Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Teorema dos Números Primos

Vinícius Denardi Boabaid Rovedo

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Reinaldo de Marchi**

Cuiabá - MT

Outubro de 2019

Teorema dos Números Primos

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Vinícius e aprovada pela comissão julgadora.

Cuiabá, 14 de outubro de 2019.

Prof. Dr. Reinaldo de Marchi
Orientador

Banca examinadora:

Prof. Dr. Reinaldo de Marchi
Prof. Dra. Thais Silva do Nascimento
Prof. Dr. Junior Cesar Alves Soares

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

D391t Denardi Boabaid Rovedo, Vinícius.
Teorema dos Números Primos / Vinícius Denardi Boabaid Rovedo. -- 2019
xii, 48 f. : il. color. ; 30 cm.

Orientador: Reinaldo de Marchi.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Cuiabá, 2019.
Inclui bibliografia.

1. Teoria analítica dos números. 2. Identidade de Abel. 3. Identidade de Selberg. 4. Produto de Dirichlet. 5. Funções de Chebyshev. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dedico este trabalho à minha primeira professora, que me colocava a tarde inteira na tabuada e caligrafia: futura doutora, Mamãe Angela Denardi.

MINISTÉRIO DA EDUCACÃO
UNIVERSIDADE FEDERAL DE MATO GROSSO
PRÓ-REITORIA DE ENSINO DE PÓS-GRADUACÃO
Programa de Pós-Graduação em Ensino de Matemática em Rede Nacional - Profmat,
Av. Fernando Corrêa da Costa, 2367 - Boa Esperança - 78.060-900 - Cuiabá/MT
Fone: (65) 3615-8576 – E-mail : profmat@ufmt.br

FOLHA DE APROVAÇÃO

Título: "Teorema dos números primos"

Autor: Vinicius Denardi Boabaid Rovedo

defendida e aprovada em 14/10/2019.

Composição da Banca Examinadora:

Reinaldo de Marchi

Presidente Banca/Orientador Doutor Reinaldo de Marchi
Instituição: Universidade Federal de Mato Grosso

Thais S. do Nascimento

Examinadora Interna Doutora Thais Silva do Nascimento
Instituição: Universidade Federal de Mato Grosso

Junior Cesar Alves Soares

Examinador Externo Doutor Junior Cesar Alves Soares
Instituição: UNEMAT - Barra do Bugres

CUIABÁ,09/10/2019.

Agradecimentos

Muito obrigado à todos os professores nesse dia 15/10/2019, meu grupo do Profmat e amigos, especialmente meu grande orientador Reinaldo. Ele me ensinou tudo que sei sobre esse trabalho. Teve a paciência de me aguentar até nas suas férias, domingos no celular e no desespero da defesa. Muitíssimo obrigado, Kingnaldo!!

Existe padrão na distribuição dos números primos?

Dúvida de Séculos.

Resumo

Neste trabalho resgatamos um problema do século XVIII, conhecido por Teorema dos Números Primos, conjecturado por Gauss e Legendre, de modo independente. Tal teorema afirma que a contagem dos números primos até x, denotado por $\pi(x)$, se comporta assintoticamente como $x/\log x$. Nosso intuito é conhecer a demonstração elementar decorrente da identidade de Selberg e as ideias de Erdös e que usa ferramentas da chamada Teoria Analítica dos Números.

Palavras chave: Teoria analítica dos números, identidade de Abel, identidade de Selberg, produto de Dirichlet, funções de Chebyshev.

Abstract

In this paper we rescue an 18th century problem, know as Prime Numbers Theorem, conjectured by Gauss and Legendre independently. Such theorem claims that counting prime numbers until x , denoted by $\pi(x)$, behave asymptotically as $x/\log x$. Our intention is to know the elementary demonstration arising from the Selberg's Identity and ideas from Erdos and uses tools from the called Analytic Number Theory.

Keywords: Analytic Number Theory, Abel's Identity, Selberg's Identity, Dirichlet's Products, Chebshev's functions.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

De acordo com a História da Matemática, os números eram representados por pedras e se relacionavam no que os humanos não sabiam que era uma função entre pedras e animais domesticados.

Baseado na referência Apostol (1976), em registros históricos, 5700 a.C, os antigos Sumérios já tinham um calendário e em 2500 a.C haviam desenvolvido um sistema numérico de base 60, na qual foram transmitidos a outros povos do antigo Oriente Médio. O povo da Babilônia escrevia em tábuas de argila uma Matemática mais elaborada, com problemas de geometria que datavam de 2000 a.C.

Por 5000 anos os números foram usados para registrar transações comerciais, estoques de mantimentos agrícolas, agricultura, medição de terras, porém apenas em 600 a.C é que houve uma primeira tentativa de se estudar a Teoria dos Números. Os primeiros foram os gregos Pitagóricos. Inicialmente classificaram os inteiros em pares, ímpares, compostos e os números primos.

Em 300 a.C tivemos Euclides que escreveu uma coletânea de 13 Livros chamada "Os Elementos". Essa coleção transformou a Matemática numa ciência dedutiva, pois usava fatos matemáticos seguidos por uma rigorosa demonstração. Euclides dedicou três livros para a Teoria dos Números, sendo o livro IX o que possui a demonstração de que existem infinitos números primos. Essa mesma demonstração é feita nos cursos de Matemática das universidades atualmente.

Após Euclides aparece outro grego, Diofanto de Alexandria em 250 d.C. Muitos problemas originários da Teoria dos Números, como equações com solução nos números inteiros, foram trabalhadas por Diofanto. Essas equações são conhecidas como Equações Diofantinas e são de suma importância em várias áreas da Matemática.

A Teoria dos Números realmente floresceu a partir do século XVII. Considerado o pai da Teoria Moderna dos Números, o francês Fermat se inspirou nos trabalhos de

Diofanto. Ele descobriu que todo número primo da forma $4n + 1$ pode ser escrito como soma de dois quadrados.

Logo após Fermat, no século XVIII, os estudos sobre Teoria dos Números foram desenvolvidos por Euler(1701-1783), Lagrange(1736-1813), Legendre(1752-1833), Gauss(1777-1855) e Dirichlet. O campo de estudos ficou tão vasto que em alguns assuntos requerem conhecimento em matemática avançada.

Mesmo tão estudada, o assunto sobre os números primos continua com vários problemas em aberto:

1) Conjectura dos Primos Gêmeos: Existem infinitos pares de primos gêmeos ao longo dos infinitos números primos. Por exemplo: 3 e 5, 5 e 7, 11 e 13, 17 e 19, 1151 e 1153.

2) Conjectura de Goldbach: Todo número par maior que 2 pode ser escrito como soma de dois outros números primos. Por exemplo, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $100 = 47 + 5$.

3) Primos Palíndromos: Primos palíndromos são números primos que podem ser lidos de trás para frente ou vice-versa e permanecem o mesmo número. Como: 11, 101, 131, 151, etc.

Este trabalho tem como objeto de estudo um problema referente ao século XVIII. Gauss e Legendre propuseram, independentemente, que a quantidade de números primos menores ou igual a x e denotada por $\pi(x)$ se comporta aproximadamente como a função $x/\log x$ quando x assume valores cada vez maiores. Mais precisamente, a conjectura afirma que

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

Cerca de 100 anos depois, o russo Chebyshev provou, em 1851, que se a razão tende a um limite, então esse limite é 1. Porém sua demonstração foi incompleta, tendo em vista que não provou se de fato tal limite existe, embora tenha obtido desigualdades que apontavam cada vez mais na validade dessa conjectura.

Em 1859 Riemann percebeu que tal conjectura estava relacionada com a função definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

que aparece em uma fórmula descoberta por Euler em 1737 e que envolve os números primos. Riemann utilizou de valores complexos para s e conectou a distribuição dos números primos às propriedades dessa função, desenvolvendo grandes ideias, mas não conseguiu chegar na demonstração da conjectura, tendo falecido em 1866. Na literatura, a função ζ é conhecida como função zeta de Riemann.

Apenas 30 anos depois, já com todas as ferramentas matemáticas necessárias é que em 1896, J. Hadamard e C.J. de la Vallée Poussin, provaram quase simultânea e independentemente a validade da conjectura dos números primos, hoje conhecido como Teorema dos Números Primos.

Em 1949, Atle Selberg e Paul Erdös apresentaram uma prova que não utilizava a função $\zeta(s)$, e sim argumentos mais elementares, a saber, conhecimento em Cálculo e Teoria dos Números. Nosso objetivo nesse trabalho é entender um pouco sobre essa demonstração do Teorema dos Números Primos.

No Capítulo 1 serão abordadas as Funções Aritméticas: definição e exemplos da Função de Euler e de Möbius: $\varphi(n)$ e $\mu(n)$, respectivamente. A convolução de Dirichlet e a Inversão de Möbius.

No Capítulo 2 apresentamos as funções de Chebyshev, falaremos sobre o Teorema de Abel e algumas suas aplicações, em particular, formas equivalentes do teorema dos números primos. Também adicionamos nesse capítulo a identidade de Selberg, que possibilitou a obtenção da demonstração elementar do TNP.

No Capítulo 3 faremos a demonstração do Teorema dos Números Primos e desenvolvemos três aplicações que são consequências desse teorema.

Capítulo 1

Funções Aritméticas

Neste capítulo abordaremos as funções aritméticas: Função de Euler, Função de Möbius e a Convolução de Dirichlet. A Convolução será usada para mostrar a relação entre funções aritméticas, como a Inversa da Função Möbius, que relaciona as funções de Euler e Möbius. Este estudo está baseado no excelente livro Apostol (1976) e no livro Murty (2008).

Começaremos definindo o que é uma função Aritmética. Na teoria dos números existe uma preocupação sobre sequências de números Reais e Complexos. Chamaremos essas sequências de funções aritméticas:

Definição 1.1. *Uma função aritmética f é uma função que a cada número natural n associa um número, real ou complexo, $f(n)$. Em símbolos,*

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{R} \textit{ ou } \mathbb{C} \\ & n & \longmapsto & f(n) \end{array}$$

A seguir, apresentamos dois exemplos desse tipo de função importantes na Teoria dos Números: a função de Möbius $\mu(n)$ e a função de Euler $\varphi(n)$.

