Analytic Number Theory

A Project Report Submitted
in Partial Fulfilment of the Requirements
for the Degree of

BACHELOR OF TECHNOLOGY

in

Mathematics and Computing

by

Sahilpreet singh thind
(Roll No. 170123043)

to the

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI - 781039,INDIA
April 2021

CERTIFICATE

This is to certify that the work contained in this project entitled "**Analytic Number Theory**" submitted by **Sahilpreet singh thind** (**Roll No 170123043**) to the Department of Mathematics, Indian Institute of Technology towards partial requirement of **Bachelor of Technology** in Mathematics and Computing has been carried out by him under my supervision.

It is also certified that this report is a survey work based on the references in the bibliography

Turnitin Similarity:

Guwahati -781039
April 2021

(Dr. Pratyoosh Kumar)
Project Supervisor

ABSTRACT

In mathematics, analytic number theory is a branch of number theory that uses methods from mathematical analysis to solve problems about the integers. Johann Peter Gustav Lejeune Dirichlet is credited with the creation of analytic number theory, a field in which he found several deep results and in proving them introduced some fundamental tools, many of which were later named after him. Theorems and results within analytic number theory tend not to be exact structural results about the integers, for which algebraic and geometrical tools are more appropriate. Instead, they give approximate bounds and estimates for various number theoretical function. We begin by establishing basic ideas about prime numbers and with time we hope to understand and establish some structure around prime numbers, their occurrences and their behavior in general.

Contents

Chapter 1

Introduction

1.1 History

One may reasonably define analytic number theory as the branch of mathematics that uses analytical techniques to address number-theoretical problems. But this "definition", while correct, is scarcely more informative than the phrase it purports to define. What kind of problems are suited to"analytical techniques"? What kind of mathematical techniques will be used? What style of mathematics is this, and what will its study teach you beyond the statements of theorems and their proofs? The next few sections try to answer these questions.

The great advances of mathematics in Germany during the first half of the 19^{th} century are to a predominantly large extent associated with the pioneering work of C.F. Gaus (1777–1855), C.G.J. Jacobi (1804–1851), and G. Lejeune Dirichlet (1805–1859). In fact, virtually all leading German mathematicians of the second half of the nineteenth century were their disciples, or disciples of their disciples. Dirichlet was a number theorist at heart but while studying in Paris, being a very likeable person, he was befriended by Fourier and other like-minded mathematics, and he learned analysis from them. Thus equipped, he was able to lay the foundation for the application of

Fourier analysis to (analytic) theory of numbers.

Dirichlet's mastery in the application of analysis to number theory manifests itself most impressively in his proof of the theorem on an infinitude of primes in any arithmetic progression of the form $(l + kq)_{k\geq 1}$,where a and m are co-prime natural numbers. But first we begin by establishing basic ideas like divisibility of integers, and in particular properties of prime numbers, **The fundamental theorem of arithmetic** and some other abstract ideas.

1.2 Euclid's Algorithm

Euclid's Algorithm : For any two integers a and b where $b > 0$, there exist integers q and r with $0 \leq r \leq b$ such that

$$a = qb + r$$

Here q denotes the quotient when a is divided by b and r is the remainder.

Proof. First we prove the existence of q and r, then we prove the uniqueness.

Existence. The set containing all non-negative integers of the form $a - qb$ with $q \in \mathbb{Z}$ is non-empty and since $b \neq 0$ it also contains arbitrary large positive integers, we name this set S. Let the smallest element in S be r, so that

$$r = a - qb$$

for some integer q. By construction 0, and we assume that r. If not, we can write $r = b + s$, so $b + s = a - qb$, which then implies

$$s = a - (q + 1)b$$

Hence $s \in S$ with $s < r$, and this contradicts the our assumption that r is the smallest element in S. So $r < b$, hence q and r satisfy the conditions of the theorem.

Uniqueness. Suppose we had q_1 and r_1 such that $a = q_1 b + r_1$ where $0 \leq r_1 < b$. By subtraction we get

$$(q - q_1)b = r_1 - r$$

The absolute value of LHS is 0 or $\geq b$, while the absolute value of RHS is $< b$. Hence both LHS and RHS must be 0, so we have $q = q_1$ and $r = r_1$.

1.3 The fundamental theorem of arithmetic

Bézout's identity : Let a and b be nonzero integers, and let $d = \gcd(a, b)$. Then there exist integers m and n such that

$$ma \;+\; nb \;=\; d.$$

That is, the greatest common divisor of a and b can always be expressed as a linear combination of a and b. This is particular surprising when a and b are relatively prime, in which case $ma + nb = 1$.

