1960

The prime number theorem

BOSTON UNIVERSITY

GRADUATE SCHOOL

Thesis

PRIME NUMBER THEOREM

by

HUGH W. LYNCH

(B.S. Ed., Boston Teachers College, 1952)

Submitted in partial fulfilment of the
requirements for the degree of
Master of Arts
1960

Approved
by

First Reader ....Philip T. Maker....
Professor of Mathematics

Second Reader ....Thomas B. Knapp....
Professor of Mathematics

Outline

Notation [1]

Suppose that n is an integral variable which tends to infinity, x a continuous variable which tends to a limiting value; that $g(n)$ or $g(x)$ is a positive function of n or x; and that $f(n)$ or $f(x)$ is any other function of n or x. Then

(1) $f = O(g)$ means that $|f| < Ag$ where A is independent of n or x for all values of n or x in question.

(2) $f = o(g)$ means that $f/g \to 0$. This is stronger than and implies (1).

(3) $f \sim g$ means that $f/g \to 1$. In these circumstances we say f is asymptotic to g.

(4) $f \asymp g$ means that $Ag < f < Ag$ where the two A's (which are not the same) are both positive and independent of n or x. Thus $f \asymp g$ asserts that f is of the same order of magnitude as g.

(5) $(n,m) = 1$ means that one is the only divisor of both n and m.

(6) Suppose P is a possible property of a positive integer; and $P(x)$ the number of numbers less than x which possess the property P. If $P(x) \sim x$, i.e. , if the number of numbers less than x which do not possess this property is $o(x)$, then we say that almost all numbers possess this property.

1. This notation is due to Hardy and Wright, page 7

The Prime Number Theorem

One of the most famous problems in arithmetic is the prime number theorem which can be stated as follows:

The number $N(x)$ of primes less than or equal to x is asymptotically equal to $x/\log x$, that is, the limit of $N(x)\log x/x$ as x goes to infinity is one.

This problem was worked on by many renowned mathematicians including Gauss, Dirichlet, Legendre, Riemann, Tchebycheff, Wiener, and Landau. The actual formula for the distribution of primes was first proposed by Gauss but almost a century elapsed before the theorem itself was proven independently by Hadamard and Poussin. Since then there have been several proofs and reformulations of proofs.

We will first give a resume of the history of the prime number theorem. Then we will introduce several arithmetical functions which we will use to discuss the work of Tchebycheff who contributed to the development of the proof of the theorem although he was unable to prove the theorem itself. We will demonstrate his work to show how much he was able to accomplish by simple methods and without the aid of modern analysis. We shall, employing his methods, prove his theorems that $N(x)$ is of the same order of magnitude as x and that the limit of $N(x)\log x/x$ is 1, if the limit exists.

In order to prove that the limit of the above ratio exists and hence prove the prime number theorem itself, we will need the famous Riemann zeta-function $Z(s)$, where $s = r + it$. We will define $Z(s)$ both as an infinite series and as an infinite product and will discuss its convergence. We will prove several theorems concerning the distribution of the zeros of $Z(s)$. The theorem that $Z(s)$ has no zeros on $r = 1$ has been considered a most essential step in any proof of the prime number theorem. Therefore, we shall, for historical reasons, give both Hadamard's argument and Poussin's proof of this theorem. Each of these two men was able to prove the main theorem by making use of this theorem.

At this point we will be in a position to discuss proofs of the prime number theorem. We will state,without proof, Landau's lemma on asymptotic expansions. Then we will indicate his proof of the main theorem using this lemma. Finally we will discuss Bochner's proof of the prime number theorem. To do this we will state his theorem on asymptotic expansions. We will outline the main steps of the proof of this preliminary theorem so as to indicate the amount of mathematics needed to prove the prime number theorem. Making use of this theorem we will prove the prime number theorem.

A History of the Prime Number Theorem

The ancient Greeks were interested in prime numbers. Eratosthenes (275 - 194 B.C.) invented a 'sieve' for finding primes. All composite numbers were sifted out as follows. Write down the number two followed by all odd numbers from three up in succession. Remove all multiples of three by crossing out every third number after the three. By canceling every fifth number after the five we remove all multiples of five. In this fashion, after crossing out all multiples of 7, 11, 13, etc.,we have left only prime numbers. The most interesting thing about this simple method of finding primes was that no better way of finding the number of primes in the series 1, 2, 3, ...n was found until the nineteenth century.