1.1 Função de Möbius

A função de Möbius $\mu : \mathbb{N} \to \mathbb{R}$ é definida da seguinte maneira:

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^k, & \text{se } n \text{ é produto de } k \text{ primos distintos} \\ 0, & \text{para os demais casos} \end{cases}$$

Assim, se $n = p_1 p_2 \cdots p_k$ com $p_1, p_2, \cdots, p_k$ números primos distintos, então $\mu(n) = (-1)^k$. Já se na decomposição do número n, ocorre uma potência de primo maior ou igual a 2, então o valor da função de Möbius nesse caso será 0. Por exemplo, veja a tabela 1.1

Tabela 1.1: Valores para $\mu(n)$

n	1	2	3	5	6	8	9	10	30
$\mu(n)$	1	-1	-1	-1	1	0	0	1	-1

pois

$$\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$$
$$\mu(8) = \mu(2^3) = 0$$
$$\mu(9) = \mu(3^2) = 0$$
$$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1$$
$$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$$

A função de Möbius está presente em diversas áreas da Teoria dos Números. Uma delas é a propriedade da somatória $\sum_{d|n} \mu(d)$, tomada sobre os divisores $d \in \mathbb{N}$ de $n \in \mathbb{N}$. Denotamos por $[x]$ o maior inteiro menor ou igual a x, isto é,

$$[x] = \max\{n \in \mathbb{Z} : n \leq x\}.$$

Assim,

$$
\begin{aligned}
[\pi] &= 3 \\
[\sqrt{50}] &= 7 \\
[1-\sqrt{5}] &= -2
\end{aligned}
$$

O teorema a seguir nos diz que ao somarmos todos os valores de $\mu(d)$, sendo d divisor de n, teremos um total que dará 1 se $n = 1$ e 0 para $n \geq 2$. Usando a função menor inteiro, podemos denotar isso como $\left[\dfrac{1}{n}\right]$. Para sua demonstração, recordemos a fórmula de Newton:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k, \quad \text{para } n \in \mathbb{N}$$

Estamos prontos para provar o:

Teorema 1.1. *Se $n \geq 1$, então*

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & se \quad n = 1 \\ 0 & se \quad n > 1 \end{cases}$$

Demonstração. Para $n = 1$ a propriedade é claramente verdadeira. Para $n > 1$, lembrando que $\mu(n) = 0$ sempre que $n = p_1^{a_1} \cdots p_k^{a_k}$ e $a_i \geq 2$ para algum $i = 1, 2, \cdots, k$. Isso significa que na somatória os únicos valores, não nulos, são para $d = 1$ e para os divisores de n formados por distintos fatores primos, com no máximo expoente 1. Sendo assim, usaremos apenas os divisores com expoentes de cada fator primo: $a_1 = \cdots = a_k = 1$. Daí, observando que a escolha de m primos do conjunto $\{p_1, p_2, \cdots, p_k\}$ é dada por $\binom{k}{m}$, temos que

$$
\begin{aligned}
\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k) \\
&\quad + \mu(p_1 p_2 p_3) + \cdots + \mu(p_1 p_2 \cdots p_k) \\
&= 1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \binom{k}{3}(-1)^3 + \cdots + \binom{k}{k}(-1)^k \\
&= (1-1)^k = 0
\end{aligned}
$$

onde usamos a fórmula do binômio de Newton na última passagem. Isso encerra a demonstração. □

1.2 A Função de Euler

Sendo $n \geq 1$, a função de Euler $\varphi(n)$ é definida como sendo a quantidade de números, não maiores que n, que sejam primos com n. Em símbolos:

$$\varphi(n) = \#\{k \in \mathbb{N} : k \leq n \text{ e } \operatorname{mdc}(k, n) = 1\} \tag{1.1}$$

Assim, a função de Euler faz a contagem de números (cardinalidade) que são coprimos com n. Os coprimos com n são os k números que possuem máximo divisor comum (mdc) iguais a 1. Na tabela 1.2, temos alguns valores para $\varphi(n)$.

Tabela 1.2: Valores para $\varphi(n)$

n	1	2	4	5	8	10
$\varphi(n)$	1	1	2	4	4	4

$\varphi(12) = 4$ pois os coprimos de 12 são 1, 5, 7 e 11.
$\varphi(15) = 8$ pois os coprimos com 15 são 1, 2, 4, 7, 8, 11, 13 e 14.
$\varphi(7) = 6$ pois 1, 2, 3, 4, 5 e 6 são coprimos com 7. Como 7 é número primo, todos os números menores que ele serão primos com 7. Dessa maneira já podemos pensar em:

$$\varphi(p) = p - 1, \text{ se } p \text{ é primo.}$$

Seguindo o mesmo tipo de somatória da função Möbius, também temos uma fórmula para a soma sobre os divisores de n para a função φ:

Teorema 1.2. *Se $n \geq 1$, então*

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

Antes de demonstrar esse resultado, vamos fazer algumas considerações. Aqui temos o somatório de $\varphi(d)$, apenas os d que dividem n, dando como resultado o próprio n. Vejamos como funciona esse teorema para $n = 30$. Os divisores de 30 são $1, 2, 3, 5, 6, 10, 15, 30$. Da definição da função de Euler, temos que Assim, pela tabela 1.3, temos que

Tabela 1.3: Valores de $\varphi(d)$, para os divisores d de 30

d	1	2	3	5	6	10	15	30
$\varphi(d)$	1	1	2	4	2	4	8	8

$$\sum_{d|30} \varphi(d) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$$

Para cada divisor d de 30, vamos denotar $q_d = 30/d$. Observamos que o número de elementos q_d é o mesmo que o número de elementos de d. Isso significa que eles percorrem os mesmos números com $1 \leq q \leq n$ em $\varphi(q)$. Explicitamente temos, conforme a tabela 1.4 a seguir.

Tabela 1.4: Valores de $\varphi(q)$, com $q = 30/d$ e d divisor de 30

d	1	2	3	5	6	10	15	30
$q = 30/d$	30	15	10	6	5	3	2	1

Com isso podemos ver que a soma de $\varphi(d)$ é igual a soma $\varphi(q)$, com $qd = 30$.

Demonstração do Teorema 1.2. Chamaremos de S o conjunto dos números menores que ou igual a n, $S = \{1, 2, \cdots, n\}$. Vamos distribuir os elementos de S em conjuntos disjuntos. Para isso, definimos o conjunto

$$A(d) = \{k \in S : \text{mdc}(k, n) = d\}.$$

O conjunto $A(d)$ é formado por todos os elementos de S tais que o mdc com n é igual a d. Os conjuntos $A(d)$ são disjuntos dois a dois, isto é $A(d_1) \cap A(d_2) = \emptyset$ para $d_1 \neq d_2$, e sua união é o conjunto S. Denotando por $f(d)$ o número de elementos de $A(d)$, temos que

$$\sum_{d|n} f(d) = n \tag{1.2}$$

Mas $\text{mdc}(k, n) = d$ se, e somente se $\text{mdc}(k/d, n/d) = 1$ e $0 \leq k \leq n$ se, e somente se $0 \leq k/d \leq n/d$. Fazendo agora $q = k/d$, temos uma correspondência de elementos um à um dos elementos de $A(d)$ e com os inteiros q satisfazendo $0 < q \leq n/d$, tais que $\text{mdc}(q, n/d) = 1$. Relembre que a quantidade de q que são primos com n/d é $\varphi(n/d)$.

Consequentemente temos $f(d) = \varphi(n/d)$ e substituindo em (1.2) , obtemos:

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

que é equivalente a dizer que

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

uma vez que d e n/d percorrem o mesmo conjunto dos divisores de n. $\square$

1.3 Relação entre as funções $\varphi(n)$ e $\mu(n)$

Teorema 1.3. *Se* $n \geq 1$, *então*

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

Demonstração. Primeiramente vamos reescrever a primeira fórmula de $\varphi(n)$ em (1.1). Dessa maneira encontramos uma nova forma de contar a quantidade de primos com n:

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{\text{mdc}(k,n)} \right]$$

Teremos valor nulo para $\text{mdc}(k,n) \neq 1$, sendo contado apenas os valores 1 para $\text{mdc}(k,n) = 1$, que possuem máximo divisor comum $\text{mdc}(k,n) = 1$. Essa escrita permite que k percorra todos os inteiros $\leq n$. Vamos aplicar o Teorema 1.1 substituindo o n por $\text{mdc}(k,n)$:

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|\text{mdc}(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|k \\ d|n}} \mu(d)$$

Fixado um d, divisor de n, devemos somar todos os k inteiros no intervalo $1 \leq k \leq n$, que são múltiplos com d. Sendo assim podemos escrever $k = qd$, então temos $1 \leq k \leq n$ se e somente se $1 \leq q \leq n/d$. Consequentemente a somatória em n pode ser reescrita:

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}$$

Como queríamos provar.

□

Teorema 1.4. *Se $n > 1$, então*

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right) \tag{1.3}$$

Demonstração. Sendo $n > 1$, chamaremos de $p_1, p_2, \cdots, p_r$ os divisores primos de n. Reescrevendo o produto e usando a distributiva nos diversos fatores, obtemos:

$$\begin{aligned}\prod_{p|n}\left(1 - \frac{1}{p}\right) &= \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \sum \frac{(-1)^r}{p_1 p_2 \cdots p_r}\end{aligned} \tag{1.4}$$

À direita de (1.4), os termos como $\sum \frac{1}{p_i p_j p_k}$ entende-se que foi considerado todos os possíveis produtos de $p_i p_j p_k$ de distintos fatores primos de n escolhidos três de cada vez. Da mesma forma para os de 4 primos, 5 primos, etc. Podemos notar que cada termo à direita de (1.4) é da forma $\pm 1/d$, na qual d é um divisor de n e possui valor 1 ou é um produto de divisores de n (produto de primos distintos). O numerador ± 1 é exatamente d . Uma vez que $d = 0$ para algum d divisível por um quadrado de p_i, podemos ver que a somatória em acima é igual ao que temos no Teorema 1.3

$$\sum_{d|n} \frac{\mu(d)}{d},$$

e isto prova o teorema.