Proof. Let x be the smallest positive integer that can be expressed as a linear combination of a and b. We know that x is a multiple of d, since a and b are both multiples of d. We claim that $x = d$. Suppose to the contrary that $x > d$. Then x cannot be a common divisor of a and b, so either $x \nmid a$ or $x \nmid b$. Without loss of generality, suppose that $x \nmid a$. Then

$$a \div x \;=\; q \text{ R } r$$

where the remainder r is positive. But $r = a - qx$, so r can be written as a linear combination of a and b. This is a contradiction, since r is necessarily less than x. □

The numbers m and n for which $ma + nb = \gcd(a, b)$ are known as ***Bézout coefficients***.

Corrollary 1.1 : Let a, b, and c be nonzero integers. Then c can be written as a linear combination of a and b if and only if c is a multiple of $\gcd(a, b)$.

We can use Bézout's identity to prove Euclid's lemma:

Euclid's Lemma : If p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. Suppose that $p \mid ab$ and $p \nmid a$. We must prove that $p \mid b$.
Since $p \nmid a$ and p is prime, the greatest common divisor of p and a must be 1. Therefore, by Bézout's identity, there exist integers m and n such that

$$ma \;+\; np \;=\; 1.$$

Multiplying through by b gives

$$mab \;+\; npb \;=\; b.$$

Since $p \mid ab$, the left side of this equation is divisible by p, and therefore $p \mid b$. □

The Fundamental Theorem of Arithmetic

We are now in a position to prove the fundamental theorem of arithmetic. We begin by proving a slightly stronger version of Euclid's lemma:

Generalized Euclid's Lemma. If p is prime and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

Proof. This is a straightforward induction. The base case $n = 2$ is Euclid's lemma. For $n > 2$, observe that

$$a_1 \cdots a_n \;=\; (a_1 \cdots a_{n-1})a_n.$$

By Euclid's lemma, either $p \mid a_1 \cdots a_{n-1}$ or $p \mid a_n$. In the first case, it follows from our inductive hypothesis that $p \mid a_i$ for some $i \leq n-1$.

The next lemma tells us exactly which primes must appear in a prime factorization:

Lemma 5.1. Let p and $q_1, \ldots, q_n$ be primes. Then $p \mid q_1 \cdots q_n$ if and only if $p \in \{q_1, \ldots, q_n\}$.

Proof. If $p \in \{q_1, \ldots, q_n\}$, then clearly $p \mid q_1 \cdots q_n$. Conversely, if $p \mid q_1 \cdots q_n$, then by the previous lemma $p \mid q_i$ for some i. Since q_i is prime and $p \neq 1$, we deduce that $p = q_i$. □

Fundamental Theorem of Arithmetic. Let a be composite. Then there exists a unique sequence of primes $p_1 \leq \cdots \leq p_n$ such that $a = p_1 \cdots p_n$.

In the statement of this theorem, we have added the artificial requirement that $p_1 \leq \cdots \leq p_n$ to eliminate any ambiguity regarding the ordering of the primes in the factorization of a.

Proof. The prime factorization theorem establishes existence. For uniqueness, suppose that

$$p_1 \cdots p_m = q_1 \cdots q_n$$

where $p_1 \leq \cdots \leq p_m$ and $q_1 \leq \cdots \leq q_n$ are primes. We wish to prove that $m = n$ and $p_i = q_i$ for each i. Without loss of generality, we may assume that $m \leq n$. We proceed by induction on m.

Base Case: For $m = 1$, the equation is $p_1 = q_1 \cdots q_n$. Since p_1 is prime, the only possibility is that $n = 1$, with $p_1 = q_1$.

Induction Step: For $m > 1$, it follows from the previous lemma that p_m is the largest prime divisor of $p_1 \cdots p_m$, and q_n is the largest prime divisor of $q_1 \cdots q_n$. Since $p_1 \cdots p_m = q_1 \cdots q_n$, we conclude that $p_m = q_n$. Dividing these out leaves

$$p_1 \cdots p_{m-1} \;=\; q_1 \cdots q_{n-1}.$$

The rest now follows from our induction hypothesis. □

Chapter 2

The Infinitude of Primes

2.1 General ideas

Euclid may have been the first to give a proof that there are infinitely many primes and even after 2000 years it stands as an excellent model of reasoning.

Theorem. *There are infinitely many primes.*

Proof. Lets say there are not infinitely many primes and we denote them by $p_1, ..., p_n$. Then we can define a number N in such a way that its larger than any p_i, and hence it cannot be prime because of our assumption.

$$N = p_1 p_2 ... p_n + 1$$

So N must be divisible by a prime that belongs to our set of primes, but this is a contradiction since every prime in our set does not divide N. Thus our assumption was wrong and there are infinitely many primes.

