(b) para $k = 2$, temos $4 = \pi(2^{2+1}) = \pi(8), \leq \frac{5 \cdot 2^2}{2} = 10$,

(c) para $k = 3$, temos $6 = \pi(2^{3+1}) = \pi(16) \leq \frac{5 \cdot 2^3}{3} = \frac{40}{3}$,

(d) para $k = 4$, temos $11 = \pi(2^{4+1}) = \pi(32) \leq \frac{5 \cdot 2^4}{4} = 20$,

(e) para $k = 5$ temos $18 = \pi(2^{5+1}) = \pi(64) \leq \frac{5 \cdot 2^5}{5} = 32$.

Para $k \geq 5$ faremos uma soma telescópica e uma indução. Temos:

$$\pi(2^2) - \pi(2) < \frac{2 \cdot 2 \log 2}{\log 2}$$
$$\pi(2^3) - \pi(2^2) < \frac{2 \cdot 2^2 \log 2}{\log 2^2}$$
$$\vdots$$
$$\pi(2^{k+1}) - \pi(2^k) < \frac{2 \cdot 2^k \log 2}{\log 2^k}.$$

Somando tudo obtemos

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

Agora vamos provar por indução que

$$1 + 2 \sum_{i=1}^{k} \frac{2^i}{i} < 5 \cdot \frac{2^k}{k}. \tag{2.2}$$

A base da indução $k = 5$ já foi feita anteriormente. Suponha agora que a Desigualdade (2.2) é válida para algum $k \geq 5$. Somando $\frac{2^{k+1}}{k+1}$ a ambos os lados da Hipótese, temos

$$1 + 2 \sum_{i=1}^{k+1} \frac{2^i}{i} < \frac{5 \cdot 2^k}{k} + 2 \cdot \frac{2^{k+1}}{k+1} \leq 5 \cdot \frac{2^{k+1}}{k+1},$$

sendo a última desigualdade equivalente a $k \geq 5$. Agora, fixado um $x \geq 2$, seja k um natural tal que $2^k < x \leq 2^{k+1}$. Temos

$$\pi(x) \leq \pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k} \leq \frac{5x \log 2}{\log x},$$

uma vez que $\log x > k \log 2$. Assim, provamos que $\pi(x) \leq C \frac{x}{\log x}$.

Vamos provar agora a cota inferior. Seja $\binom{2n}{n} = \prod_{p<2n} p^{\gamma_p}$ a fatoração de $\binom{2n}{n}$ em primos. Pelo Lema 2.3.1, temos $p^{\gamma_p} \leq 2n$, que equivale a $\gamma_p \log p \leq \log 2n$. Aplicando logaritmo na fatoração, obtemos

$$\log \binom{2n}{n} = \sum_{p<2n} \gamma_p \log p \leq \sum_{p<2n} \log(2n) \leq \pi(2n) \log(2n).$$

Como

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^n,$$

temos

$$\pi(2n) \geq \frac{\log \binom{2n}{n}}{\log(2n)} \geq \frac{n \log 2}{\log(2n)} \geq c \frac{n}{\log n}$$

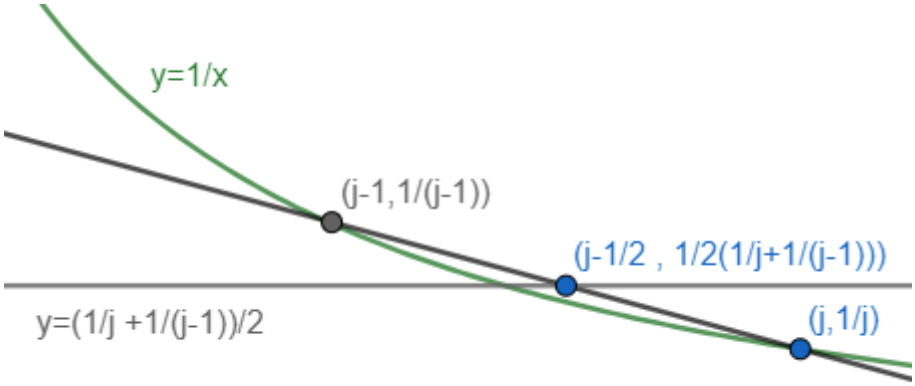
para algum $c > 0$. Dessa forma, $\pi(x) \geq c \frac{x}{\log x}$ para todo x par. Como $\pi(2k-1) = \pi(2k)$ o

resultado se estende para todo $x \geq 2$.

□

Lema 2.3.4. $\sum_{j=1}^{n} \frac{1}{j} = \log n + O(1)$.

Demonstração. Seja $g : \mathbb{R}_+ \to \mathbb{R}$ dada por $g(x) = 1/x$. Temos $g'(x) = -1/x^2 < 0$ e $g''(x) = 2/x^3 > 0$, o que implica que $g(x)$ é estritamente decrescente e possui concavidade voltada para cima. Assim, para $j \geq 2$ inteiro, a reta $y = 1/j$ fica abaixo do gráfico $y = 1/x$ para $x \in [j-1, j]$.