□

Propriedades da função aritmética $\varphi(n)$ podem ser deduzidas a partir do Teorema 1.4. Mostraremos algumas aplicações no teorema seguinte:

Teorema 1.5. *A função $\varphi(n)$ de Euler possui as seguintes propriedades:*

a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1}$ *para todo primo p e $\alpha \geq 1$*

b) $\varphi(m \cdot n) = \dfrac{\varphi(n) \cdot \varphi(m) \cdot d}{\varphi(d)}$ *sendo $d = \mathrm{mdc}(m, n)$*

c) $\varphi(m \cdot n) = \varphi(n) \cdot \varphi(m)$ *se* $\mathrm{mdc}(m, n) = 1$

d) $a \mid b$ *implica* $\varphi(a) \mid \varphi(b)$

Demonstração. A parte a) é imediata, bastando tomar $n = p^{\alpha}$ em (1.3). Para provar, podemos notar que cada divisor primo de mn é divisor primo de m ou de n, e aqueles primos que dividem ambos, m e n, também dividem $\mathrm{mdc}(m, n)$. Em consequência disso e de que $\mathrm{mdc}(m, n) = d$, temos pelo Teorema 1.4

$$\frac{\varphi(mn)}{mn} = \prod_{p \mid mn} \left(1 - \frac{1}{p}\right) = \frac{\displaystyle\prod_{p \mid m} \left(1 - \frac{1}{p}\right) \prod_{p \mid n} \left(1 - \frac{1}{p}\right)}{\displaystyle\prod_{p \mid \mathrm{mdc}(m,n)} \left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m} \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}}$$

$\square$

Dessa maneira chegamos a b). A parte c) é um caso especial de b) para $\mathrm{mdc}(m, n) = 1$. Agora iremos deduzir d) a partir de b). Como $a \mid b$, temos $b = ac$, em que $1 \leq c \leq b$. Se $c = b$, $a = 1$ e d) é satisfeita. Assim iremos assumir $c < b$. Por b), sendo $d = \mathrm{mdc}(a, c)$ temos:

$$\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(a)\frac{\varphi(c)}{\varphi(d)} \tag{1.5}$$

Agora o resultado segue por indução em b. Para $b = 1$, o resultado é imediato. Suponha que a propriedade d) seja válida para todos os inteiros menores do que b. Então ela é válida para c, dessa forma $\varphi(d) \mid \varphi(c)$ desde que $d \mid c$. Consequentemente o membro à direita de (1.5) é um múltiplo de $\varphi(a)$, pois $\varphi(b) = d\varphi(a)t = \varphi(a)dt$, com t inteiro. Isso significa que $\varphi(a) \mid \varphi(b)$. Isso nos prova d).

1.4 O produto de Dirichlet para Funções Aritméticas

No Teorema 1.3 foi provado que

$$\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$$

A somatória à direita ocorre frequentemente em Teoria dos Números. Essas somas tem a forma:

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Na qual f e g são funções aritméticas. É proveitoso estudarmos algumas propriedades em que essas somas possuem em comum. Essas propriedades ocorrem naturalmente na teoria das Séries de Dirichlet. É proveitoso tratarmos essas somatórias como um novo tipo de multiplicação de funções aritméticas. Um ponto de vista trazido por E.T. Bell em 1915.

Definição 1.2. *Se f e g são duas funções aritméticas, definiremos o produto de Dirichlet (ou Convolução) dessas funções como sendo a função h dada pela equação:*

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Usaremos a notação $f * g$ para h e $(f * g)(n)$ para $h(n)$. Denotamos por N a função em que $N(n) = n$ para todo $n \in \mathbb{N}$. O Teorema 1.3 seria escrito desta forma:

$$\varphi = \mu * N$$

Veremos as propriedades algébricas do produto de Dirichlet neste próximo teorema.

Teorema 1.6. *A multiplicação de Dirichlet é comutativa e associativa, isto é, para qualquer função aritmética f, g e k, temos:*

a) $f * g = g * f$ (lei da comutatividade)

b) $(f * g) * k = f * (g * k)$ (lei da associatividade)

Demonstração. Primeiro iremos reescrever a definição $f * g$ da seguinte maneira:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

de forma que a, b variam entre todos os inteiros positivos em que o produto seja n. Dessa forma, como a multiplicação e a soma são comutativa nos inteiros, a lei da comutatividade em Dirichlet está provada. Para a Lei da Associatividade faremos $A = g*k$ e consideremos

$$f * A = f * (g * k)$$

$$(f * A)(n) = \sum_{ad=n} f(a)A(d) = \sum_{ad=n} f(a) \sum_{bc=d} g(b)k(c) = \sum_{abc=n} f(a)g(b)k(c)$$

Se fizermos $B = f * g$ e considerarmos $B * k$ chegaremos ao mesmo resultado:

$$(B * k)(n) = \sum_{dc=n} B(d)k(c) = \sum_{ab=d} f(a)g(b) \sum_{cd=n} k(c) = \sum_{abc=n} f(a)g(b)k(c)$$

Como podemos ver $f{*}A = B{*}k$. Isso prova a associatividade no produto de Dirichlet. □

Agora veremos que no Produto de Dirichlet temos o elemento Identidade.

Definição 1.3. *A função aritmética I, chamada de função identidade, é definida por*

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1, & se\ n = 1 \\ 0, & se\ n > 1 \end{cases}$$

Teorema 1.7. *Para toda função aritmética f, temos $f * I = I * f = f$.*

Demonstração. Utilizando o Produto de Dirichlet temos:

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = f(n)$$

Pois $I(d/n) = 0$ para $d < n$ e $I(n/n) = I(1) = 1$. Isso termina a demonstração.

□

1.5 A inversa de Dirichlet e a fórmula da Inversa de Möbius

Nesta seção iremos estudar as inversas de funções aritméticas no sentido do Produto de Dirichlet.

Teorema 1.8. *Se f é uma função aritmética, com $f(1) \neq 0$, então existe uma única função aritmética f^{-1}, chamada inversa de Dirichlet de f, tal que:*

$$f * f^{-1} = f^{-1} * f = I$$

Ainda mais, f^{-1} é dada pela fórmula recursiva

$$f^{-1}(1) = \frac{1}{f(1)} \quad e \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d), \forall n > 1$$

Demonstração. Dada f, devemos mostrar que a equação $f*f^{-1}(n) = I(n)$ tem uma única solução para os valores de $f^{-1}(n)$. Para $n = 1$ temos de resolver a equação $f*f^{-1}(1) = I(1)$ que se reduz a

$$f(1)f^{-1}(1) = 1$$

Como $f(1) \neq 0$, temos uma única solução cujo resultado é $f^{-1}(1) = 1/f(1)$. Suponha agora que os valores da função $f^{-1}(k)$ foram determinadas de maneira única para todo $k < n$. Então devemos solucionar a equação

$$f * f^{-1}(n) = I(n)$$

Escrevendo de outra forma, devemos resolver:

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

Teremos a fórmula da inversa escrita para todo n ao fazer $n = d$:

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

Se os valores de $f^{-1}(d)$ são conhecidos para todos os divisores $d < n$, existem valores únicos de $f^{-1}(n)$ escritos da forma:

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

desde que $f(1) \neq 0$. Isso estabelece a existência e unicidade de f^{-1} por indução. □

Os resultados anteriores está resumido no corolário seguinte.

Corolário 1.9. *O conjunto $\mathcal{A} = \{f : f$ é uma função aritmética com $f(1) \neq 0\}$ é um grupo comutativo com o produto de Dirichlet.*

Definição 1.4. *Definimos a função aritmética unidade como sendo $u(n)$, de maneira que $u(n) = 1$ para todo $n \in \mathbb{N}$.*

Com essa definição, podemos reescrever o Teorema 1.1 na notação de Dirichlet:

$$\sum_{d|n} \mu(d) = I(n) \Leftrightarrow \mu * u = I.$$

Assim as funções μ e u são inversas no sentido de Dirichlet, ou seja, $\mu = u^{-1}$ e $u = \mu^{-1}$.

Vamos usar as inversas escritas anteriormente para demonstrar com mais agilidade o próximo teorema:

Teorema 1.10 (A fórmula da inversa de Möbius:)**.** *Se*

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

então

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

Além disso, vale a recíproca.

Demonstração. Com a unidade u, podemos escrever $f = g * u$. Multiplicando ambos os lados dessa equação por μ e usando as propriedades da convolução, temos

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g,$$

donde segue uma implicação. Para a recíproca, basta multiplicar $g = f * \mu$ por u e proceder de modo análogo. $\square$

Uma aplicação dessa fórmula que acabamos de demonstrar é apresentado no próximo teorema. Antes precisaremos da definição seguinte.

Definição 1.5. *Definimos a função Mangoldt pela fórmula*

$$\Lambda(n) = \begin{cases} \log p, & se\ n = p^k,\ para\ algum\ primo\ p\ e\ k \geq 1 \\ 0, & caso\ contrário. \end{cases}$$

Teorema 1.11. *Se $n \geq 1$, então*

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

Demonstração. Escrevendo a fatoração de n, temos que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

segue que

$$\log n = \sum_{i=1}^{k} \alpha_i \log p_i = \sum_{d|n} \Lambda(n).$$

Pela teorema anterior (fórmula da inversa de Möbius), obtemos

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d}.$$

Como $\log \frac{n}{d} = \log n - \log d$, temos:

$$\sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d,$$

desde que $\sum_{d|n} \mu(d) = 0$ se $n > 1$ e $\log 1 = 0$. □

Com as propriedades da função unidade e identidade, concluímos o estudo sobre a convolução de Dirichlet. Esse conhecimento será acrescido às funções de Chebyshev, que estudaremos no próximo capítulo.

Capítulo 2

Resultados da Teoria Analítica dos Números

Neste capítulo apresentamos vários resultados muito utilizados em Teoria Analítica dos Números, essenciais para familiarizar o leitor com as notações, simbologia e ferramentas próprias desse estudo.

As funções de Chebyshev fazem parte do rol usual para tratar o Teorema dos Números Primos (TPN), aparecendo naturalmente. Também estudamos a fórmula de Abel, que é usada para obter identidades assintóticas para função aritméticas. Como consequência dessas ferramentas, relacionamos alguns resultados equivalente ao Teorema dos Números Primos. Uma identidade devido a Selberg é provada, sendo a chave da primeira demonstração elementar do TNP, dada em 1949, que contou com a colaboração de Paul Erdös.

2.1 Funções de Chebyshev $\psi(x)$ e $\vartheta(x)$

Nessa seção, desenvolvemos resultados que serão usados na demonstração do TNP, seguindo variações das ideias de Selberg e Erdös e que podem ser encontradas no livro do Apostol. No entanto, convém observar que as fórmulas apresentadas aqui são interessantes por si mesmas, como por exemplo a identidade de Abel e o Teorema de Shapiro e várias de suas consequências.

Definição 2.1. *Para $x > 0$, definimos a função ψ de Chebyshev pela fórmula*

$$\psi(x) = \sum_{n \leq x} \Lambda(n)$$

Como $\Lambda(n) = 0$ para qualquer número n que não seja potência de primo, podemos reescrever a definição de ψ da seguinte maneira:

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \sum_{p} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p$$

A soma sobre m é na verdade finita. Para ver isso, notamos que a soma sobre p é vazia se $x^{1/m} < 2$, ou seja, se $m > \log_2 x$. Assim, podemos escrever

$$\psi(x) = \sum_{m \leq \log_2 x} \sum_{p \leq x^{1/m}} \log p$$

Essa função pode ser escrita de outro modo, a partir de outra função definida por Chebyshev.

Definição 2.2. *Para $x > 0$, definimos a função ϑ de Chebyshev pela fórmula*

$$\vartheta(x) = \sum_{p \leq x} \log p$$

onde p varia no conjunto dos números primos menores ou igual a x.