Euclid's argument can be modified to deduce finer results like specific subsets of prime numbers being infinite. Those sets being specific representations of prime numbers, since all prime numbers > 2 can divided into 2 sets, prime numbers of the form 4k+1 and 4k+3, and since there are infinitely may primes, at least one of these sets has to be infinite. It is relatively trivial to prove that the class 4k+3 has infinitely many primes, but it remains to determine if the class of primes of the form 4k+1 is infinite. So we go ahead to look into more general ideas like Legendre's statement :

if q and l are relatively prime, then the sequence

$$l + kq, \quad k \in \mathbb{Z}$$

contains infinitely many primes.

This assertion was proved by Dirichlet using the ideas of Euler's analytical approach to prime numbers involving his product formula, which we'll explore in the coming sections.

2.2 The zeta function and its Euler product

The whole of analytic number theory rests on one marvellous formula due to Leonhard Euler (1707-1783):

$$\sum_{n \in \mathbb{N}, n>0} n^{-s} = \prod_{primes \ p} (1 - p^{-s})^{-1}$$

Euler's Product Formula equates the Dirichlet series $\sum n^{-s}$ on the left with the infinite product on the right. To make the formula precise, we must develop the theory of infinite products, which we do in the next Section. To understand the implications of the formula, we must develop the theory of Dirichlet series, which we do in the next Chapter.
We begin with a brief overview of infinite products. Let $\{A_n\}_{n=1}^{\infty}$ be a sequence of real numbers, we define

$$\prod_{n=1}^{\infty} A_n = \lim_{N \to \infty} \prod_{n=1}^{N} A_n$$

This product converges if the limit exists. To make our calculations easier we take logarithms and change products into sums. Now we define some properties of of the function log x, defined for positive real numbers that we shall need later.

Properties of logarithm and exponential functions
(i) e^{logx} = x
(ii) $log(1+x) = x + E(x)$ where $|E(x)| \leq x^2$ if $|x| < 1/2$
(iii) If $log(1+x) = y$ and $|x| < 1/2$, then $y \leq 2|x|$

We can also write property (ii) in terms of O notation as log(1+x) = x+ $O(x^2)$.

Proposition. Suppose $a_n \neq 1$ for $n \in \mathbb{N}$. Then

$$\sum |a_n| \ \ convergent \implies \prod (1+a_n) \ \ convergent$$

For the function $Log(1+x)$ if $|x| < 1/2$ then $|Log(1+x)| \leq |x|$, by property (iii). Now suppose $\sum |a_n|$ converges. Then $a_n \to 0$; and so

$$|a_n| \leq 1/2$$

for $n \geq N$. It follows that

$$|Log(1+a_n)| \leq 2|a_n|$$

for $n \geq N$.Hence

$$\sum Log(1+a_n) \ \ converges$$

With these general ideas behind us we can now shift our focus to the main topic of this chapter, the zeta function :

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

The Zeta-function was first introduced by Euler with the computation of

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2}$$

but it was Riemann who, in the 1850's, generalized its use and showed that the distribution of primes is related to $\zeta(s)$. It is easy to show that

$$\zeta(s) \leq 1 + \frac{1}{s-1}$$

and that the series defining ζ converges uniformly on each half-line $s > s_0 > 1$, hence ζ is continuous when $s > 1$. Now we move towards the main result of Euler's product formula.

Theorem. For $s > 1$, the Riemann zeta function is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}}$$

where p_k is the k^{th} prime. This is Euler's product, called by Havil the "all-important formul" and by Derbyshire the"golden key". This can be proved by expanding the product, writing each term as a geometric series, expanding, multiplying, and rearranging terms :

$$\prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}} = \frac{1}{1 - \frac{1}{p_1^s}} \frac{1}{1 - \frac{1}{p_2^s}} \frac{1}{1 - \frac{1}{p_3^s}} \cdots$$

$$= \left[\sum_{k=0}^{\infty} \left(\frac{1}{p_1^s}\right)^k\right] \left[\sum_{k=0}^{\infty} \left(\frac{1}{p_2^s}\right)^k\right] \left[\sum_{k=0}^{\infty} \left(\frac{1}{p_3^s}\right)^k\right] \cdots$$

$$= \left(1 + \frac{1}{p_1^s} + \frac{1}{p_1^{2s}} + \frac{1}{p_1^{3s}} + \ldots\right) \left(1 + \frac{1}{p_2^s} + \frac{1}{p_2^{2s}} + \frac{1}{p_2^{3s}} + \ldots\right) \cdots$$

$$= 1 + \sum_{1 \leq i} \frac{1}{p_i^s} + \sum_{1 \leq i \leq j} \frac{1}{p_i^s p_j^s} + \sum_{1 \leq i \leq j \leq k} \frac{1}{p_i^s p_j^s p_k^s} + \ldots$$