Com isso temos que

$$\frac{1}{j} < \int_{j-1}^{j} \frac{1}{x} dx < \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right). \tag{2.3}$$

Somando de $j = 2$ até n, obtemos

$$\begin{aligned}
\int_1^n \frac{1}{x} dx = \sum_{j=2}^{n} \int_{j-1}^{j} \frac{1}{x} dx &< \sum_{j=2}^{n} \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right) \\
&= \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2} + \frac{1}{3}\right) + \cdots + \frac{1}{2}\left(\frac{1}{n-1} + \frac{1}{n}\right) \\
&= \frac{1}{2}\left(1 + 2 \cdot \frac{1}{2} + 2 \cdot \frac{1}{3} + \cdots + 2 \cdot \frac{1}{n-1} + \frac{1}{n}\right) \\
&= \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{2n} \\
&= \frac{1}{2} - \frac{1}{2n} + \sum_{j=2}^{n} \frac{1}{j}.
\end{aligned}$$

Somando o termo $j = 1$ e usando que $\int_1^n \frac{1}{x} dx = \log n$, obtemos

$$\log n < \frac{1}{2} - \frac{1}{2n} + \sum_{j=2}^{n} \frac{1}{j} \Rightarrow \frac{1}{2} + \frac{1}{2n} + \log n < \sum_{j=2}^{n} \frac{1}{j}. \tag{2.4}$$

Por outro lado, somando a Equação (2.3) de $j = 2$ até n e depois somando 1 em cada lado,

temos

$$\log n > \sum_{j=2}^{n} \frac{1}{j} \Rightarrow 1 + \log n > \sum_{j=1}^{n} \frac{1}{j}.$$

Portanto segue o resultado.

□

Lema 2.3.5. $\displaystyle\sum_{j=1}^{n} \log j = \left(n + \frac{1}{2}\right) \log n - n + O(1).$

Demonstração. Seja $g(x) = \log x$ para $x \geq 2$. Como $g'(x) = \frac{1}{x} > 0$ e $g''(x) = -\frac{1}{x^2} < 0$ temos que g é estritamente crescente e tem concavidade voltada para baixo. Portanto, para todo inteiro $j \geq 2$, a reta ao qual o ponto $(j, \log j)$ pertence, que tem inclinação $g'(j) = 1/j$, que fica acima de $y = g(x)$ no intervalo $[j-1, j]$, que por sua vez fica por cima da reta que passa pelos pontos $(j-1, \log(j-1))$ e $(j, \log j)$. Assim, temos

$$\log j - \frac{1}{2j} > \int_{j-1}^{j} \log x dx > \frac{1}{2}(\log(j-1) + \log j) \tag{2.5}$$

Fazendo a soma das Desigualdades em (2.3) de $j = 2$ até n, segue que

$$\sum_{j=2}^{n} \log j - \sum_{j=2}^{n} \frac{1}{2j} > \int_{1}^{n} \log x dx > \sum_{j=2}^{n} \frac{1}{2}(\log(j-1) + \log j) = \sum_{j=2}^{n} \log j - \frac{1}{2} \log n.$$

Como $\int_1^n \log x dx = n \log n - n + 1$ e $\log 1 = 0$, segue que

$$\left(n + \frac{1}{2}\right) \log n - n + 1 > \sum_{j=1}^{n} \log j > n \log n - n + 1 + \frac{1}{2} \sum_{j=2}^{n} \frac{1}{j} = n \log n - n + \frac{1}{2} + \frac{1}{2} \sum_{j=1}^{n} \frac{1}{j}.$$

Logo, pela última desigualdade de (2.4) temos

$$\left(n + \frac{1}{2}\right) \log n - n + 1 > \sum_{j=1}^{n} \log j > \left(n + \frac{1}{2}\right) \log n - n + \frac{1}{4n} + \frac{3}{4}$$

e o resultado segue. □

Lema 2.3.6. $\displaystyle\sum_{j=2}^{n} \frac{1}{j \log j} = \log \log n + O(1).$

Demonstração. Seja $g(x) = \frac{1}{x \log x}$ para $x \geq 2$. Como $g'(x) = -\frac{\log x + 1}{x^2 \log^2 x} < 0$ e $g''(x) = \frac{2 \log^2 x + 3 \log x + 2}{x^3 \log^3 x} > 0$, segue pelo mesmo argumento dos dois últimos lemas que

$$\frac{1}{j \cdot \log j} < \int_{j-1}^{j} \frac{1}{x \cdot \log x} dx < \frac{1}{2} \left(\frac{1}{(j-1) \log(j-1)} + \frac{1}{j \log j} \right).$$

Somando para $j = 3$ até n, obtemos

$$\sum_{j=3}^{n} \frac{1}{j \log j} < \int_2^n \frac{1}{x \log x} dx < \frac{1}{2} \sum_{j=3}^{n} \left(\frac{1}{(j-1)\log(j-1)} + \frac{1}{j \log j} \right).$$

Como

$$\int_2^n \frac{1}{x \log x} dx = \log\log n - \log\log 2,$$

os mesmos argumentos nos lemas anteriores podem ser aplicados de forma a obter a demonstração desse.

□

Teorema 2.3.7 (1ª fórmula de Mertens)**.** *Sejam p um número primo e n um número inteiro positivo. Temos*

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

Demonstração. Considere $n! = \prod_{p \leq n} p^{v_p}$, onde $v_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$. Assim temos

$$\sum_{k=1}^{n} \log k = \log n! = \log \prod_{p \leq n} p^{v_p} = \sum_{p \leq n} \log p^{v_p} = \sum_{p \leq n} v_p \log p.$$

Observemos que

$$\begin{aligned} \frac{n}{p} - 1 < \left\lfloor \frac{n}{p} \right\rfloor &\leq v_p \\ &< \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \\ &= \frac{n}{p} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \\ &= \frac{n}{p} \cdot \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}. \end{aligned}$$

Daí

$$\begin{aligned} \sum_{k=1}^{n} \log k = \sum_{p \leq n} v_p \log p &< \sum_{p \leq n} \frac{n}{p-1} \log p = n \sum_{p \leq n} \frac{\log p}{p-1} \cdot \frac{p}{p} \\ &= n \sum_{p \leq n} \frac{\log p}{p} \left[1 + \frac{1}{p-1} \right] = n \sum_{p \leq n} \frac{\log p}{p} + n \sum_{p \leq n} \frac{\log p}{p(p-1)}. \end{aligned}$$