A question that attracted the attention of many mathematicians was that of finding a formula giving all the primes or the exact number of primes less than an indefinite integer n. Since this search met with no success, attempts were made to find simple formulas that would give only primes even though they might not give all the primes. Fermat, for example, claimed that all numbers of the form $F(n) = 2^{2^n} + 1$ were primes. But in 1732, Euler showed that F(5) is not a prime,[1] Similar formulas met the same fate. Finally this futile approach was put aside and mathematicians began instead to seek for information concerning the average distribution of primes among the integers.

This problem was known to Gauss. He stated that x/logx would approximate N(x) and the larger the value of x the better the approximation. It is not known if he ever proved this statement. His answer was found on the back of a copy

1. What is Mathematics, page 482.

of Schulze's Table of Logarithms.[2] Such a book seems a strange place to find the answer to the distribution of primes.

Other empirical formulas were suggested. Gauss later condidered $\int_2^x (\log x)^{-1}\, dx$ of which $x/\log x$ is the leading term. Legendre, unaware of this, suggested the formula $x\,(A \log x + B)^{-1}$. Dirichlet showed that this formula, which Abel quotes as " the most marvelous in mathematics," was correct only to the leading term.[3]

In 1859 the great Russian mathematician P.Tchebycheff made the first great advance in the theory of prime numbers. His work was the first attempt at a rigorous study of the problem. He did not prove the prime number theorem as the tools of modern analysis were not then available. However, by elementary methods, he was able to prove rigorously that the number of primes not greater than x is between 0.921Q and 1.106Q where $Q = x/\log x$. Later J.J.Sylvester obtained by the same methods the limits 0.95Q and 1.05Q.[4] Tchebycheff's limits provided a proof for the famous Bertrand postulate that there is at least one prime between x and 2x - 2. He proved that the limit, if existent, of $N(x) \log x/x$ is one.

All that remained to prove the prime number theorem was to prove the existence of this limit. The famous Riemann zeta - function Z(s) was needed for this. Riemann set forth six properties of the zeta - function, none of which he was able to prove. Five have since been proven. The remaining one, that all the zeros in the strip $0 \leq r \leq 1$ have real part ½, remains unproved. Riemann conjectured that this property was true. This is the famous Riemann hypothesis.

2. <u>The World of Mathematics</u>, page 157
3. <u>A Source Book in Mathematics</u>, page 128
4. <u>The Development of Mathematics</u>, page 314

Attempts to prove or disprove this have resulted in a great deal of mathematical activity. This has increased since Hardy was able to prove in 1914 that Z(s) has an infinity of zeros on $r = \frac{1}{2}$.[5] The zeta - function which was first studied only because of its importance in prime number theory has since become important also in the theory of analytic functions in general.

The prime number theorem was proven independently in 1896 by J.Hadamard and de la Vallee Poussin. The methods used depended on a knowledge of the zeta - function in a region of the complex s-plane.

The theorem was also proven in 1901 by von Koch of Stockholm , in 1903 by E.Landau, and in 1915 by Hardy and Littlewood.[6] Their proofs are for the most part refinements of the Poussin - Hadamard proof.

N.Wiener, in 1930, deduced the proof of the prime number theorem almost as a corollary from his work on Tauberian theorems. The theorems were so named by Hardy after the German analyst Tauber. They evolved from the converse of Abel's theorem on convergent power series.[7] His proof involved the behaviour of the zeta - function merely on the line $r = 1$. S.Bochner, Landau, and T.Estermann have refined Wiener's proof. In this paper we shall discuss the proofs due to the first two of these.

5. <u>The Development of Mathematics</u>, page 315
6. <u>A History of Mathematics</u>, page 439
7. <u>The Development of Mathematics</u>, page 315

Arithmetical Functions and Elementary Theorems

In this section we will introduce several arithmetical functions which have long been associated with the prime number theorem. We will also prove a few elementary theorems concerning these functions. Our aim here is to provide for future needs. The material presented now will be needed in later sections when we will discuss the work of Tchebycheff, Landau, and Bochner.