$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + ...$$

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

$$= \zeta(s)$$

By the fundamental theorem of arithmetic, each integer ≥ 1 occurs in this way uniquely, hence the product equals

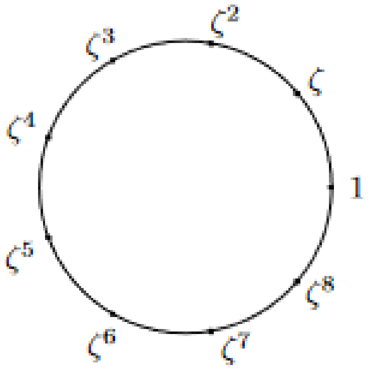
$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

Chapter 3

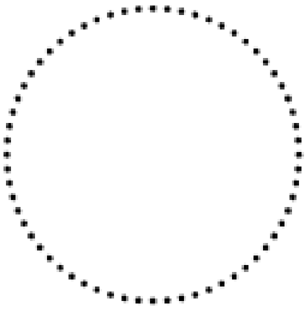
Brief overview of Finite Abelian groups

We begin by introduction to the simplest finite Abelian group $\mathbb{Z}(N)$ which has the group of N^{th} roots of unity as its underlying space.
Another way of realizing this group is as $\mathbb{Z}/N\mathbb{Z}$ (equivalence classes of integers modulo N)
This basically divides the unit circle into uniform divisions which get more finer as $N \to \infty$

3.1 $\mathbb{Z}(N)$



$Z(9),\ \zeta = e^{2\pi i/9}$



$Z(N),\ N = 2^6$

For a finite cyclic group G of order n we have $G = \{e, g, g^2, ..., g^{n-1}\}$, where e is the identity element and $g^i = g^j$ whenever $i \equiv j \ (mod\ n)$; in particular $g^n = g^0 = e$, and $g^1 = g^{n-1}$. An abstract group defined by this multiplication is often denoted C_n, and we say that G is isomorphic to the standard cyclic group C_n. Such a group is also isomorphic to $\mathbb{Z}/n\mathbb{Z}$, the group of integers modulo n with the addition operation, which is the standard cyclic group in additive notation. Set of N^{th} roots of 1 is exactly

$$\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, e^{2\pi i 3/N}, ..., e^{2\pi i(N-1)/N}\}$$

We can also visualize this using $\zeta = e^{2\pi i/N}$. Clearly if n and m differ by an integer multiple of N, then $\zeta^n = \zeta^m$. We can also note that the set $\mathbb{Z}(N)$ satisfies all the properties of an Abelian group under complex multiplication.

An equivalent approach is to associate to each root of unity ω the class of integers n so that $\zeta^n = \omega$. Doing so for each root of unity we obtain a partition of the integers in N disjoint infinite classes. To add two of these classes, choose any integer in each one of them, say n and m, respectively, and define the sum of the classes to be the class which contains the integer $n + m$. We formalize the above notions. Two integers x and y are congruent modulo N if the difference xy is divisible by N, and we write $x \equiv y \ (mod\ N)$. In other words, this means that x and y differ by an integer multiple of N. It is an easy exercise to check the properties of Abelian groups:

3.2 $\mathbf{Z}^*(q)$

We define an integer $n \in \mathbb{Z}(q)$ to be a unit if there exists an integer $m \in \mathbb{Z}(q)$ so that

$$nm \equiv 1 \ mod\ q$$

$\mathbb{Z}^*(q)$ is the set of units in $\mathbb{Z}(q)$

Example : Group of units in $\mathbb{Z}(6) = \{0, 1, 2, 3, 4, 5\}$ is

$$\mathbb{Z}^*(q) = \{1, 5\}$$

Example : Group of units in $\mathbb{Z}(4) = \{0, 1, 3\}$ is

$$\mathbb{Z}^*(q) = \{1, 3\}$$

This reflects the fact that odd integers are divided into two classes depending on whether they are of the form $4k + 1$ or $4k + 3$. In fact, $\mathbb{Z}^*(4)$is isomorphic to $\mathbb{Z}(2)$. We can notice that multiplication in $\mathbb{Z}^*(4)$ corresponds to addition in $\mathbb{Z}(q)$

3.3 Characters

The classical definition of a character of a finite Abelian group G is a multiplicative mapping of the group G into the multiplicative group of all the roots of unity. In other words, a character on G is a complex-valued function which satisfies the following condition :

$$e(a \cdot b) = e(a)e(b) \ for \ all \ a, b \in G$$

The trivial or unit character is defined by $e(a) = 1$ for all $a \in G$. If G is a finite Abelian group, we denote by $\hat{G}$ the set of all characters of G.