Vamos provar que o último somatório da linha acima converge. De fato, temos

$$\sum_{p \leq n} \frac{\log p}{p(p-1)} < \sum_{p} \frac{\log p}{p(p-1)} < \sum_{j \geq 2} \frac{\log j}{j(j-1)} < \sum_{j=1}^{\infty} \frac{\sqrt{j}}{j^2} = \sum_{j=1}^{\infty} \frac{1}{j^{3/2}} < \infty,$$

o que implica

$$\begin{aligned}
&\sum_{k=1}^{n} \log k \leq n \sum_{p \leq n} \frac{\log p}{p} + nO(1) \\
\Rightarrow &\sum_{p \leq n} \frac{\log p}{p} \geq \frac{1}{n} \sum_{k=1}^{n} \log k + O(1) \\
&\qquad = \frac{1}{n} \left[\left(n + \frac{1}{2} \right) \log n - n + O(1) \right] + O(1) = \log n + O(1).
\end{aligned}$$

Falta mostrar que

$$\sum_{p \leq n} \frac{\log p}{p} \leq \log n + O(1).$$

Usando o Lema 2.3.5, temos

$$\begin{aligned}
\sum_{k=1}^{n} \log k &= \sum_{p \leq n} v_p \log p > \sum_{p \leq n} \left(\frac{n}{p} - 1 \right) \log p = \sum_{p \leq n} \frac{n \log p}{p} - \sum_{p \leq n} \log p \\
\Rightarrow \sum \frac{\log p}{p} &< \left(\sum_{k=1}^{n} \log k \right) \frac{1}{n} + \left(\sum_{p \leq n} \log p \right) \frac{1}{n} \\
&\leq \left(\frac{n + 1/2}{n} \right) \log n + O(1) + \left(\sum_{p \leq n} \log n \right) \frac{1}{n} \\
&\leq \log n + O(1) + \frac{\log n}{n} \sum_{p \leq n} 1 \\
&= \log n + O(1) + \frac{\log n}{n} \pi(n) \\
&\leq \log n + O(1) + \frac{\log n}{n} \cdot \frac{Cn}{\log n} \\
&= \log n + O(1).
\end{aligned}$$

Assim, temos a primeira fórmula de Mertens:

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

□

Teorema 2.3.8 (2ª fórmula de Mertens)**.** *Seja p um número primo e n um número natural. Temos que*

$$\sum_{p \leq n} \frac{1}{p} = \log \log n + O(1).$$

Demonstração. Sejam

$$a_k = \begin{cases} \frac{\log k}{k} & \text{se } k \text{ é primo} \\ 0 & \text{caso contrário} \end{cases} \quad \text{e} \quad S_n = \sum_{k=1}^{n} a_k = \sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

Observamos que $S_k - S_{k-1} = a_1 + a_2 + \cdots + a_{k-1} + a_k - (a_1 + a_2 + \cdots + a_{k-1}) = a_k$. Assim temos

$$\begin{aligned}
\sum_{p\leq n}\frac{1}{p} &= \sum_{k=2}^{n}\frac{a_k}{\log k} = \sum_{k=2}^{n}\frac{S_k - S_{k-1}}{\log k} = \sum_{k=2}^{n}\frac{S_k}{\log k} - \sum_{k=2}^{n}\frac{S_{k-1}}{\log k} \\
&= \frac{S_2}{\log 2} + \frac{S_3}{\log 3} + \cdots + \frac{S_{x-1}}{\log n - 1} + \frac{S_n}{\log n} - \frac{S_2}{\log 3} - \frac{S_3}{\log 4} - \cdots - \frac{S_{n-1}}{\log n} \\
&= S_2\left(\frac{1}{\log 2} - \frac{1}{\log 3}\right) + S_3\left(\frac{1}{\log 3} - \frac{1}{\log 4}\right) + \cdots + S_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n} S_k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n}(\log k + O(1))\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n}\left[\log k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + O(1)\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right)\right] + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n}\log k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + O(1)\sum_{k=2}^{n}\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n}\left(1 - \frac{\log k}{\log(k+1)}\right) + O(1) + \frac{\log n + O(1)}{\log(n+1)} \\
&= \sum_{k=2}^{n}\frac{\log(k+1) - \log k}{\log(k+1)} + O(1).
\end{aligned}$$

Como

$$\frac{1}{k+1} \leq \int_k^{k+1}\frac{1}{x}dx \leq \frac{1}{k}$$

e

$$\int_k^{k+1}\frac{1}{x}dx = \log(k+1) - \log k,$$

obtemos

$$\frac{1}{(k+1)\log(k+1)} \leq \frac{\log(k+1) - \log k}{\log(k+1)} \leq \frac{1}{k\log(k+1)},$$

logo

$$\begin{aligned}
0 &\leq \sum_{k=2}^{n}\frac{1}{k\log(k+1)} - \sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)} = \sum_{k=2}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right)\frac{1}{\log(k+1)} \\
&\leq \sum_{k=2}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right) = \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) = \frac{1}{2} - \frac{1}{n+1}.
\end{aligned}$$

Isso implica que podemos trocar $\displaystyle\sum_{k=2}^{n}\frac{\log(k+1) - \log k}{\log(k+1)}$ por $\displaystyle\sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)} + O(1)$,

logo

$$\sum_{p\leq n}\frac{1}{p}=\sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)}+O(1)=\log\log n+O(1).$$

□

2.4 O Teorema de Clement

A seguir, vamos apresentar uma caracterização dos primos gêmeos devida a Clement. Mas antes precisamos do seguinte lema.