Definition 1. Euler's Function

We denote by $E(m)$ the number of integers not greater than and prime to m, that is, the number of values of n such that $0 \leq n \leq m$ and $(n,m) = 1$

Theorem 1. $E(n) = n\prod_{p|n}(1-p^{-1})$

Proof - Let $p, p', \ldots$ be the different prime factors of n. Then the number of integers not greater than n and divisible by p is n/p. The number not greater than n and divisible by p and p' is n/pp'; and so on. Hence the number of integers not greater than n and prime to m is

$$E(n) = n - \sum n/p + \sum n/pp' - \ldots = n\prod_{p|n}(1-p^{-1})$$

$$E(60) = 60\ (1-1/2)\ (1-1/3)\ (1-1/5) = 16$$

Making use of the general principle used in the proof of the above theorem we shall prove

Theorem 2. Almost all numbers are composite ; $N(x) = o(x)$.[8]

Proof - Denote $[x]$ by $F(x)$. If $H(x,r)$ is the number of numbers which do not exceed x and are not divisible by any of the first r primes $p_1, p_2, \ldots\ p_r$, then

8. This proof follows closely the proof on page 341 in Hardy and Wright.

(1) $H(x,r) = F(x) - \sum_i F\left(\frac{x}{p_i}\right) + \sum_{i,j} F\left(\frac{x}{p_i p_j}\right) - \ldots,$

where i, j, ... are unequal and range from 1 to r.

It is plain that

(2) $N(x) \leq H(x,r) + r$

The number of brackets in (1) is $1 + \binom{r}{1} + \ldots = 2^r$ and hence the error involved in removing the brackets will be less than 2^r. Hence (2) becomes

$$N(x) \leq x - \sum_i \frac{x}{p_i} + \sum_{i,j} \frac{x}{p_i\ p_j} - \ldots + r + 2^r$$

$$= x \prod_{p \leq p_r} (1-p^{-1}) + r + 2^r < x \prod_{p \leq p_r} (1-p^{-1}) + 2^{r+1}.$$

Now $\prod (1-p^{-1})^{-1}$ is divergent. This can be seen by noting that

$$\prod_{p \leq N} (1-p^{-1})^{-1} = \prod_{p \leq N} (1 + p^{-1} + p^{-2} + \ldots) \geq \sum_1^N n^{-1} > \log N$$

Hence $\prod (1-p^{-1})$ diverges to zero and there exists an r(e) such that

$$N(x) \leq \frac{ex}{2} + 2^{r+1}.$$

We can also find an x'(e) such that $N(x) < ex$ for all $x \geq x'$.

Another arithmetical function associated with prime number theory is

<u>Definition</u> 2. the Mobius function which is defined as follows:

(1) $U(1) = 1$

(2) $U(n) = 0$ if n has a squared factor

(3) $U(p_1, p_2, \ldots p_r) = (-1)^r$ if all the primes p_1, $p_2, \ldots p_r$ are different.

$U(2) = 1 \quad U(6) = 1 \quad U(4) = 0$

The following three arithmetical functions have to do with logarithms.

<u>Definition</u> 3. The function A(n) is defined by

$A(n) = \log p \qquad \text{if } (n = p^m)$

$A(n) = 0 \qquad\qquad (n \neq p^m)$

i.e., as being log p when n is a prime p or one of its powers and zero otherwise

$A(1) = A(14) = 0$

$A(3) = A(27) = \log 3$

Definition 4. The function $W(x)$ is defined by

(3) $W(x) = \sum_{p^m \leq x} \log p = \sum_{n \leq x} A(n)$

$W(1) = 0 \quad W(2) = \log 2 \quad W(8) = \log (2^3 \cdot 3.5.7)$

Definition 5. The function $L(x)$ is defined by

(4) $L(x) = \sum_{p \leq x} \log p = \log \prod_{p \leq x} p$

and is the sum of the logs of all of the primes which do not exceed x.

$L(1) = 0 \quad L(2) = \log 2 \quad L(8) = \log (2.3.5.7)$

Since $p^n \leq x$ is equivalent to $p \leq x^{1/m}$, equation (3) can also be written as

(5) $W(x) = L(x) + L(x^{1/2}) + \dots = \sum L(x^{1/m})$ where the series breaks off when $x^{1/m} < 2$ or $m > \log x / \log 2$.