Chapter 4

Dirichlet's theorem

Euler's ideas of the product function for the zeta function was the starting point in Dirichlet's argument. One of the amazing things about the proof of Dirichlet's theorem is how modern it feels. It is literally amazing to compare the scope of the proof to the arguments we used to prove some of the other theorems in the course, which historically came much later. Dirichlet's theorem comes 60 years before Minkowksi's work on the geometry of numbers and 99 years before the Chevalley-Warning theorem! Dirichlet proved his theorem in 1837. It should be noted that Fourier, who had befriended Dirichlet when the latter was a young mathematician visiting Paris, had died several years before. Besides the great activity in mathematics, that period was also a very fertile time in the arts, and in particular music. The era of Beethoven had ended only 10 years earlier, and Schumann was now reaching the heights of his creativity. But the musician whose career was closest to Dirichlet was Felix Mendelssohn. It so happens that the latter began composing his famous violin concerto the year after Dirichlet succeed in proving his theorem. We now introduce the theorem.

4.1 Euler's version of infinitude of primes

Proposition : The Series

$$\sum_p \frac{1}{p}$$

diverges, when the sum is taken over all primes.
This inherently proves that there are infinite number of prime because finitely many primes would make the series converge. Taking advantage of the continuity of log x, we take log on both sides of the Euler formula and write it as summation of log. We get, for $s > 1$:

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

Remember we already proved that $log(1 + x) = x + O(|x|^2)$ whenever $|x| \leq 1/2$. Using this we get :

$$-\sum_p [-1/p^s + O(1/p^{2s})] = log\zeta(s)$$

Now we know that $\sum_p 1/p^{2s} \leq \sum_{n=1}^{\infty} 1/n^2$ which in turn is bounded, hence we use $O(1)$ to replace $\sum_p 1/p^{2s}$. Also note that $\zeta \to \infty$ since $\sum_{n=1}^{\infty} 1/n^2 \geq \sum_{n=1}^{M} 1/n^2$ for every M. It is relatively trivial to prove that $\zeta(s)$ diverges for $s = 1$
We can rewrite $\zeta(s)$ for $s = 1$ as :

$$1 + \frac{1}{2} + (\frac{1}{3} + \frac{1}{4}) + (\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}) ......$$

Now let $S =$:

$$1 + \frac{1}{2} + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}) ...... = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} ....$$

Clearly $\zeta(1) >= S$ where S is defined above. Also note that S diverges. So clearly as $\zeta(1) \to \infty$. Also since

$$-\sum_p [-1/p^s + O(1/p^{2s})] = log\zeta(s)$$

$\sum_p -1/p^s \to \infty \ for \ s = 1$. And we finaly have that

$$\sum_p -1/p^s \to \infty$$

Now we'll look at Dirichlet's theorem using this insight.

4.2 Proof

Theorem. If q and l are relatively prime positive integers, then there are infinitely many primes of the form $l + kq$ with $k \in \mathbb{Z}$

More serious demands come from the analytic side: the main strategy is, as in Euler's proof of the infinitude of primes, to consider the function

$$\sum_{p \equiv l \ mod \ q} \frac{1}{p}$$

The above series diverges. The is the main objective here, and to get an understanding of it we revisit an older problem, are there infinitely many primes of the from $4k + 1$? This particular example has $l = 1$ and $q = 4$. We now illustrate steps of the theorem for this particular example.

Since we need to somehow arrive at specific partitions of the total set of prime numbers according to some group we consider the character on $\mathbb{Z}^*(4)$ defined by $\chi(1) = 1$ and $\chi(3) = -1$. Extending this character to all of $\mathbb{Z}$ we get :

$$\chi(n) = \begin{cases} 0 & \text{if n is even} \\ 1 & \text{if n} = 4k + 1 \\ -1 & \text{if n} = 4k + 3 \end{cases}$$

Clearly $\chi(nm) = \chi(n)\chi(m)$ (its multiplicative) on all of $\mathbb{Z}$. Define Dirichlet L-function as : $L(s, \chi) = \sum_{n-1}^{\infty} \chi(n)/n^s$ such that :

$$L(s, \chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + ...$$

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ...$$

By the alternating series test $L(1,\chi)$ is convergent and $L(1,\chi) \neq 0$. We can also see this by integrating $\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + ...$ We get :

$$\int_0^y \frac{dx}{1+x^2} = y - \frac{y^3}{3} + \frac{y^5}{5} - ....., 0 < y < 1$$

As $y \to 1$

$$\int_0^1 \frac{dx}{1+x^2} = arctan\ u|_0^1 = \frac{\pi}{4}$$

Now we can generalize Euler product formula (using the fact that χ is multiplicative) to give