Lema 2.4.1 (Wilson). *Seja $n\geq 2$ um inteiro. Então n primo se somente se $(n-1)!\equiv -1 \pmod{n}$. Caso $n=4$, temos $3!\equiv 2 \pmod{4}$ e caso $n>4$ seja composto, temos $(n-1)!\equiv 0 \pmod{n}$.*

Demonstração. ($\Rightarrow$) Suponha primeiramente que n é primo. Se $n=2$ então $(2-1)!\equiv -1 \pmod{2}$ e acabou. Suponha que n é primo ímpar. Note que a equação $x^2\equiv 1 \pmod{n}$ tem exatamente duas soluções: $x\equiv 1 \pmod{n}$ e $x\equiv n-1 \pmod{n}$, uma vez que $x^2-1=(x-1)(x+1)\equiv 0 \pmod{n}$, logo $n\mid x-1$ ou $n\mid x+1$. Em particular, os únicos números módulo n que são seus própios inversos são 1 e $n-1$. Os outros números entre 2 e $n-2$ (que possuem inverso módulo n) são distintos dos seus inversos. Com isso podemos organizar o produto $(n-1)!$ em pares de inversos como a seguir:

$$\begin{aligned}(n-1)! &= (n-1)\cdot(n-2)\cdot(n-3)\cdot\ldots\cdot 3\cdot 2\cdot 1\\ &\equiv (n-1)\cdot 1\cdot(2\cdot 2^{-1})\cdot(3\cdot 3^{-1})\cdot\ldots\\ &\equiv -1 \pmod{n}\end{aligned}$$

($\Leftarrow$) Suponha n composto. Se $n=4$ então $(4-1)!=6\equiv 2\not\equiv -1 \pmod{4}$. Se $n>4$ e $n=a^2$ (ou seja $a\geq 3$), então a e $2a$ são fatores de $(n-1)!=(n-1)\ldots(2a)\ldots(a)\ldots 2\cdot 1\equiv 0 \pmod{n}$. Por outro lado se n não é um quadrado perfeito. Então $n=ab$, onde $2\leq a<b<n$, logo $(n-1)!=(n-1)\ldots(b)\ldots(a)\ldots 2\cdot 1\equiv 0 \pmod{n}$. □

Teorema 2.4.2 (Clement). *Seja $n\geq 2$. O par $(n,n+2)$ um par de primos gêmeos se e somente se*

$$4((n-1)!+1)+n\equiv 0 \pmod{n(n+2)}.$$

Demonstração. ($\Rightarrow$) Suponha que n e $n+2$ são primos. Pelo Lema de Wilson, temos

$$4((n-1)!+1)+n\equiv 4(-1+1)+n\equiv 0 \pmod{n}.$$

Além disso

$$\begin{aligned}4((n-1)!+1)+n &\equiv 4(n-1)!+4-2 \pmod{n+2}\\ &\equiv 2(-1)(-2)(n-1)!+2 \pmod{n+2}\end{aligned}$$

$$\equiv 2(n+1)n(n-1)! + 2 \pmod{n+2}$$
$$\equiv 2((n+1)! + 1) \pmod{n+2}$$
$$\equiv 0 \pmod{n+2}.$$

Como n e $n+2$ são primos entre si (pois são primos), segue que

$$4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}.$$

($\Leftarrow$) Suponha que

$$4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}.$$

Queremos mostrar que n e $n+2$ são primos. Note que $n \neq 4$, pois caso $n = 4$ teríamos

$$4(3! + 1) + 4 = 32 \equiv 8 \pmod{24}.$$

Suponha $n \neq 4$ composto. Temos, em particular, que

$$4((n-1)! + 1) + n \equiv 0 \pmod{n},$$

o que implica que

$$4((n-1)! + 1) \equiv 0 \pmod{n}.$$

Pelo Lema de Wilson, temos $(n-1)! \equiv 0 \pmod{n}$, logo $4(0+1) \equiv 0 \pmod{n}$, ou seja, $n = 2$, o que é um absurdo pois 2 é primo. Por outro lado, suponha que $n+2$ é composto. Da mesma forma, temos

$$4((n-1)! + 1) + n \equiv 0 \pmod{n+2},$$

o que implica que

$$2((n+1)! + 1) \equiv 0 \pmod{n+2}.$$

Pelo Lema de Wilson,

$$2(0+1) \equiv 0 \pmod{n+2},$$

o que é um absurdo. Logo, n e $n+2$ são primos.

□

Não vamos demonstrar mas existe uma generalização do Teorema de Clement para pares de primos com diferença $d \geq 2$. Essa generalização afirma o seguinte:

Teorema 2.4.3. *Sejam $n, d \geq 2$ inteiros positivos com $mdc(d!, n) = 1$. Então n e $n+d$ são primos se e somente se*

$$d!d[(n-1)! + 1] + (d! - 1) \equiv 0 \pmod{n(n+d)}.$$

Capítulo 3

O crivo de Brun

Nesse capítulo, vamos apresentar o Crivo de Brun, que fornece uma cota superior para $\pi_2(x) = \#\{p \leq x; p, p+2 \text{ são primos}\}$, isto é, $\pi_2(x)$ conta o número de primos gêmeos até x. Isso permitirá obter que a soma dos inversos dos primos gêmeos converge, o que contrasta com a soma dos inversos dos primos.

3.1 O trucamento do Crivo de Brun

A principal ideia do Crivo de Brun é truncar a função de Möbius de acordo com a paridade da quantidade de números primos que dividem m, o argumento de $\sum_{d|m} \mu(d)$. Lembrando que a função de Möbius capta números livres de quadrados, e com isso conseguimos captar os números livres de quadrados que possuem no máximo uma quantidade fixa $l \geq 1$ de fatores primos. Isso irá fornecer uma cota superior ou inferior para soma da função de Möbius, dependendo apenas da paridade de l. Mas antes precisamos da seguinte definição:

Definição 3.1.1. *Seja $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ um número natural fatorado em primos. Denotamos por $w(n) = k$, o número de fatores primos distintos de n. Além disso, definimos $d(n) = \sum_{m|n} 1$ como o número de divisores de n.*

Observamos que

$$d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1),$$

pois se $m \mid n$ então $m = p_1^{\beta_1} \dots p_k^{\beta_k}$ e $0 \leq \beta_i \leq \alpha_i$ para todo i, ou seja, temos $\alpha_i + 1$ possibilidades para cada β_i. Em particular, se n é livre de quadrados ($\alpha_i = 1$ para todo i) então $d(n) = 2^{w(n)}$.