Before turning our attention to the work of Tchebycheff we shall derive the following useful inequality

(6) $L(x) \leq N(x) \log x$

We can express $N(x)$ in series form as follows : $N(x) = \sum_{p \leq x} 1$ where the notation means that the number of units to be added together is the number of primes less than x.

Hence using this form and definition 4 we have

$$L(x) = \sum_{p \leq x} \log p \leq \log x \sum_{p \leq x} 1 = N(x) \log x$$

The Work of Tchebycheff

Our aim in this section is to demonstrate the mathematics used by Tchebycheff in proving two important theorems. The first is that $N(x)$ is of order x and the second is that the limit, if existent, of $N(x) \log x/x$ is one. Before we can prove these two theorems of Tchebycheff we will have to prove two auxiliary theorems. Namely that $W(x) = L(x)+O\{x^{1/2}(\log x)^2\}$ and that both $L(x)$ and $W(x)$ are of order x. Our proof of these last two theorems will parallel the work on pages 345 - 346 in Hardy and Wright.

<u>Theorem</u> 3. $W(x) = L(x) + O\{x^{1/2} (\log x)^2\}$

Proof - From the definition of $L(x)$ we see that

$L(x) < x \log x$ for $x \geq 2$. Hence

(7) $L(x^{1/m}) < x^{1/m} \log x \leq x^{1/2} \log x$ for $m \geq 2$.

We know from (5) that the series $W(x) = \sum L(x^{1/m})$ ends when m exceeds $\log x/\log 2$ and hence the series has at most $\log x/\log 2$ terms.

Summing both sides of (7) we obtain

$\sum L(x^{1/m}) \quad \frac{\log x}{\log 2} (x^{1/2} \log x)$, and adding $L(x)$ to both sides

$$W(x) = L(x) + \sum L(x^{1/m}) \leq L(x) + O\{x^{1/2} (\log x)^2\}$$

<u>Theorem</u> 4 The functions $L(x)$ and $W(x)$ are of order x:

(8) $Ax < L(x) < Ax$ and $Ax < W(x) < Ax$

Due to the results of theorem 3 it is sufficient to prove

(9) $L(x) < Ax$ and

(10) $W(x) > Ax$

Proof of (9) - If n is an integer the binomial coefficient

$$\frac{(n+1)\,(n+2)\,\ldots\ldots 2n}{n!} = \frac{(2n)!}{n!\,n!}$$

is an integer less than $(1+1)^{2n}$. It is divisible by all the primes between $n+1$ and $2n$.

Thus $\prod_{n < p \leq 2n} p < \frac{(2n)!}{n!\,n!} < (1+1)^{2n} = 2^{2n}$

and taking the log of both sides

$\log \prod_{n < p \leq 2n} p \leq 2n \log 2$ or

$L(2n) - L(n) < 2n \log 2$

Suppose $x = 2^m$, then

$$\begin{aligned} L(x) &= L(2^m) - L(2^{m-1}) + L(2^{m-1}) - L(2^{m-2}) + \dots \\ &< (2^m + 2^{m-1} + \dots + 2) \log 2 < 2^{m+1} \log 2 \\ &= 2x \log 2 . \end{aligned}$$

On the other hand if $2^{m-1} < x < 2^m$, then

$L(x) \leq L(2^m) < 2^{m+1} \log 2 < 4x \log 2.$

Hence in either case (9) is true with $A = 4 \log 2$.

Proof of (10) - The proof of this inequality is so similar to the proof of (9) that we will omit it.[9]

We will now prove the first of Tchebycheff's theorems.

Tchebycheff's Theorems

Theorem 5 $N(x) \asymp x/ \log x$ or $Ax/ \log x < N(x) < Ax/ \log x$

Proof - From (6) we have

$N(x) \log x > L(x)$. Hence using (9) we have

$$N(x) > \frac{L(x)}{\log x} > \frac{A(x)}{\log x}$$

On the other hand

$$\begin{aligned} L(x) &\geq \sum_{x^{1/2} < p \leq x} \log p \geq \tfrac{1}{2} \log x \sum_{x^{1/2} < p \leq x} 1 \\ &= \tfrac{1}{2} \log x \left\{ N(x) - N(x^{1/2}) \right\} \geq \tfrac{1}{2} \log x \left[N(x) - x^{1/2} \right]. \end{aligned}$$