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)/p^s}$$

Taking log on both sides :

$$\log L(s,\chi) = -\sum_p \log(1 - \chi(p)/p^s)$$

$$= -\sum_p [-\frac{\chi(p)}{p^s} + O(\frac{1}{p^{2s}})]$$

$$= \sum_p \frac{\chi(p)}{p^s} + O(1)$$

If $L(1,\chi)$ is finite and non-zero (which it is in our case), then $\log L(s,\chi)$ is bounded as $s \to 1^+$, and we can conclude that the sum

$$\sum_p \frac{\chi(p)}{p^s}$$

is bounded as $s \to 1^+$. Recall our character χ

$$\chi(n) = \begin{cases} 0 & \text{if n is even} \\ 1 & \text{if n} = 4k+1 \\ -1 & \text{if n} = 4k+3 \end{cases}$$

Accordingly

$$\sum_p \chi(p)/p^s = \sum_{p\equiv 1} \frac{1}{p^s} - \sum_{p\equiv 3} \frac{1}{p^s} \text{ is bounded as } s \to 1^+$$

and we know that $\sum_p \frac{1}{p^s}$ is unbounded as $s \to 1^+$. Adding these two we get

$$2\sum_{p\equiv 1} \frac{1}{p^s} \text{ is unbounded as } s \to 1^+$$

Hence $\sum_{p\equiv 1} 1/p$ diverges and there are infinitely many primes of the form $4k+1$

4.3 Prime Number Theorem

In number theory, the prime number theorem (PNT) describes the asymptotic distribution of the prime numbers among the positive integers. It formalizes the intuitive idea that primes become less common as they become larger by precisely quantifying the rate at which this occurs. The theorem was proved independently by Jacques Hadamard and Charles Jean de la Vallée Poussin in 1896 using ideas introduced by Bernhard Riemann (in particular, the Riemann zeta function).

The first such distribution found is $\pi(N) \sim \frac{N}{log(N)}$, where $\pi(N)$ is the prime-counting function and $log(N)$ is the natural logarithm of N. This means that for large enough N, the probability that a random integer not greater than N is prime is very close to $\frac{1}{log(N)}$. Consequently, a random integer with at most 2n digits (for large enough n) is about half as likely to be prime as a random integer with at most n digits. For example, among the positive integers of at most 1000 digits, about one in 2300 is prime ($log(101000) \sim 2302.6$), whereas among positive integers of at most 2000 digits, about one in 4600 is prime ($log(102000) \sim 4605.2$). In other words, the average gap between consecutive prime numbers among the first N integers is roughly $log(N)$.

Prime-counting function in terms of the logarithmic integral

In a handwritten note on a reprint of his 1838 paper ”Sur l’usage des séries infinies dans la théorie des nombres”, which he mailed to Gauss, Dirichlet conjectured (under a slightly different form appealing to a series rather than an integral) that an even better approximation to $\pi(x)$ is given by the offset logarithmic integral function Li(x).

Definition. For $x \geq e$ we set

$$\int_e^x \frac{dt}{\log t}$$

Proposition. As $x \to \infty$,

$$Li(x) \sim \frac{x}{\log x}.$$

Proof. Integrating by parts,

$$\begin{aligned} Li(x) &= \int_e^x \frac{dt}{\log t} \\ &= \left[t\frac{1}{\log t}\right]_e^x + \int_e^x t\frac{1}{t\log t^2}dt \\ &= \frac{x}{\log x} - e + \int_e^x \frac{dt}{\log^2 t} \end{aligned}$$

It is clear from this that

$$Li(x) \to \infty \quad as \quad x \to \infty$$

Thus the result will follow if we show that

$$\int_e^x \frac{dt}{\log^2 t} = O(Li(x))$$

But

$$\begin{aligned}\int_e^x \frac{dt}{\log^2 t} &= \int_e^{x^{1/2}} \frac{dt}{\log^2 t} + \int_{x^{1/2}}^x \frac{dt}{\log^2 t} \\ &\leq x^{1/2} + \frac{1}{\log x^{1/2}} \int_{x^{1/2}}^x \frac{dt}{\log t} \\ &\leq x^{1/2} + \frac{2Li(x)}{\log x}\end{aligned}$$

From above,

$$Li(x) \geq \frac{x}{\log x} - e$$

Thus

$$x^{1/2} = O(Li(x)),$$

and so

$$\int_e^x \frac{dt}{\log^2 t} = O(Li(x)),$$

as required.
Remark.We can extend this result to give an asymptotic expansion of Li(x).Integrating by parts,

$$\begin{aligned}\int_e^x \frac{dt}{\log^2 t} &= \left[t\frac{1}{\log^n t}\right]_e^x + \int_e^x t\frac{1}{nt\log^{n+1} t}dt \\ &= \frac{x}{\log^n x} - e + \frac{1}{n}\int_e^x \frac{dt}{\log^{n+1} t}\end{aligned}$$