Lema 3.1.2. *Sejam m e l números naturais. Então*

$$\sum_{\substack{d|m \\ w(d) \leq 2l-1}} \mu(d) \leq \sum_{d|m} \mu(d) \leq \sum_{\substack{d|m \\ w(d) \leq 2l}} \mu(d).$$

Demonstração. Suponha que $m = 1$. Temos $w(d) = 0$, assim é verdadeira a sentença $1 \leq 1 \leq 1$. Para $m > 1$ temos $\sum_{d|m} \mu(m) = 0$ pelo Lema 2.2.6. Considerando $k = w(m)$, podemos

supor que m é livre de quadrados, pois caso exista $d \mid m$ que não é livre de quadrados teríamos $\mu(d) = 0$, não acrescentando nada a mais às somas. Fixado $s \in \mathbb{N}$, teremos

$$\begin{aligned}
\sum_{\substack{d|m \\ w(d)\leq s}} \mu(d) &= \sum_{j=0}^{s} \sum_{\substack{d|m \\ w(d)=j}} \mu(d) \\
&= \sum_{j=0}^{s} \sum_{\substack{d|m \\ w(d)=j}} (-1)^j \\
&= \sum_{j=0}^{s} \binom{k}{j} (-1)^j \\
&= 1 + \sum_{j=1}^{s} \binom{k}{j} (-1)^j \\
&= 1 + \sum_{j=1}^{s} \left[\binom{k-1}{j-1} + \binom{k-1}{j} \right] (-1)^j \quad \text{(Relação de Stifel)} \\
&= 1 + \binom{k-1}{0}(-1) + \binom{k-1}{1}(-1) + \binom{k-1}{1} + \binom{k-1}{2} + \dots \\
&\quad \cdots + \binom{k-1}{s-2}(-1)^{s-1} + \binom{k-1}{s-1}(-1)^{s-1} + \binom{k-1}{s-1}(-1)^s + \binom{k-1}{s}(-1)^s \\
&= 1 - 1 + \binom{k-1}{s}(-1)^s \quad \text{(Soma telescópica)} \\
&= \binom{k-1}{s}(-1)^s \\
&= \begin{cases} \geq 0, & s \text{ par,} \\ \leq 0, & s \text{ ímpar,} \end{cases}
\end{aligned}$$

como queríamos demonstrar. □

3.2 A cota superior para $\pi_2(x)$ e o Teorema de Brun

Nessa seção, vamos finalmente apresentar o Crivo de Brun. Mas antes precisamos do seguinte lema, que determina o número de soluções de uma congruência módulo m.

Lema 3.2.1. *Seja m um número livre de quadrados. O número de soluções de*

$$x(x+2) \equiv 0 \pmod{m}$$

é

$$f(m) = \frac{d(m)}{d(mdc(m,2))} = 2^{w(m)-w(mdc(w,2))}.$$

Demonstração. Observe que toda solução de $x(x+2) \equiv 0 \pmod{m}$ é solução das seguintes congruências:

$$x \equiv 0 \pmod{r} \quad \text{e} \quad x \equiv -2 \pmod{\frac{m}{r}}$$

onde $r \mid m$. Sejam r e s divisores de m e suponha que x_r e x_s são soluções do sistema de congruências acima para r e s, respectivamente. Além disso suponha que $x_r \equiv x_s \pmod m$. Podemos supor também que $0 < x_r, x_s \leq m$, de forma que $x_r = x_s$. Escreva $r = ad$ e $s = bd$, onde $d = mdc(r, s)$ e $mdc(a, b) = 1$. Seja $t = ab = \frac{mmc(r,s)}{mdc(r,s)}$, de forma que $t \mid m$. Temos que $a \mid r \mid x_r$ e $b \mid s \mid x_s$. Além disso, $a \mid r \mid \frac{m}{s} \mid x_s + 2$ e $b \mid s \mid \frac{m}{r} \mid x_r + 2$, logo $t \mid x_r$ e $t \mid x_r + 2$, pois $x_r = x_s$. Isso implica que $t \mid 2$, ou seja, $t \in \{1, 2\}$. Se $t = 1$ então $a = b = 1$, daí $r = s$, isto é, a solução do sistema é única para cada divisor r de m. Se $t = 2$ então sem perda de generalidade podemos supor que $a = 2$ e $b = 1$, daí $r = 2d$ e $s = d$, logo há duas soluções para cada divisor r de m. Note nesse caso que m é par. Dessa forma, o número de soluções para congruência inicial é $2^{w(d)}$ se m é ímpar e $2^{w(d)}/2 = 2^{w(d)-1}$ se m é par. □

Definição 3.2.2. $\pi_2(x) = \#\{p \leq x; p, p + 2$ *são primos*$\}$*, isto é,* $\pi_2(x)$ *conta o número de primos gêmeos até* x*.*

Teorema 3.2.3. *É válida a seguinte cota superior:*

$$\pi_2(x) = O\left(x\left(\frac{\log\log x}{\log x}\right)^2\right).$$

Demonstração. Sejam

$$\begin{aligned} &z \leq \sqrt{x}, \\ &p(z) = \prod_{p \leq z} p, \\ &A = \{k(k+2); k \in \mathbb{Z} \text{ e } 1 \leq k \leq x\}, \\ &y = k(k+2) \in A. \end{aligned}$$

Se k e $k + 2$ são primos e $k > z$ então $mdc(y, p(z)) = 1$. Temos

$$\pi_2(x) \leq \#\{y \in A; mdc(y, p(z)) = 1\} + \pi_2(z) \leq \#\{y \in A; mdc(y, p(z)) = 1\} + z.$$