A última fórmula para $\psi(x)$ assume a forma

$$\psi(x) = \sum_{m \leq \log_2 x} \vartheta(x^{1/m}) \tag{2.1}$$

O próximo resultado relaciona os quocientes $\psi(x)/x$ e $\vartheta(x)/x$.

Teorema 2.1. *Para $x > 0$, temos que*

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x} \log 2}$$

Demonstração. Da expressão (2.1), segue que

$$0 \leq \psi(x) - \vartheta(x) = \sum_{2 \leq m \leq \log_2 x} \vartheta(x^{1/m})$$

Além disso, pela definição de $\vartheta(x)$, temos imediatamente a desigualdade

$$\vartheta(x) \leq \sum_{p \leq x} \log x \leq x \log x$$

Assim,

$$\begin{aligned} 0 \leq \psi(x) - \vartheta(x) &\leq \sum_{2 \leq m \leq \log_2 x} x^{1/m} \log(x^{1/m}) \leq (\log_2 x)\sqrt{x} \log \sqrt{x} \\ &= \frac{\log x}{\log 2} \cdot \frac{\sqrt{x}}{2} \log x = \frac{\sqrt{x}(\log x)^2}{2 \log 2} \end{aligned}$$

Dividindo essa desigualdade por x, segue o teorema. □

2.2 Notação Assintótica

Definição 2.3. *Se $g(x) > 0$ para todo $x \geq a$, escrevemos*

$$f(x) = O(g(x)) \quad \textit{leia-se: } f(x) \textit{ é ó grande de } g(x)$$

no sentido de que o quociente $f(x)/g(x)$ é limitado para $x \geq a$, isto é, existe uma constante $M > 0$ tal que

$$|f(x)| \leq Mg(x) \quad \textit{para todo } x \geq a$$

Por exemplo, temos que

$$x^2 = O(x^3), \quad x^n = O(e^x), \forall n \in \mathbb{N} \quad \text{e} \quad \log x = O(x).$$

É importante observar que $f(x) = O(g(x))$ não implica em geral que $g(x) = O(f(x))$. Por exemplo, $x^2 = O(x^3)$, mas não é verdade que $x^3 = O(x^2)$, pois $x^3/x^2 = x$ não é limitada.

Temos ainda que vale a transitividade nessa notação, ou seja $f(x) = O(g(x))$ e $g(x) = O(h(x))$, então $f(x) = O(h(x))$. Outra fato é que se $f_1(x) = O(g(h))$ e $f_2(x) =$

$O(g(x))$, então $f_1(x) + f_2(x) = O(g(x))$.

Definição 2.4. *Se*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

dizemos que $f(x)$ é assintótico a $g(x)$ quando $x \to \infty$ e também denotamos isso por

$$f(x) \sim g(x) \quad \textit{quando} \quad x \to \infty.$$

Como exemplo, temos que

$$x^2 + x + 1 \sim x^2 \quad \text{quando} \quad x \to \infty \quad \textit{pois} \quad \lim_{x\to\infty} \frac{x^2 + x + 1}{x^2} = 1$$

Definição 2.5. *Se ocorrer que*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0,$$

denotaremos esse fato por $f(x) = o(g(x))$.

Por exemplo, $\log(x) = o(x)$, pois $\lim_{x\to\infty} \dfrac{\log x}{x} = 0$.

2.3 Relações entre $\vartheta(x)$ e $\pi(x)$

Nessa seção vamos deduzir duas fórmulas relacionando $\vartheta(x)$ e $\pi(x)$. Elas serão usadas para concluir que o Teorema dos Números Primos é equivalente a provar que

$$\lim_{n\to\infty} \frac{\vartheta(x)}{x} = 1$$

Para alcançar nosso objetivo, iremos usar a identidade de Abel, lema de Abel. Esse importante resultado relaciona uma soma discreta com uma integral, permitindo-nos obter fórmulas assintóticas usando técnicas de integração, ou seja, com auxílio da Análise Matemática, ou simplesmente o Cálculo. Convém lembrar o Teorema Fundamental do Cálculo (TFC): Se f é $C^1[a, b]$, então

$$\int_a^b f'(t)dt = f(b) - f(a),$$

que será usando demonstração da identidade de Abel.

Teorema 2.2 (Identidade de Abel)**.** *Seja* $a(n)$ *uma função aritmética e defina* $A(x) = \sum_{n \leq x} a(n)$*. Dada* $f \in C^1[y,x]$*, temos que vale a fórmula:*

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt \tag{2.2}$$

Demonstração. Denotemos por $k = [x]$ e $m = [y]$. Pela definição da função A, temos que $A(k) = A(x)$ e $A(m) = A(y)$. Observando que $a(n) = A(n) - A(n-1)$, segue que

$$\begin{aligned}
\sum_{y<n\leq x} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} [A(n) - A(n-1)]f(n) \\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m+1}^{k} A(n-1)f(n) \\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)
\end{aligned}$$

Reindexando o segundo somatório, temos

$$\sum_{y<n\leq x} a(n)f(n) = \sum_{n=m+1}^{k-1} A(n)[f(n) - f(n+1)] + A(k)f(k) - A(m)f(m+1)$$

Usando o Teorema Fundamental do Cálculo e propriedade da integral para funcões contínuas por partes, temos

$$\begin{aligned}
\sum_{y<n\leq x} a(n)f(n) &= -\sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\int_{m+1}^{k} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1)
\end{aligned}$$

Desde que $m \leq y < m+1 < k \leq x$, usando uma propriedade da integral, obtemos

$$\begin{aligned}\int_y^x A(t)f'(t)dt &= \int_y^{m+1} A(t)f'(t)dt + \int_{m+1}^k A(t)f'(t)dt + \int_k^x A(t)f'(t)dt \\ &= A(m)f(m+1) - A(m)f(y) + \int_{m+1}^k A(t)f'(t)dt + A(k)f(x) - A(k)f(k) \\ &= A(m)f(m+1) - A(y)f(y) + \int_{m+1}^k A(t)f'(t)dt + A(x)f(x) - A(k)f(k)\end{aligned}$$

e nessa última equação foi usado que $A(k) = A(x)$, $A(m) = A(y)$. Esta última identidade implica diretamente no teorema e concluímos a demonstração. □

Corolário 2.3. *Com as mesmas notações do teorema anterior e com $f \in C^1[1, x]$, temos que vale a fórmula:*

$$\sum_{n \leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt \tag{2.3}$$

A partir da Identidade de Abel, podemos expressar $\vartheta(x)$ e $\pi(x)$ em termos de integrais.

Teorema 2.4. *Se $x \geq 1$, então*

a) $\displaystyle\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$, *onde* $\displaystyle\gamma = \lim_{x \to \infty} \left(\sum_{n \leq x} \frac{1}{n} - \log x\right) \approx 0,57721$

b) $\displaystyle\sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \gamma(s) + O\left(x^{-s}\right) \quad s > 0, s \neq 1$

onde $\gamma(s)$ é uma constante que depende de s e não de x.

Demonstração. Vamos provar apenas o item a), sendo b) análogo. Para $f(x) = 1/x$ e $a(n) = 1$ no Corolário 2.3, e notando que $A(x) = [x]$, temos que

$$\sum_{n \leq x} \frac{1}{n} = [x]\frac{1}{x} + \int_1^x \frac{[t]}{t^2}dt$$

Escrevendo $[x] = x + \{x\}$, sendo $\{x\}$ a parte fracionária de x, obtemos

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n} &= \frac{x+\{x\}}{x} + \int_1^x \frac{t+\{t\}}{t^2}dt \\ &= 1 + \frac{\{x\}}{x} + \int_1^x \frac{1}{t} + \int_1^x \frac{\{t\}}{t^2}dt \\ &= \log x + 1 + \int_1^\infty \frac{\{t\}}{t^2}dt + \frac{\{x\}}{x} - \int_x^\infty \frac{\{t\}}{t^2}dt.\end{aligned}$$

A integral imprópria $\displaystyle\int_1^\infty \{t\}/t^2 dt$ existe, desde que é dominada por $\displaystyle\int_1^\infty 1/t^2 dt$. Temos ainda que

$$0 \leq \int_x^\infty \frac{\{t\}}{t^2}dt \leq \int_x^\infty \frac{1}{t^2} = -\frac{1}{t}\bigg|_x^\infty = \frac{1}{x}$$

Desse modo, podemos escrever

$$\frac{\{x\}}{x} - \int_x^\infty \frac{\{t\}}{t^2} = O\left(\frac{1}{x}\right) \text{ e } \gamma = 1 + \int_1^\infty \frac{\{t\}}{t^2}dt,$$

sendo γ chamada de constante de Euler-Mascheroni. Daí, com essas considerações, segue que

$$\sum_{n\leq x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right).$$

Finalmente, isolando γ e tomando o limite quando $x \to \infty$, concluímos o resultado. □

Nosso próximo resultado relaciona as funções $\vartheta(x)$ e $\pi(x)$.

Teorema 2.5. *Para $x \geq 2$, temos que*

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt \tag{2.4}$$

e

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt \tag{2.5}$$

Demonstração. Primeiramente considere a função a definida da seguinte maneira: $a(n) = 1$ se n é primo e $a(n) = 0$ caso contrário. Essa é a função característica do conjunto dos primos. Isso nos permite escrever:

$$\pi(x) = \sum_{p\leq x} 1 = \sum_{n\leq x} a(n) \quad \text{e} \quad \vartheta(x) = \sum_{p\leq x}\log p = \sum_{n\leq x} a(n)\log n$$

Agora fazendo $f(x) = \log x$ na identidade de Abel, obtemos

$$\vartheta(x) = \sum_{n \le x} a(n) \log n = \pi(x) \log x - \int_1^x \frac{\pi(t)}{t} dt$$

que comprova (2.4), desde que $\pi(t) = 0$ para $t < 2$. Para a outra identidade, vamos considerar $b(n) = a(n) \log n$ e assim, temos

$$\pi(x) = \sum_{3/2 < n \le x} b(n) \frac{1}{\log n} \quad \text{e} \quad \vartheta(x) = \sum_{n \le x} b(n)$$

Tomando $f(x) = 1/\log x$ na identidade de Abel, com $y = 3/2$, concluímos que

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\vartheta(t)}{t \log^2 t} dt$$

que implica em (2.5) desde que $\vartheta(t) = 0$ pra $t < 2$. □

2.4 Proposições Equivalentes do Teorema dos Números Primos

Teorema 2.6. *As seguintes relações são logicamente equivalentes:*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1 \tag{2.6}$$

$$\lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1 \tag{2.7}$$

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \tag{2.8}$$

Demonstração. A equivalência entre (2.7) e (2.8) é consequência do Teorema 2.1. Basta então provar a equivalência entre (2.6) e (2.7). Da equação (2.4), obtemos

$$\frac{\vartheta(x)}{x} = \frac{\pi(x) \log x}{x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt \tag{2.9}$$

Supondo a validade de (2.6), temos que $\pi(t)/t = O(1/\log t)$, e assim,

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right)$$

Além disso,

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log \sqrt{x}}$$

O que implica em

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{dt}{\log t} = 0$$

Esse fato, juntamente com a equação (2.9) implica em (2.7). Agora, assumindo (2.7), temos pelo Teorema 2.1 que

$$\frac{\pi(x)\log x}{x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$$

Desse modo, para obtermos (2.6), é suficiente mostrar que

$$\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt = 0 \tag{2.10}$$

Como estamos assumindo (2.7), é imediato que $\vartheta(t) = O(t)$ e por consequência,

$$\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right)$$

No entanto,

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}}$$

que implica em

$$\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}dt = 0,$$

comprovando (2.10). Portanto, (2.7) implica em (2.6) . □

2.5 Teorema de Shapiro e Aplicações

Nessa seção, tratamos de um resultado devido a Shapiro, que nos permite, a partir de identidades com a parte inteira, remover esse colchetes e obter novas identidades.