It follows that

$$Li(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{1}{2!}\frac{x}{\log^3 x} + ... + \frac{1}{(n-1)!}\frac{x}{\log^n x} + O(\frac{x}{\log^{n+1} x})$$

Corollary. .The Prime Number Theorem can be stated in the form:

$$\pi(x) \sim Li(x)$$

Remark. This is actually a more accurate form of the Prime Number Theorem, in the following sense. It has been shown that

$$\pi(x) - Li(x)$$

changes sign infinitely often, ie however large x gets we find that sometimes $\pi(x) \geq Li(x)$, and sometimes $\pi(x) < Li(x)$. On the other hand, it follows from the Remark above that Li(x) is substantially larger than $\frac{x}{\log x}$; and it has also been shown that $\pi(x) > \frac{x}{\log x}$ for all sufficiently large x.
The logarithmic integral Li(x) is larger than $\pi(x)$ for "small" values of x. This is because it is (in some sense) counting not primes, but prime powers, where a power p^n of a prime p is counted as $\frac{1}{/}n$ of a prime. This suggests that Li(x) should usually be larger than $\pi(x)$ by roughly $Li(\sqrt{x})/2$, and in particular should always be larger than $\pi(x)$. However, in 1914, J. E. Littlewood proved that $\pi(x) - Li(x))$ changes sign infinitely often. The first value of x where $\pi(x)$ exceeds Li(x) is probably around $x = 10^{316}$. (On the other hand, the offset logarithmic integral Li(x) is smaller than $\pi(x)$ already for x = 2; indeed, Li(2) = 0, while $\pi(2)$ = 1.)

prime number race Although we have in particular

$$\pi_{4,1}(x) \sim \pi_{4,3}(x),$$

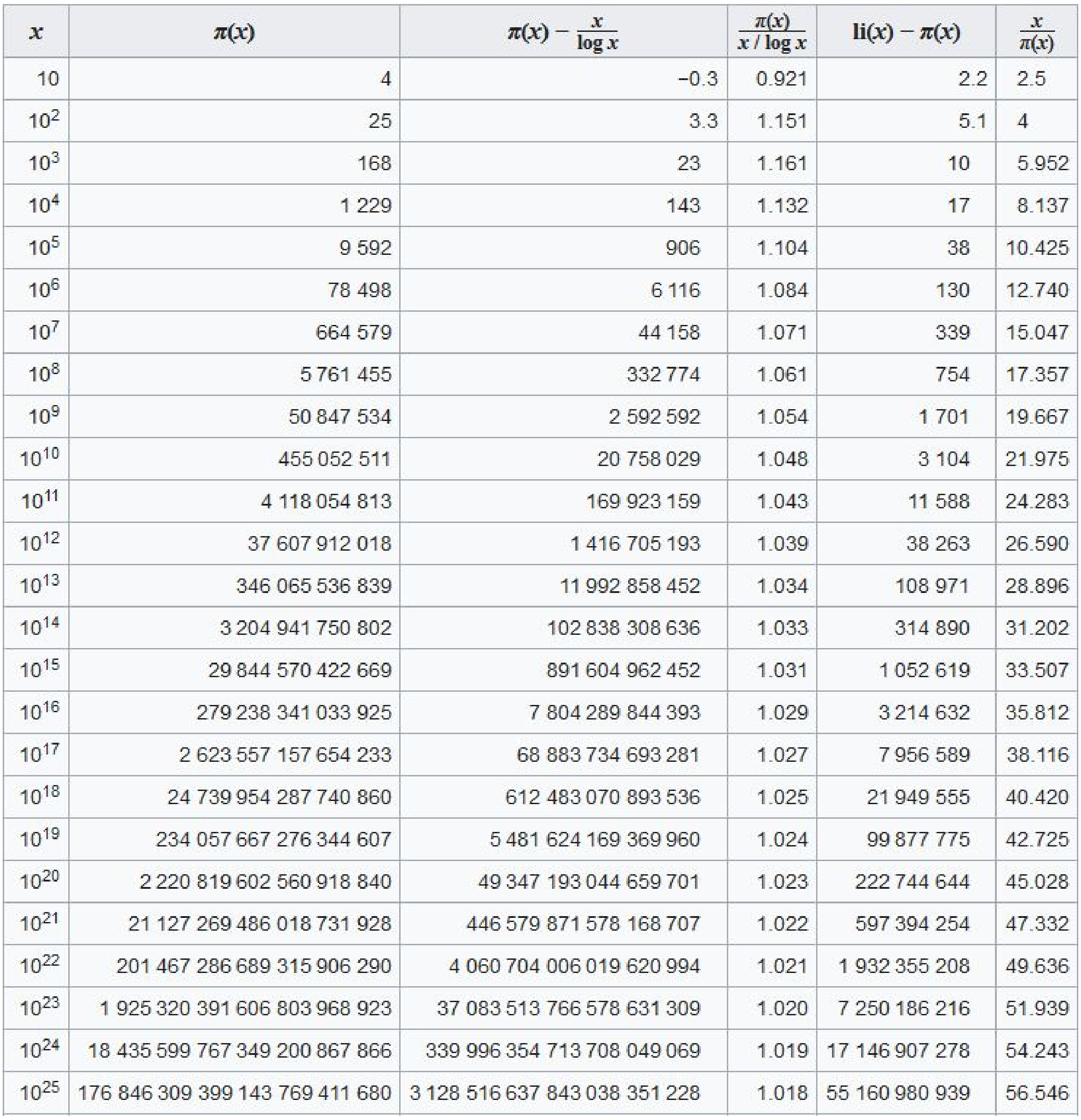
empirically the primes congruent to 3 are more numerous and are nearly always ahead in this "prime number race"; the first reversal occurs at x = 26861. However Littlewood showed in 1914 that there are infinitely many sign changes for the function