Pelos Lemas 2.2.6 e 3.1.2, temos

$$\begin{aligned} \#\{y \in A; mdc(y, p(z)) = 1\} = \sum_{\substack{y \in A \\ mdc(y,p(z))=1}} 1 &= \sum_{y \in A} \sum_{d \mid mdc(y,p(z))} \mu(d) \leq \sum_{y \in A} \sum_{\substack{d \mid mdc(y,p(z)) \\ w(d) \leq 2l}} \mu(d) \\ &= \sum_{\substack{d \mid p(z) \\ w(d) \leq 2l}} \sum_{\substack{y \in A \\ d \mid y}} \mu(d) = \sum_{\substack{d \mid p(z) \\ w(d) \leq 2l}} \mu(d) \sum_{\substack{y \in A \\ d \mid y}} 1 = \sum_{\substack{d \mid p(z) \\ w(d) \leq 2l}} \mu(d)|A_d|, \end{aligned}$$

onde $A_d = \{y \in A; d \mid y\}$. Note que

$$\left||A_d| - \frac{x}{d} \cdot f(d)\right| < f(d),$$

onde $f(d) = 2^{w(d)-w((d,2))}$ pelo Lema 3.2.1. De fato, temos $f(d)$ soluções para a congruência

$y \equiv 0 \pmod d \iff k(k+2) \equiv 0 \pmod d$ no intervalo $[1,d]$, o que implica que o número de soluções da congruência $y \equiv 0 \pmod d$ em $[1,x]$ está entre o número de soluções em $[1,\lfloor x/d \rfloor]$ e $[1,\lfloor x/d \rfloor + 1]$, daí segue a desigualdade anterior. Assim obtemos

$$\begin{aligned}
\#\{y \in A; mdc(y,p(z))=1\} &\leq \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \mu(d)\cdot |A_d| \\
&\leq \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \mu(d)\cdot \left(\frac{x}{d}\cdot f(d) + f(d)\right) \\
&= x \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \frac{\mu(d)f(d)}{d} + \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \mu(d)f(d) \\
&\leq x \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \frac{\mu(d)f(d)}{d} + O\left(\sum_{\substack{d|p(z)\\ w(d)\leq 2l}} f(d)\right).
\end{aligned}$$

Como $d \mid p(z)$ e $w(d) \leq 2l$ temos $d \leq z^{2l}$. Assim, pelo Lema 2.3.4, segue que

$$\begin{aligned}
\sum_{\substack{d|p(z)\\ w(d)\leq 2l}} f(d) &\leq \sum_{1\leq r\leq z^{2l}} d(r) = \sum_{1\leq r\leq z^{2l}} \sum_{m|r} 1 = \sum_{1\leq m\leq z^{2l}} \sum_{\substack{m|r\\ r\leq z^{2l}}} 1 = \sum_{1\leq m\leq z^{2l}} \left\lfloor \frac{z^{2l}}{m} \right\rfloor \\
&\leq \sum_{1\leq m\leq z^{2l}} \left(\frac{z^{2l}}{m} + 1\right) = z^{2l} \sum_{1\leq m\leq z^{2l}} \frac{1}{m} + O(z^{2l}) = z^{2l}\log z^{2l} + O(z^{2l}) \\
&= O(z^{2l}\log z^{2l}).
\end{aligned}$$

Escolhemos

$$z = e^{\frac{\log x}{20\log\log x}} = x^{\frac{1}{20\log\log x}} \quad \text{e} \quad l = \left\lfloor \frac{\log x}{4\log z} \right\rfloor = \left\lfloor \frac{\log x}{4\frac{\log x}{20\log\log x}} \right\rfloor = \lfloor 5\log\log x \rfloor$$

de forma que

$$\begin{aligned}
z^{2l}\log z^{2l} &= e^{\frac{\log x}{20\log\log x}\cdot 2\lfloor 5\log\log x\rfloor} \cdot \frac{\log x}{20\log\log x}\cdot 2\lfloor 5\log\log x\rfloor \\
&\leq \left(e^{\log x}\right)^{\frac{1}{2}} \cdot \frac{\log x}{2} = \frac{\sqrt{x}\log x}{2} = O(\sqrt{x}\log x),
\end{aligned}$$

o que determina o termo do erro. Falta estimar o termo principal. Temos

$$x\cdot \sum_{\substack{d|p(z)\\ w(d)\leq 2l}} \frac{\mu(d)f(d)}{d} = x\cdot \left(\sum_{d|p(z)} \frac{\mu(d)f(d)}{d} - \sum_{\substack{d|p(z)\\ w(d)\geq 2l+1}} \frac{\mu(d)f(d)}{d}\right). \tag{3.1}$$

Observe que $\mu(d)$, $f(d)$ e d são funções multiplicativas, então $\sum_{d|p(z)} \frac{\mu(d)f(d)}{d}$ é multiplicativa.

Fatorando, usando a Proposição 2.2.3, o Lema 3.2.1 e a 2^a Fórmula de Mertens, temos:

$$\begin{aligned}
\sum_{d|p(z)} \frac{\mu(d)f(d)}{d} &= \prod_{\substack{q|p(z)\\ q \text{ primo}}} \left(1 + \frac{\mu(q)f(q)}{q} + \frac{\mu(q^2)f(q^2)}{q^2} + \frac{\mu(q^3)f(q^3)}{q^3} + \dots\right) \\
&= \prod_{\substack{q|p(z)\\ q \text{ primo}}} \left(1 - \frac{f(q)}{q}\right) \\
&= \prod_{\substack{2<q\leq z\\ q \text{ primo}}} \left(1 - \frac{f(q)}{q}\right) \cdot \left(1 - \frac{1}{2}\right) \\
&= \frac{1}{2} \prod_{2<q\leq z} \left(1 - \frac{f(q)}{q}\right) \\
&= \frac{1}{2} \prod_{2<q\leq z} \left(1 - \frac{2}{q}\right) \\
&= \frac{1}{2} \prod_{2<q\leq z} e^{\log\left(1-\frac{2}{q}\right)} \\
&= \frac{1}{2} e^{\sum_{2<q\leq z} \log\left(1-\frac{2}{q}\right)} \\
&= \frac{1}{2} e^{\sum_{2<q\leq z} \left(-\frac{2}{q} - \frac{4}{q^2} - \frac{8}{q^3} - \dots\right)} \\
&= \frac{1}{2} e^{\sum_{2<q\leq z} \left(O(1/q^2) - \frac{2}{q}\right)} \\
&= \frac{1}{2} e^{\left(O(1) - 2\sum_{2<q\leq z} \frac{1}{q}\right)} \\
&= \frac{1}{2} \cdot e^{O(1)} \cdot e^{-2\log\log z} \\
&= O(1) \cdot e^{-2\log\log z} \\
&= O\left(e^{-2\log\log z}\right) \\
&= O\left((\log z)^{-2}\right) \\
&= O\left(\frac{1}{\log^2 z}\right) \\
&= O\left(\frac{1}{\left(\frac{\log x}{20\log\log x}\right)^2}\right) \\
&= O\left(\frac{400(\log\log x)^2}{(\log x)^2}\right) \\
&= O\left(\frac{(\log\log x)^2}{(\log x)^2}\right),
\end{aligned}$$

o que limita o 1° termo dentro do parênteses da Equação (3.1). Para estimar o termo restante, notemos que se $w(d) \geq 2l+1$ então $f(d) = 2^{w(d)-w(mdc(d,2))} \geq 2^{2l}$, o que implica que $f(d) \leq$

$\frac{f(d)^2}{2^{2l}}$, logo o segundo termo do parênteses em (3.1) vale

$$\left| \sum_{\substack{d|p(z) \\ w(d)\geq 2l+1}} \frac{\mu(d)f(d)}{d} \right| \leq 2^{-2l} \sum_{d|p(z)} \frac{(f(d))^2}{d}.$$

Como $\frac{(f(d))^2}{d}$ é multiplicativa, temos que $\sum_{d|p(z)} \frac{(f(d))^2}{d}$ também é multiplicativa. Logo

$$\begin{aligned}
\sum_{d|p(z)} \frac{(f(d))^2}{d} &= \prod_{\substack{q \text{ primo} \\ q|p(z)}} \left(1 + \frac{(f(q))^2}{d}\right) \\
&= \frac{3}{2} \prod_{\substack{q \text{ primo} \\ 3\leq q\leq z}} \left(1 + \frac{4}{q}\right) \\
&= \frac{3}{2} e^{\sum_{\substack{q \text{ primo} \\ 3\leq q\leq z}} \log\left(1+\frac{4}{q}\right)} \\
&= e^{O(1)+4\sum_{3\leq q\leq z} \frac{1}{q}} \\
&= e^{O(1)+4\log\log z} \\
&= O(\log^4 z),
\end{aligned}$$

logo

$$\begin{aligned}
\left| \sum_{\substack{d|p(z) \\ W(d)\geq 2l+1}} \frac{\mu(d)f(d)}{d} \right| &= O(2^{-2l}\log^4 z) \\
&= O(e^{-10\log 2\log\log x}\log^4 z) \\
&= O(\log^{-6} x \log^4 x) \\
&= O\left(\frac{1}{\log^2 x}\right).
\end{aligned}$$

Juntando todas as partes, obtemos $\pi_2(x) = O\left(\frac{(\log\log x)^2}{(\log x)^2}\right)$.

□

Com esse resultado em mãos, podemos provar o principal teorema dessa dissertação.

Teorema 3.2.4 (Brun). *A soma*

$$\sum_{p,p+2 \text{ primos}} \frac{1}{p}$$

converge.

Demonstração. Temos

$$\sum_{p,p+2 \text{ primos}} \frac{1}{p} = \sum_{n=0}^{\infty} \sum_{\substack{p,p+2 \text{ primos} \\ 2^n\leq p<2^{n+1}}} \frac{1}{p}$$

$$
\begin{aligned}
&\leq \sum_{n=0}^{\infty} \sum_{\substack{p,p+2 \text{ primos} \\ 2^n \leq p < 2^{n+1}}} \frac{1}{2^n} \\
&\leq \sum_{n=0}^{\infty} \frac{1}{2^n} \sum_{\substack{p,p+2 \text{ primos} \\ 2^n \leq p < 2^{n+1}}} 1 \\
&\leq \sum_{n=0}^{\infty} \frac{\pi_2(2^{n+1})}{2^n} \\
&= \sum_{n=0}^{\infty} \frac{O\left(2^{n+1}\left(\frac{\log\log 2^{n+1}}{\log 2^{n+1}}\right)^2\right)}{2^n} \\
&= \sum_{n=0}^{\infty} \frac{O\left(2^{n+1}\left(\frac{\log[(n+1)\log 2]}{(n+1)\log 2}\right)^2\right)}{2^n} \\
&= \sum_{n=0}^{\infty} O\left(\left(\frac{\log[(n+1)\log 2]}{(n+1)\log 2}\right)^2\right) \\
&= O\left(\sum_{n=0}^{\infty} \frac{\log^2(n+1)}{(n+1)^2}\right) < \infty.
\end{aligned}
$$

□

Capítulo 4

Conclusão

O Crivo de Brun fornece uma cota superior para o número de primos gêmeos até um certo valor x. Essa cota é dada por $O\left(x\left(\frac{\log\log x}{\log x}\right)^2\right)$. Mas essa cota pode ser melhorada fazendo-se estimativas mais apuradas. De fato, o melhor resultado obtido até hoje é $\pi_2(x) < \frac{Cx}{\log x^2}$ para alguma constante $0 < C < 100$ (ver [2]).