Teorema 2.7. *Seja $a(n)$ uma sequência não-negativa tal que*

$$\sum_{n\leq x} a(n)\left[\frac{x}{n}\right] = x\log x + O(x) \text{ para todo } x \geq 1 \tag{2.11}$$

Então:

a) Para $x \geq 1$, temos que

$$\sum_{n\leq x}\frac{a(n)}{n} = \log x + O(1)$$

b) Existe uma constante $B > 0$ tal que

$$\sum_{n\leq x} a(n) \leq Bx \text{ para todo } x \geq 1$$

c) Existe uma constante $A > 0$ e um $x_0 > 0$ tal que

$$\sum_{n\leq x} a(n) \geq Ax \text{ para todo } x \geq x_0$$

Demonstração. Vamos denotar

$$S(x) = \sum_{n\leq x} a(n) \quad \text{e} \quad T(x) = \sum_{n\leq x} a(n)\left[\frac{x}{n}\right]$$

Inicialmente, provaremos b). Para isso, vamos provar a validade da seguinte desigualdade:

$$S(x) - S\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right) \tag{2.12}$$

Temos que

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n\leq x}\left[\frac{x}{n}\right]a(n) - 2\sum_{n\leq x/2}\left[\frac{x}{2n}\right]a(n) \\ &= \sum_{n\leq x/2}\left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right)a(n) + \sum_{x/2<n\leq x}\left[\frac{x}{n}\right]a(n) \end{aligned}$$

Desde que $[2y] - 2[y] = 0$ ou 1, a primeira somatória é não negativa, e portanto

$$T(x) - 2T\left(\frac{x}{2}\right) \geq \sum_{x/2<n\leq x}\left[\frac{x}{n}\right]a(n) \geq \sum_{x/2<n\leq x} a(n) = S(x) - S\left(\frac{x}{2}\right)$$

comprovando (2.12). Da equação (2.11), segue que

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= x\log x + O(x) - 2\left(\frac{x}{2}\log\frac{x}{2} + O(x)\right) \\ &= x\log x + O(x) - x\log x + x\log 2 = O(x) \end{aligned}$$

Daí, por (2.12), concluímos que $S(x) - S\left(\frac{x}{2}\right) = O(x)$. Isso nos permite obter uma constante $K > 0$ tal que

$$S(x) - S\left(\frac{x}{2}\right) \leq Kx \ \forall x \geq 1.$$

Aplicando essa desigualdade sucessivamente para $x/2$, $x/4$ e assim por diante, obtemos

$$\begin{aligned} S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) &\leq K\frac{x}{2} \\ S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) &\leq K\frac{x}{4}. \end{aligned}$$

Contudo, temos que $S(X/2^n) = 0$ quando $2^n > x$. Somando essas desigualdades, temos que

$$S(x) \leq K\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) \leq 2Kx,$$

ou seja, provamos *b*) com $B = 2K$. Agora vamos verificar *a*). Desde que $[x] = x + O(1)$, obtemos

$$\begin{aligned} T(x) &= \sum_{n\leq x} a(n)\left[\frac{x}{n}\right] = \sum_{n\leq x} a(n)\left(\frac{x}{n} + O(1)\right) \\ &= x\sum_{n\leq x}\frac{a(n)}{n} + O\left(\sum_{n\leq x} a(n)\right) = x\sum_{n\leq x}\frac{a(n)}{n} + O(x) \end{aligned}$$

pela parte *b*). Desse modo,

$$\sum_{n\leq x}\frac{a(n)}{n} = \frac{1}{x}T(x) + O(1) = \log x + O(1),$$

o que implica em *a*), visto que $\log x = O(x)$. Vamos estabelecer agora *c*). Para isso, considere

$$A(x) = \sum_{n\leq x}\frac{a(n)}{n}$$

Podemos reescrever $a)$ com

$$A(x) = \log x + R(x), \quad \text{com} \quad R(x) = O(1),$$

Como $R(x) = O(1)$, existe uma constante $M > 0$ tal que $|R(x)| \leq M$ para todo $x \geq 1$. Seja $\alpha \in (0,1)$ a ser especificado mais adiante e considere a diferença

$$A(x) - A(\alpha x) = \sum_{\alpha x < x \leq x} \frac{a(n)}{n}$$

Sendo $x \geq 1$ e $\alpha x \geq 1$, podemos estimar

$$\begin{aligned} A(x) - A(\alpha x) &= \log x + R(x) - \log \alpha x - R(\alpha x) \\ &\geq \log x - |R(x)| - \log \alpha - \log x - |R(\alpha x)| \\ &\geq -\log \alpha - 2M. \end{aligned}$$

Desde que $\lim\limits_{\alpha \to 0}(-\log \alpha - 2M) = +\infty$, e usando o Teorema do Valor Intermediário para a função $h(\alpha) = -\log \alpha - 2M$, concluímos que existe $\alpha \in (0,1)$ tal que $-\log \alpha - 2M = 1$ Para este α, temos a validade da desigualdade

$$A(x) - A(\alpha x) \geq 1 \quad \text{se} \quad x \geq 1/\alpha.$$

Mas

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leq x} \frac{a(n)}{n} \leq \frac{1}{\alpha x} \sum_{n \leq x} a(n) = \frac{S(x)}{\alpha x}$$

Essas duas inequações nos permitem concluir que

$$\frac{S(x)}{\alpha x} \geq 1 \quad \text{se} \quad x \geq \frac{1}{\alpha}$$

Isso prova $c)$ com $A = \alpha$ e $x_0 = 1/\alpha$. $\square$

Teorema 2.8. *Para $x \geq 2$, temos que vale a estimativa*

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x - x + O(\log x)$$

Demonstração. Pela definição da função de Mangoldt, temos que

$$\sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{m|n} \Lambda(m) = \sum_{m \leq x} \Lambda(m) \sum_{\substack{n \leq x \\ m|n}} 1 = \sum_{m \leq x} \Lambda(m) \left[\frac{x}{m}\right].$$

Usando a identidade de Abel, e observando que $[x] = x + \{x\}$, obtemos

$$\begin{aligned} \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] &= \sum_{n \leq x} \log n = [x] \log x - \int_1^x \frac{[t]}{t} dt \\ &= x \log x + \int_1^x dt + \{x\} \log x + \int_1^x \frac{\{t\}}{t} dt \\ &= x \log x - x + O(\log x) \end{aligned}$$

□

Notando que $-x + O(\log x) = O(x)$, verificamos que

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x + O(x),$$

e usando diretamente o Teorema 2.7, obtemos o seguinte resultado.

Teorema 2.9. *Para todo $x \geq 1$, temos que*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1) \tag{2.13}$$

Além disso, existem constantes positivas c_1 e c_2 tais que

$$\psi(x) \leq c_1 x \quad \textit{para todo} \quad x \geq 1$$

e

$$\psi(x) \geq c_2 x \quad \textit{para todo} \quad x \quad \textit{suficientemente grande.}$$

De modo semelhante, temos um resultado para a função $\vartheta(x)$.

Teorema 2.10. *Para todo $x \geq 1$, temos que*

$$\sum_{p \leq x} \frac{\log(p)}{p} = \log x + O(1) \tag{2.14}$$

Além disso, existem constantes positivas c_1 e c_2 tais que

$$\vartheta(x) \leq c_1 x \quad \textit{para todo} \quad x \geq 1$$

e

$$\vartheta(x) \geq c_2 x \quad \textit{para todo} \quad x \quad \textit{suficientemente grande.}$$

Demonstração. Pela definição da função de Mangoldt, e observando que $[x/n] = 0$ para $n > x$, temos que

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{p \leq x} \left[\frac{x}{p}\right] \log p + \sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right] \log p$$

Vamos provar que a segunda soma acima é $O(x)$. De fato,

$$\begin{aligned}
\sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right] \log p \leq \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right] &\leq \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \frac{x}{p^m} \\
= x \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \left(\frac{1}{p}\right)^m &= \sum_{p \leq x} \log p \frac{1}{p^2} \frac{1}{1 - 1/p} \\
x \sum_{p \leq x} \frac{\log p}{p(p-1)} \leq x \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} &= O(x)
\end{aligned}$$

onde usamos a fórmula da soma de uma progressão geométrica e a convergência da série numérica $\sum_{n=2}^{\infty} \log n / n(n-1)$ (basta observar que o termo $\log n / n(n-1)$ é dominado por $1/n^{3/2}$ para n grande e usar o teste da comparação).