$$\pi_{4,1}(x) \sim \pi_{4,3}(x),$$

so the lead in the race switches back and forth infinitely many times. The phenomenon that $\pi_{4,3}(x)$ is ahead most of the time is called

Chebyshev's bias. The prime number race generalizes to other moduli and is the subject of much research.

The table compares exact values of $\pi(x)$ to the two approximations $\frac{x}{\log x}$ and Li(x). The last column, $\frac{x}{\pi(x)}$, is the average prime gap below x.



x	$\pi(x)$	$\pi(x) - \frac{x}{\log x}$	$\frac{\pi(x)}{x / \log x}$	$\mathrm{li}(x) - \pi(x)$	$\frac{x}{\pi(x)}$
10	4	-0.3	0.921	2.2	2.5
10^2	25	3.3	1.151	5.1	4
10^3	168	23	1.161	10	5.952
10^4	1 229	143	1.132	17	8.137
10^5	9 592	906	1.104	38	10.425
10^6	78 498	6 116	1.084	130	12.740
10^7	664 579	44 158	1.071	339	15.047
10^8	5 761 455	332 774	1.061	754	17.357
10^9	50 847 534	2 592 592	1.054	1 701	19.667
10^{10}	455 052 511	20 758 029	1.048	3 104	21.975
10^{11}	4 118 054 813	169 923 159	1.043	11 588	24.283
10^{12}	37 607 912 018	1 416 705 193	1.039	38 263	26.590
10^{13}	346 065 536 839	11 992 858 452	1.034	108 971	28.896
10^{14}	3 204 941 750 802	102 838 308 636	1.033	314 890	31.202
10^{15}	29 844 570 422 669	891 604 962 452	1.031	1 052 619	33.507
10^{16}	279 238 341 033 925	7 804 289 844 393	1.029	3 214 632	35.812
10^{17}	2 623 557 157 654 233	68 883 734 693 281	1.027	7 956 589	38.116
10^{18}	24 739 954 287 740 860	612 483 070 893 536	1.025	21 949 555	40.420
10^{19}	234 057 667 276 344 607	5 481 624 169 369 960	1.024	99 877 775	42.725
10^{20}	2 220 819 602 560 918 840	49 347 193 044 659 701	1.023	222 744 644	45.028
10^{21}	21 127 269 486 018 731 928	446 579 871 578 168 707	1.022	597 394 254	47.332
10^{22}	201 467 286 689 315 906 290	4 060 704 006 019 620 994	1.021	1 932 355 208	49.636
10^{23}	1 925 320 391 606 803 968 923	37 083 513 766 578 631 309	1.020	7 250 186 216	51.939
10^{24}	18 435 599 767 349 200 867 866	339 996 354 713 708 049 069	1.019	17 146 907 278	54.243
10^{25}	176 846 309 399 143 769 411 680	3 128 516 637 843 038 351 228	1.018	55 160 980 939	56.546

....

Bibliography

[1] Elias M. Stein and Rami Shakarchi. *Princeton Lectures in Analysis.* Princeton University Press, Princeton and Oxford Analysis, 2002.

[2] Elstrodt, Jürgen. *The Life and Work of Gustav Lejeune Dirichlet (1805–1859).* Clay Mathematics Proceedings. Retrieved 2007-12-25.

[3] Titchmarsh,Edward Charles. *The Theory of the Riemann Zeta Function (2nd ed.)* Oxford University Press.

[4] Wikipedia articles for Analytic number theory
`https://en.wikipedia.org/wiki/Analytic_number_theory`
`https://en.wikipedia.org/wiki/Dirichlet's_theorem`