4.1 Conjecturas

Acredita-se, mas não se sabe provar, que é válida a seguinte relação:

Conjectura 4.1.1 (Hardy-Littlewood)**.**

$$\pi_2(x) \sim 2C\frac{x}{(\log x)^2},$$

onde $C = \prod_{p\geq 3}\left(1 - \frac{1}{(p-1)^2}\right)$ *e* $f(x) \sim g(x)$ *significa que* $\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1$.

Na verdade, ainda não se sabe provar nem o seguinte resultado:

Conjectura 4.1.2 (Conjectura dos Primos Gêmios)**.** *Existem infinitos pares de primos gêmeos. Em outras palavras,*

$$\lim_{x\to\infty}\pi_2(x) = \infty.$$

Em geral o método do Crivo fornece cotas superiores para as quantidades que queremos contar. Para obter o resultado anterior, precisaremos de uma cota inferior para $\pi_2(x)$, e o método do Crivo ainda não conseguiu evoluir a tal ponto. É importante ressaltar que o método do Crivo de Brun fornece estimativas similares para outros tipos de primos, como os primos de Sophie Germain. Um número primo p é primo de Sophie Germain se $2p + 1$ também for primo. Os primos de Sophie Germain são conhecidos por terem sidos os primeiros casos provados do último Teorema de Fermat (ver [1, Proposição 7.2]). Na Seção 3.2, podemos adaptar todos os cálculos de forma a obter as mesmas estimativas para os primos de Sophie Germain. Em particular, os primos de Sophie Germain até x também

são limitados superiormente por $O\left(x\left(\frac{\log\log x}{\log x}\right)^2\right)$ e também vale que a soma dos inversos dos primos de Sophie Germain converge. Basta adaptar o Lema 3.2.1 para congruência $x(2x+1) \equiv 0 \pmod{m}$ e o Teorema 3.2.3 tomando $A = \{k(2k+1); 1 \leq k \leq x\}$. Em geral, os mesmos resultados e conjecturas podem ser adaptados para pares de primos (p, q) tais que $ap = bq + C$ e $p \leq x$.

4.2 Outras formas de atacar o problema

A tentativa de mostrar que existem infinitos primos gêmeos usando a soma de seus inversos falha no momento que descobrimos que essa soma converge, logo ou temos finitos termos, ou infinitos termos mas muito espaçados. Por outro lado diversas tentativas de se aproximar da Conjectura dos Primos Gêmeos foram e ainda estão sendo feitas. A seguir, vamos citar alguns resultados.

Teorema 4.2.1 (Chen, [3]). *Existem infinitos primos p para os quais $p + 2$ possui no máximo dois fatores primos.*

Do Teorema dos Números Primos, segue que o n-ésimo primo, p_n , satisfaz $p_n \sim n \log n$. Disso concluímos que $p_{n+1} - p_n \sim \log n$, ou seja, na média a diferença entre primos consecutivos é $\log n$. Por outro lado, tomando valores particulares de n, podemos ter $p_{n+1} - p_n$ tão pequeno ou tão grande (em relação à média) quanto quisérmos. De fato, em 2005 foi provado o seguinte:

Teorema 4.2.2 (Goldston, Pintiz, Yildirim, [5]). *Dado $\varepsilon > 0$ existem infinitos n tais que*

$$\frac{p_{n+1} - p_n}{\log n} < \varepsilon$$

O método GPY usa basicamente dois ingredientes: o crivo de Selberg e o Teorema de Bombieri-Vinogradov. Em maio de 2013, Zhang melhorou o Teorema de Bombieri-Vinogradov e provou o seguinte:

Teorema 4.2.3 (Zhang, [10]). *Existem infinitos n tais que*

$$p_{n+1} - p_n < 70000000.$$

Em um projeto colaborativo, chamado de Polymath, diversos matemáticos conseguiram diminuir essa cota para 4680, em poucos meses. Em novembro de 2013, Maynard (e, de forma independente, Tao) melhorou o Crivo de Selberg e, sem usar a melhora de Zhang para Teorema de Bombieri-Vinogradov, provou o seguinte:

Teorema 4.2.4 (Maynard, [9]). *Existem infinitos n tais que $p_{n+1} - p_n \leq 600$.*

Em alguns meses, o Polymath diminuiu a cota de 600 para 246 e esse resultado permanece até hoje.

Referências Bibliográficas

[1] BROCHERO MARTINEZ, F.E.; et al.; *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 5ª edição. Rio de Janeiro: IMPA, 2018.

[2] BRUN, V.; *Le crible d'Eratostène et la théorème de Goldbach, Vindenskapsselskapets Skrifter Kristiania, Matematisk Naturvidenskapeling* Klasse No. 3, 1920, 1-36.

[3] CHEN, J.R.; *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*. Sci. Sinica. 16, 1973, 157–176.

[4] COJOCARU, A.C., MURTY, M.R.; *An introduction to sieve methods and their applications*. Cambridge Univesity Press, 2005.

[5] GOLDSTON, D.A., PINTZ, J., YILDIRIM, C.Y.; *Primes in tuples I*. Annals of Mathematics 170, 2009, 819-862.

[6] HEFEZ, A.; *Aritmética*. 2ª ed. Coleção PROFMAT, SBM, 2016.

[7] KUO, W., et al.; *The shifted Turán sieve method on tournaments*. Canad. Math. Bull. 62 (4), 2019, 841-855.

[8] LIU, Y.-R., MURTY, M.R.; *Sieve methods in combinatorics*. J. Combin. Theory Ser. A 111, 2005, 1-23.

[9] MAYNARD, J.; *Small gaps between primes*. Ann. of Math. 181, 2015, 1-31.

[10] ZHANG, Y.; *Bounded gaps between primes*. Ann. of Math. 179, 2014, 1121–1174.