Dessa forma, essas considerações e o Teorema 2.8, implicam que

$$\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] + O(x) = x \log x + O(x)$$

Seja $a(n) = 1$ se n é primo e $a(n) = 0$ se $n = 1$ ou composto, chamada de função característica dos primos. Com o auxílio dessa função e usando o Teorema 2.7, concluímos a demonstração. $\square$

Teorema 2.11. *Para todo $x \geq 1$, temos que*

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x),$$

e

$$\sum_{n \leq x} \vartheta\left(\frac{x}{n}\right) = x \log x + O(x).$$

Teorema 2.12. *Seja F uma função real ou complexa, definida sobre o intervalo $(0, \infty)$ e defina*

$$G(x) = \log x \sum_{n \leq x} F\left(\frac{x}{n}\right)$$

Então

$$F(x) \log x + \sum_{n \leq x} F\left(\frac{x}{n}\right) \Lambda(n) = \sum_{d \leq x} \mu(d) G\left(\frac{x}{d}\right)$$

Demonstração. Podemos escrever $F(x) \log x$ como uma soma:

$$F(x) \log x = \sum_{n \leq x} \left[\frac{1}{n}\right] F\left(\frac{x}{n}\right) \log \frac{x}{n} = \sum_{n \leq x} F\left(\frac{x}{n}\right) \log \frac{x}{n} \sum_{d|n} \mu(d)$$

Lembrando da fórmula

$$\Lambda(n) = \sum_{d|n} \log \frac{n}{d} \mu(d)$$

descrita no Teorema 1.11, temos que

$$\sum_{n \leq x} F\left(\frac{x}{n}\right) \Lambda(n) = \sum_{n \leq x} F\left(\frac{x}{n}\right) \log \frac{x}{n} \sum_{d|n} \mu(d)$$

Somando essas equações, obtemos

$$\begin{aligned} F(x) \log x + \sum_{n \leq x} F\left(\frac{x}{n}\right) \Lambda(n) &= \sum_{n \leq x} F\left(\frac{x}{n}\right) \sum_{d|n} \mu(d) \left(\log \frac{x}{n} + \log \frac{n}{d}\right) \\ &= \sum_{dn \leq x} \sum_{d|n} F\left(\frac{x}{n}\right) \mu(d) \log \frac{x}{d} \end{aligned}$$

Nessa última somatória, escrevemos $n = qd$ para obter

$$\sum_{d \leq x} \sum_{d|n} F\left(\frac{x}{n}\right) \mu(d) \log \frac{x}{d} = \sum_{d \leq x} \mu(d) \log \frac{x}{d} \sum_{q|n/d} F\left(\frac{x}{qd}\right) = \sum_{d \leq x} \mu(d) G\left(\frac{x}{d}\right)$$

e assim, segue o resultado. $\square$

2.6 Demonstração da Identidade de Selberg

Nesta seção iremos demonstrar uma identidade conhecida por identidade de Selberg (2.15), tendo sido publicado uma versão em 1948. Ela foi a chave para obtenção de uma demonstração elementar do TNP. Também é importante saber que o TNP implica nessa fórmula assintótica.

$$\vartheta(x)\log x + \sum_{p\leq x}\log p\ \vartheta\left(\frac{x}{p}\right) = 2x\log x + O(x) \tag{2.15}$$

Existem variações dessa identidade, tais como uma em que aparece $\psi(x)$ no lugar de $\vartheta(x)$, juntamente com a função $\Lambda(n)$.

No Teorema 2.12, tomando $F_1(x) = \psi(x)$ e $F_2(x) = x-\gamma-1$, sendo γ a constante de Euler, obtemos, respectivamente,

$$\begin{aligned} G_1(x) = \log x \sum_{n\leq x}\psi\left(\frac{x}{n}\right) &= \log x(x\log x + -x\log x + O(\log x)) \\ &= x\log^2 x - x\log x + O(\log^2 x), \end{aligned}$$

sendo usando o Teorema 2.11, e

$$\begin{aligned} G_2(x) = \log x\sum_{n\leq x}\left(\frac{x}{n}-\gamma-1\right) &= x\log x\sum_{n\leq x}\frac{1}{n} - (\gamma+1)[x]\log x \\ &= x\log x\left(\log x + \gamma + O\left(\frac{1}{x}\right)\right) - (\gamma+1)\log x(x+O(1)) \\ &= x\log^2 x + \gamma x\log x + O(\log x) - \gamma x\log x - x\log x \\ &= x\log^2 x - x\log x + O(\log x) \end{aligned}$$

Dessa forma, temos que

$$G_1(x) - G_2(x) = O(\log^2 x) = O(\sqrt{x}).$$

Agora aplicando o Teorema 2.12 para cada uma das funções F_1 e F_2 e subtraindo as equações obtidas, obtemos que o lado direito tem a seguinte estimativa:

$$\sum_{d\leq x}\mu(d)\left(G_1\left(\frac{x}{d}\right)-G_2\left(\frac{x}{d}\right)\right)=O\left(\sum_{d\leq x}\sqrt{\frac{x}{p}}\right)=O\left(\sqrt{x}\sum_{d\leq x}\frac{1}{\sqrt{d}}\right)=O(x)$$

Desse modo, temos

$$(\psi(x)-x-\gamma-1)\log x+\sum_{n\leq x}\left(\psi\left(\frac{x}{p}\right)+\frac{x}{n}\Lambda(n)+\gamma+1\right)\Lambda(n)=O(x),$$

ou ainda,

$$\psi(x)\log x+\sum_{n\leq x}\psi\left(\frac{x}{p}\right)\Lambda(n)=x\log x+(\gamma+1)\log x+x\sum_{n\leq x}\frac{\Lambda(n)}{n}+(\gamma+1)\sum_{n\leq x}\Lambda(n).$$

Usando a equação (2.13), que $\log x=O(x)$ e que $\sum\limits_{n\leq x}\Lambda(n)=\psi(x)=O(x)$, chegamos na seguinte identidade de Selberg

$$\psi(x)\log x+\sum_{n\leq x}\psi\left(\frac{x}{p}\right)\Lambda(n)=2x\log x+O(x)$$

Vamos agora provar que essa identidade implica em (2.15). Primeiramente, de (2.1), temos que $\psi(x)-\vartheta(x)=O(\sqrt{x}\log^2 x)$, e portanto

$$\psi(x)\log x=\vartheta(x)\log x+O(\sqrt{x}\log^2 x)\log x=\vartheta(x)\log x+O(\sqrt{x}\log^3 x)$$

Como $\log x\leq C\sqrt[6]{x}$ para x suficientemente grande, temos que $\sqrt{x}\log^3 x=O(\sqrt{x}\sqrt{x})=O(x)$, e isso nos dá que

$$\psi(x)\log x=\vartheta(x)\log x+O(x)$$

Para concluir o teorema, basta verificar a seguinte fórmula assintótica

$$\sum_{n\leq x}\psi\left(\frac{x}{p}\right)\Lambda(n)=\sum_{p\leq x}\vartheta\left(\frac{x}{p}\right)\log p+O(x)$$

De fato,

$$\sum_{n\leq x}\psi\left(\frac{x}{p}\right)\Lambda(n)-\sum_{p\leq x}\vartheta\left(\frac{x}{p}\right)\log p=\sum_{p\leq x}\sum_{m=2}^{\log_2 x}\vartheta\left(\frac{x}{p^m}\right)\log p$$

Desde que $\vartheta(x) = O(x)$, procedendo do mesmo modo da demonstração do Teorema 2.14, concluímos que

$$\sum_{p\leq x} \sum_{m=2}^{\log_2 x} \vartheta\left(\frac{x}{p^m}\right) \log p = O\left(\sum_{p\leq x} \sum_{m=2}^{\log_2 x} \frac{x}{p^m} \log p\right) = O(x),$$

e com isso concluímos o teorema.

Capítulo 3

Prova Elementar do Teorema dos Números Primos

> Acreditou-se durante muito tempo que métodos analíticos deviam ser empregados na demonstração do Teorema dos Números Primos. Houve grande surpresa na comunidade matemática, quando Erdös, assim como Selberg, em 1949, deram uma demonstração utilizando unicamente as estimativas elementares de certas funções aritméticas (Ribenboim (2012)).

Vamos falar mais um pouco da função $\pi(x)$, que conta os números primos que são menores ou igual a x. Em símbolos:

$$\pi(x) = \#\{p \leq x : \text{sendo } p \text{ um número primo}\}$$

Por exemplo, consultando a lista dos primos no Apêndice A, obtemos as seguintes contagens listadas na tabela 3.1:

Tabela 3.1: Alguns valores de $\pi(x)$

x	1	2	5	10	30	100	1000	10000
$\pi(x)$	0	1	3	4	10	25	168	1229

O método usual para encontrar números primos em um determinado intervalo é usar o famoso Crivo de Eratóstenes.

A função $\pi(x)$ é uma tanto irregular, ficando constante em intervalos. Sabendo que para a função $\pi(x)$ não se comporta bem, será que é possível encontrar uma função “mais regular”que seja uma boa aproximação para ela? Em outras palavras, $\pi(x) \approx f(x)$ para x suficientemente grande, para alguma função $f(x)$ conhecida? Vejamos o comportamento gráfico da função $\pi(x)$ para alguns valores de x.

O gráfico dessa função para valores abaixo de 25 é apresentado a seguir:

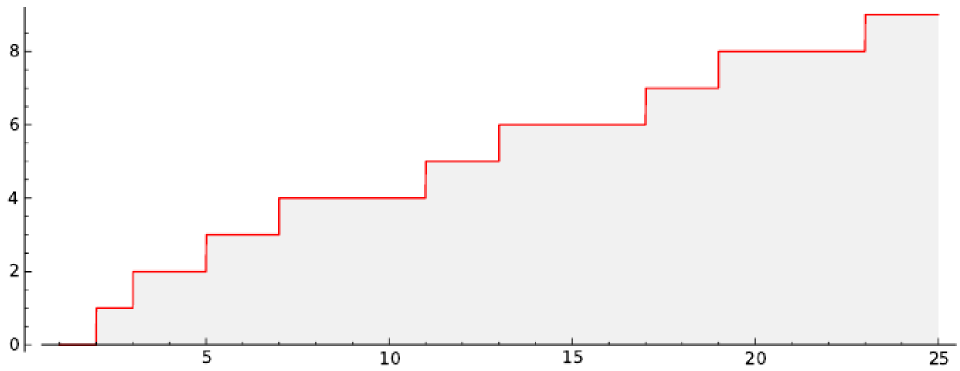


Figura 3.1: Gráfico da Função $\pi(x)$ para $x \leq 25$

Para valores abaixo de 100, o gráfico de $\pi(x)$ fica:

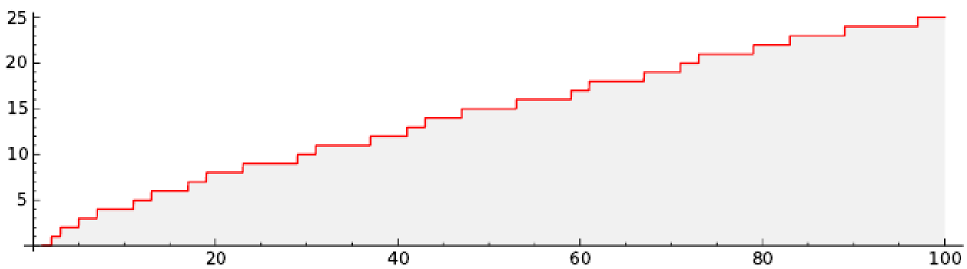


Figura 3.2: Gráfico da Função $\pi(x)$ para $x \leq 100$

Para valores abaixo de 1000 e 10000, os gráficos para $\pi(x)$ são, respectivamente:

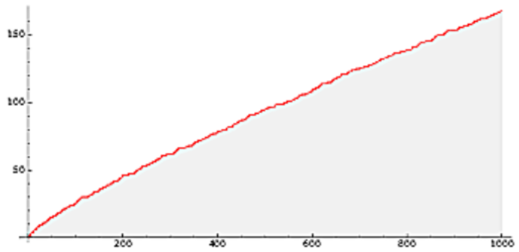


Figura 3.3: Gráfico da Função $\pi(x)$ para $x \leq 1000$

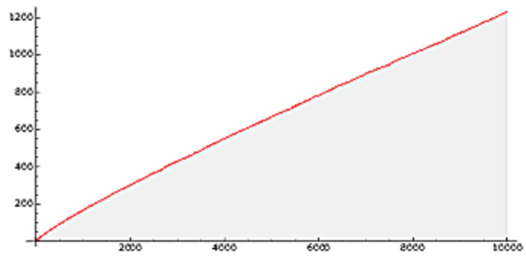
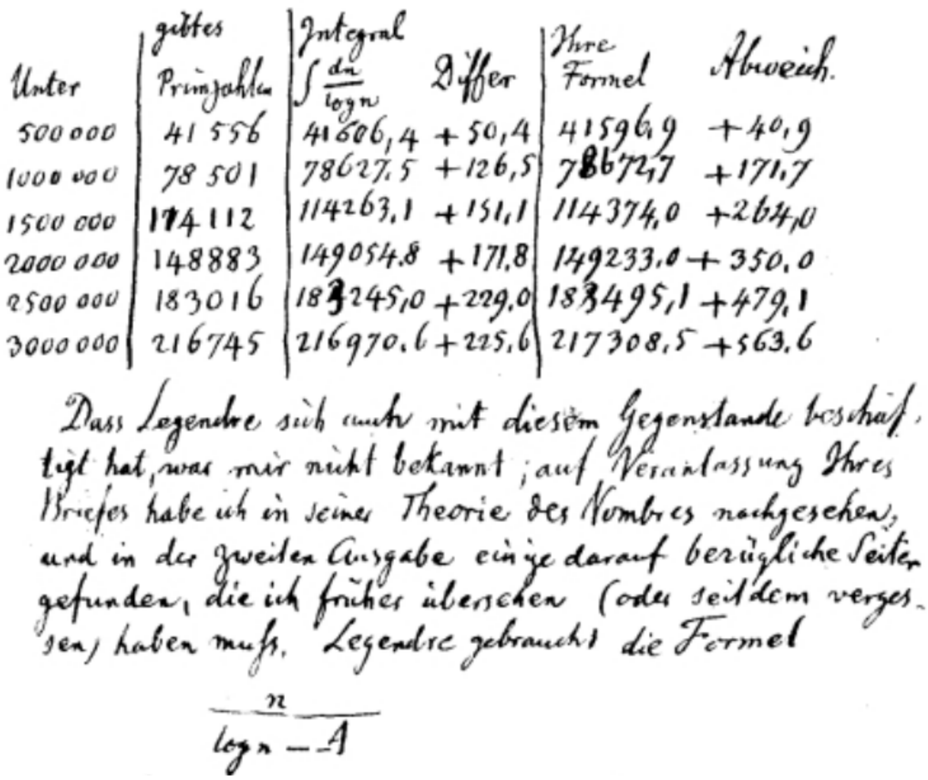


Figura 3.4: Gráfico da Função $\pi(x)$ para $x \leq 10000$

Os gráficos sugerem que a função $\pi(x)$ aparenta-se regular quando x torna-se cada vez maior. Dessa forma, faz sentido buscar uma função $f(x)$ que seja uma boa aproximação para $\pi(x)$ no sentido assintótico.

A seguir, apresentamos um trecho da uma carta de Gauss à Encke, datada de 24 de dezembro 1849.



Unter	gezählte Primzahlen	Integral $\int \frac{dn}{\log n}$	Differ	Ihre Formel	Abweich.
500000	41556	41606,4	+50,4	41596,9	+40,9
1000000	78501	78627,5	+126,5	78672,7	+171,7
1500000	114112	114263,1	+151,1	114374,0	+264,0
2000000	148883	149054,8	+171,8	149233,0	+350,0
2500000	183016	183245,0	+229,0	183495,1	+479,1
3000000	216745	216970,6	+225,6	217308,5	+563,6

Dass Legendre sich auch mit diesem Gegenstande beschäftigt hat, war mir nicht bekannt; auf Veranlassung Ihres Briefes habe ich in seiner Theorie des Nombres nachgesehen, und in der zweiten Ausgabe einige darauf bezügliche Seiten gefunden, die ich früher übersehen (oder seitdem vergessen) haben muss. Legendre gebraucht die Formel

$$\frac{n}{\log n - A}$$

Figura 3.5: Fonte: Gauss (1849)

Através dessa tabela de valores, Gauss conjecturou que para x suficientemente grande, vale

$$\pi(x) \approx \frac{x}{\log x}$$

e

$$\pi(x) \approx Li(x) := \int_2^x \frac{dt}{\log t}$$

sendo a segunda aproximação melhor.

Para se ter uma ideia dos valores produzidos por essas funções, observe a tabela 3.2

Tabela 3.2: Comparações das aproximações

x	$\pi(x)$	$x/\log x$	$Li(x)$
100	25	21,71	29,08
1000	168	144,76	176,56
10000	1229	1085,74	1245,09
100000	9592	8685,89	9628,76

Uma evidência gráfica desses comportametos assintóticos, podem ser vistos no gráfico abaixo:

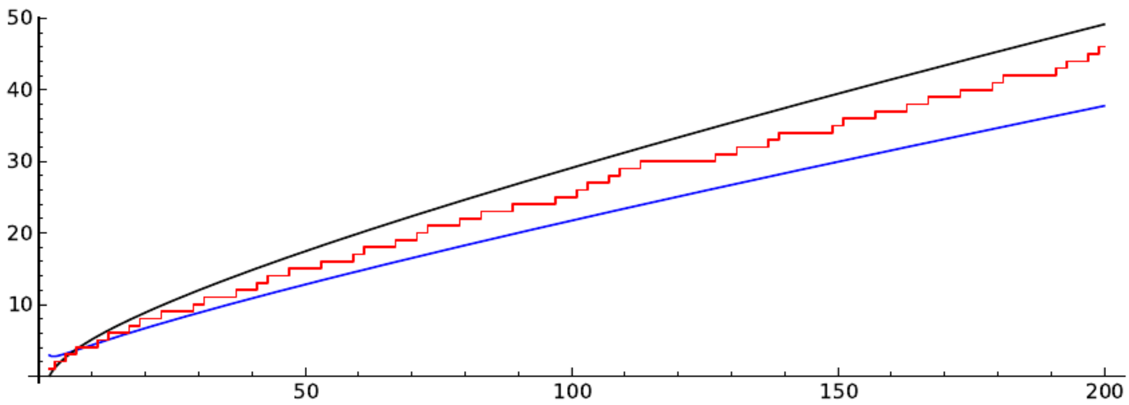


Figura 3.6: Gráficos de $Li(x)$ (topo), $\pi(x)$ (meio) e $x/\log x$ (inferior)

Estamos prontos para apresentar nesse capítulo, uma demonstração elementar do Teorema dos Números Primos, publicada por Selberg [veja Selberg (1949) e Erdös (1949)]. Como observado no Teorema 2.6, o TNP é equivalente a provar a validade do limite

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1 \tag{3.1}$$

sendo $\vartheta(x)$ a função de Chebyshev definida por

$$\vartheta(x) = \sum_{p\leq x} \log p \tag{3.2}$$

e p variando entre os números primos.

A ideia básica da demonstração é fazer uso da fórmula assintótica

$$\vartheta(x)\log x+\sum_{p\leq x}\log p\ \vartheta\left(\frac{x}{p}\right)=2x\log x+O(x) \tag{3.3}$$

Para ilustrar o uso dessa identidade, de modo informal, observamos que a fórmula (3.3) implica que

$$\frac{\vartheta(x)}{x}+\frac{1}{\log x}\sum_{p\leq x}\frac{\log p}{p}\frac{\vartheta(x/p)}{x/p}\to 2\quad\text{quando}\quad x\to\infty$$

Se tivessemos $\dfrac{\vartheta(x)}{x}\to l$ quando $x\to\infty$, e usando a identidade (2.14), o limite acima implicaria que $l+l=2$, ou seja, $l=1$. No entanto, precisamos garantir a existência de tal limite. Desse modo, vamos introduzir as seguintes notações:

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x}=a\qquad\text{e}\qquad\limsup_{x\to\infty}\frac{\vartheta(x)}{x}=A$$

Em função do Teorema 2.10, tais limites são finitos. Além disso, vale que $a\leq A$, restando provar a desigualdade oposta.

Lema 3.1. *Com as notações acima, temos que $a+A=2$.*

Demonstração. Desde que $A=\limsup\limits_{x\to\infty}\dfrac{\vartheta(x)}{x}$, podemos obter uma sequência $x_n\to\infty$ tal que $\vartheta(x_n)=Ax_n+o(x_n)$, e portanto

$$\vartheta(x_n)\log x_n=Ax_n\log x_n+o(x_n\log x_n).$$

Pela identidade de Selberg (3.3), segue que

$$\sum_{p\leq x_n}\vartheta\left(\frac{x_n}{p}\right)\log p=(2-A)x_n\log x_n+o(x_n\log x_n)$$

Fixado $\delta>0$, temos que $\vartheta\left(\dfrac{x_n}{p}\right)>(a-\delta)\dfrac{x_n}{p}$ para n sificientemente grande. Essa desigualdade e 2.14 implicam que

$$\begin{aligned}\sum_{p\leq x_n}\vartheta\left(\frac{x_n}{p}\right)\log p&\geq\sum_{p\leq x_n}(a-\delta)\frac{x_n}{p}\log p\geq(a-\delta)x_n\sum_{p\leq x_n}\frac{\log p}{p}\\&\geq(a-\delta)x_n\log x_n+o(x_n\log x_n).\end{aligned}$$

Juntando essas estimativas, vemos que para n suficientemente grande vale

$$(2-A)x_n \log x_n \geq (a-\delta)x_n \log x_n + o(x_n \log x_n)$$

Dividindo essa desigualdade por $x_n \log x_n$ e fazendo $n \to \infty$, concluímos que

$$2 - A \geq a - \delta.$$

Como δ foi tomado de modo arbitrário, podemos fazer $\delta \to 0$, obtendo

$$2 \geq a + A.$$

De modo análogo, trabalhando com uma sequência $x'_n \to \infty$ tal que $\vartheta(x'_n) = ax'_n + o(x'_n)$, segue que $2 \leq a + A$ e portanto, o lema está provado. □

O lema a aseguir também será importante na demonstração do TNP e sua demonstração será omitida.

Lema 3.2. *Fazendo $x \to \infty$ de modo que $\vartheta(x) = Ax + o(x)$. Então, para qualquer primo $p_i \leq x$, exceto para o conjunto dos primos satisfazendo*

$$\sum \frac{\log p}{p} = o(\log x) \tag{3.4}$$

nós temos que

$$\vartheta\left(\frac{x}{p_i}\right) = a\frac{x}{p_i} + o\left(\frac{x}{p_i}\right) \tag{3.5}$$

3.1 Demonstração do Teorema dos Números Primos

Primeiramente, tomando x suficiente grande, com $\vartheta(x) = ax + o(x)$, podemos deduzir de (3.3), do Lema (3.2) e do Teorema (2.14), que

$$\begin{aligned}\vartheta(x)\log x + \sum_{p\leq x} \log p \ \vartheta\left(\frac{x}{p}\right) &= (a+A)x\log x + O(x) \\ &= ax\log x + Ax\sum_{p\leq x}\frac{\log p}{p} + O(x)\end{aligned}$$

Daí,

$$(\vartheta(x) - ax)\log x + \sum_{p\leq x} \log p \left[\vartheta\left(\frac{x}{p}\right) - A\frac{x}{p}\right] = O(x). \tag{3.6}$$

Assim, podemos concluir que

$$\sum_{p\leq x} \log p \left[\vartheta\left(\frac{x}{p}\right) - A\frac{x}{p}\right] = o(x\log x). \tag{3.7}$$

Afirmamos que fixado $\delta > 0$, para x suficientemente grande, vale

$$\vartheta\left(\frac{x}{p}\right) > (A-\delta)\frac{x}{p} \tag{3.8}$$

exceto possivelmente para um conjunto S dos primos abaixo de x e satisfazendo

$$\sum_{p\in S} \frac{\log p}{p} = o(\log x).$$

De fato, se existisse algum primo $p \notin S$ satisfazendo a desigualdade oposta a (3.8), tomando p_0 como o menor desses primos, segue que

$$\begin{aligned} o(x\log x) = \sum_{p\leq x} \log p \left[\vartheta\left(\frac{x}{p}\right) - A\frac{x}{p}\right] &\leq \sum_{p\leq x, p\notin S} \log p \left[\vartheta\left(\frac{x}{p_0}\right) - A\frac{x}{p_0}\right] + o(x\log x) \\ \leq -\delta x \sum_{p\leq x, p\notin S} \frac{\log p}{p_0} + o(x\log x) &\leq \delta x \sum_{p\leq x, p\notin S} \frac{\log p}{p} = -\delta x\log x + o(x\log x). \end{aligned}$$

Isso implica que $\delta x\log x + o(x\log x) \leq 0$. Dividindo por $x\log x$ e fazendo $x\to\infty$, obtemos que $\delta \leq 0$, uma contradição.

Pelo Lema 3.2, podemos deduzir que existe um x', com $\sqrt{x} < x' < x$ satisfazendo $\vartheta(x') = Ax' + o(x')$. Agora usando (3.6), permutando a e A e substituindo x por x', deduzimos que

$$\vartheta\left(\frac{x'}{p}\right) < (a+\delta)\frac{x'}{p} \tag{3.9}$$

exceto possivelmente para o conjunto dos primos abaixo de x' e satisfazendo

$$\sum \frac{\log p}{p} = o(\log x)$$

No artigo (Erdös (1949)), Erdös mostra que é possível obter primos p e p', não pertencentes ao conjunto S, com

$$\frac{x}{p} < \frac{x'}{p'} < (1+\delta)\frac{x}{p}$$

Daí, segue de (3.8), (3.9) e da monotonicidade de $\vartheta(x)$ que

$$(A-\delta)\frac{x}{p} < \vartheta\left(\frac{x}{p}\right) \leq \vartheta\left(\frac{x'}{p'}\right) < (a+\delta)\frac{x'}{p'} < (a+\delta)(1+\delta)\frac{x}{p}$$

ou seja,

$$A-\delta < (a+\delta)(1+\delta).$$

Fazendo δ tender a 0, obtemos $A \leq a$. Com isso, concluímos que $a = A$ e desde que $a + A = 2$, temos provado que $a = A = 1$, ou seja, existe o limite

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$$

3.2 Algumas Aplicações do Teorema dos Números Primos

Apresentamos aqui três aplicações diretas a partir do Teorema dos Números Primos.

Aplicação 1: Para $a > 0$ e $b > 0$, temos que

$$\lim_{x\to\infty} \frac{\pi(ax)}{\pi(bx)} = \frac{a}{b}$$

De fato, pelo TNP obtemos

$$\lim_{x\to\infty} \frac{\pi(ax)}{\pi(bx)} = \lim_{x\to\infty} \frac{a}{b}\frac{\frac{\pi(ax)}{ax}}{\frac{\pi(bx)}{bx}} = \frac{a}{b}\frac{\lim_{x\to\infty}\frac{\pi(ax)}{ax}}{\lim_{x\to\infty}\frac{\pi(bx)}{bx}} = \frac{a}{b}$$

Aplicação 2: Para $0 < a < b$, temos que existe x_0 tal que $\pi(ax) < \pi(bx)$ para todo $x \geq x_0$.

Para verificar esse fato, convém observar que para qualquer $c > 0$, temos que

$$\lim_{x\to\infty} \frac{\log x}{\log cx} = 1,$$

e consequentemente,

$$\frac{1}{\log cx} = \frac{1}{\log x} + o\left(\frac{1}{\log x}\right).$$

Pelo TNP, segue que

$$\begin{aligned}\pi(bx) - \pi(ax) &= (b-a)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right)\\ &= (b-a+o(1))\frac{x}{\log x}\end{aligned}$$

Agora basta tomar x_0 de modo que $b-a+o(1) > 0$ para todo $x \geq x_0$ e com isso também teremos que $\pi(bx) - \pi(ax) > 0$, concluindo o resultado.

O resultado contido na Aplicação 2 nos informa que dados $0 < a < b$, para x suficientemente grande, existe pelo menos um número primo no intervalo (ax, bx). Com o uso desse resultado, podemos fazer uma outra aplicação que nos permite obter a densidade de um determinado conjunto nos reais positivos.

Aplicação 3: O conjunto $A = \{p/q : p, q \text{ primos}\}$ é denso em $\mathbb{R}^+$, ou seja, dados $0 < a < b$, existe $p/q \in (a, b)$, com p e q sendo números primos.

Segue da Aplicação 2 que existe um primo no intervalo (ax, bx) para todo $x \geq x_o$. Tomando um primo $q \geq x_0$, concluímos que existe um primo p no intervalo (aq, bq) e portanto $p/q \in (a, b)$.

Conclusão

Para que serve contar números primos até um certo x? Podemos interpretar a conjectura, abordada no trabalho, de algumas maneiras: densidade dos números primos, porcentagem, probabilidade de se encontrar um primo até x. Essa é uma informação útil? Para pesquisadores dos números, sim, pois temos uma estatística a interpretar, propriedades a descobrir, uma curiosidade a se investigar. Sabemos que os números primos são de suma importância em nosso dia a dia, como na codificação de mensagens, nossas senhas, segurança digital.

Devemos entender que para um matemático, nem sempre o tesouro está no final do arco-íris. Passamos por Gauss, Dirichlet, Chebyshev, Riemann, Hadammard, Poussim, Selberg e Erdös, apenas para demonstrar esse teorema? Claro que não. Nesses 300 anos, tiveram vários seminários e convenções em que grandes matemáticos trocavam ideias, demonstrações, pesquisas, muitas vezes através de cartas, já que não existia internet nos séculos XVIII, XIX e metade do XX. Esse é o tesouro desse teorema: novas funções, inovadoras fórmulas e técnicas nas demonstrações, a arte da descoberta de uma nova fronteira a atingir com esses conhecimentos.

Esse é um trabalho que vem a enriquecer os interessados nos números primos, que valorizam demonstrações em Matemática. Serve como um ponto inicial, um roteiro para quem tiver interesse no Teorema dos Números Primos.

Referências Bibliográficas

Apostol, T. M. (1976). *Introduction to analytic number theory.* Springer.

Erdös, P. (1949). On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proceedings of the National Academy of Sciences of the United States of America*, 35(7):374.

Gauss, C. F. (1849). Carta de gauss à encke, göttingen, 24 de dezembro de 1849. Disponível em `https://gauss.adw-goe.de/handle/gauss/199` Acesso em: 15/10/2019.

Murty, M. R. (2008). *Problems in analytic number theory*, volume 206. Springer Science & Business Media.

Ribenboim, P. (2012). *Números primos: velhos mistérios e novos recordes.* IMPA.

Selberg, A. (1949). An elementary proof of the prime-number theorem. *Ann. Math*, 50(2):305–313.

Apêndice A

Primos até 10000

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253, 3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371, 3373, 3389, 3391, 3407, 3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539, 3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823, 3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127, 4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441, 4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733, 4751, 4759, 4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903, 4909, 4919, 4931, 4933, 4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021, 5023, 5039, 5051, 5059, 5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189, 5197, 5209, 5227, 5231, 5233, 5237, 5261, 5273, 5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393, 5399, 5407, 5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477, 5479, 5483, 5501, 5503, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657, 5659, 5669, 5683, 5689, 5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, 5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, 6131, 6133, 6143, 6151, 6163, 6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277, 6287, 6299, 6301, 6311, 6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421, 6427, 6449, 6451, 6469, 6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599, 6607, 6619, 6637, 6653, 6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763, 6779, 6781, 6791, 6793, 6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911, 6917, 6947, 6949, 6959, 6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237, 7243, 7247, 7253, 7283, 7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481, 7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573, 7577, 7583, 7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753, 7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883, 7901, 7907, 7919, 7927, 7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081, 8087, 8089, 8093, 8101, 8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233, 8237, 8243, 8263, 8269, 8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389, 8419, 8423, 8429, 8431, 8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581, 8597, 8599, 8609, 8623, 8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719, 8731, 8737, 8741, 8747, 8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863, 8867, 8887, 8893, 8923, 8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001, 9007, 9011, 9013, 9029, 9041, 9043, 9049, 9059, 9067, 9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203, 9209, 9221, 9227, 9239, 9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371, 9377, 9391, 9397, 9403, 9413, 9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497, 9511, 9521, 9533, 9539, 9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679, 9689, 9697, 9719, 9721, 9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833, 9839, 9851, 9857, 9859, 9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973