Hence $N(x) \leq 2L(x) / \log x + x^{1/2}$ and

$N(x) < Ax/ \log x$

9. For a proof see Hardy and Wright, page 345

By using Tchebycheff's methods we can prove that if $N(x) \log x/x$ approaches a limit as x approaches infinity, then this limit is one. This will, of course, not prove that the limit is one since $N(x) \log x/x$ could oscillate without approaching a limit. This is as far as Tchebycheff was able to go in his attempt to prove the prime number theorem. We can prove that as x approaches infinity the limit, if existent, of each of the three ratios $W(x)/x$, $L(x)/x$, and $N(x) \log x/x$ will be one. We will omit the proof of the second of these since it is so similar to that of the first. Our proofs of the first and third of these will depend largely on that given by Mathews.[10]

<u>Theorem</u> 6. If the limit, as x approaches infinity, of $W(x)/x$ exists, this limit is one.

Proof - Our proof will consist of three parts. First we will prove that $\lim_{x\to\infty} V(x)/x \log x = 1$. Then, using this property , we shall prove by means of contradiction that given any $a > 1$ there exists an infinite number of positive integers x such that $W(x) < ax$; and also given any $b < 1$ there exists an infinite number of positive integers x such that $W(x) > bx$.

<u>Part</u> 1. Proof that $\lim_{x\to\infty} V(x)/x \log x = 1$

Let $F(x)$ be used instead of $[x]$. Define $C(x)$ to be 0 or 1 according as x is less than or greater than one. We have

(11) $F(x) = C(x) + C(x/2) + \ldots\ldots C(x/n) + \ldots = \sum_{1}^{\infty} C(x/n)$

The series is just 1+1+ .... to $F(x)$ terms, i.e., it is $F(x)$.

(12) Let $s_n = 1 + \frac{1}{2} + \ldots\ldots 1/n$, and

(13) $V(x,n) = F(x) + F(x/2) + \ldots F(x/n)$; Now for $p > 1$

$F(x)/p - 1 < F(x/p) < F(x)/p$, hence

(14) $S_n F(x) - n + 1 < V(x,n) < S_n F(x)$

10. <u>Theory of Numbers</u>, page 347

Now $\log \langle (p+1)/p \rangle < 1/p < \log \langle p/(p-1) \rangle$ and so

$\log(n+1) - \log 2 < S_n - 1 < \log n$

and $\log(n+1) < S_n < 1 + \log n$

From this and (14) we have

(15) $F(x) \log(n+1) - n+1 < V(x,n) < F(x) \langle 1 + \log n \rangle$

Let $V(x) = F(x) + F(x/2) + \ldots . F(x/n) + \ldots = \sum_1^{\infty} F(x/n)$;

Since $F(x/n) = 0$ if $n > F(x)$ we have:

$V(x) = V\langle x, F(x) \rangle$; hence from 15 we obtain

$F(x) \log \langle F(x) + 1 \rangle - F(x) + 1 < V(x) < F(x) \langle 1 + \log F(x) \rangle$

Dividing by $x \log x$ we have

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

Part 2. We assume that given any a greater than one, there exists only a finite number of positive integers x for which $W(x) < ax$. We will show this assumption leads to a contradiction and hence that there exists an infinite number of such x.

Let y be the greatest value of x for which this is so, then for all values of x greater than y, $W(x) > ax$.

We can find a finite number d such that for all integral values of x

(16) $W(x) > a(x+1) - d$

If x exceeds 1, $F(x)$ is less than x+1 and $C(x)$ equals 1.

If x is less than one, $W(x) = F(x) = C(x) = 0$.

From this and (16) we have

(17) $W(x) > aF(x) - dC(x)$

Now change x successively into $x/2$, $x/3$, $x/4$, ... and add; then since the inequality only fails when $W(x)$, $F(x)$ and $C(x)$ all vanish, we have

(18) $T(x) = \sum_1^{\infty} W(x/n) > a \sum_1^{\infty} F(x/n) - d \sum_1^{\infty} C(x)$ and

(19) $\dfrac{T(x)}{x \log x} > \dfrac{a\, V(x)}{x \log x} - \dfrac{d\, F(x)}{x \log x}$

The limit of $V(x)/(x \log x)$ is 1; the limit of $F(x)/x$ is 0; and the limit of $T(x)/(x \log x)$ is 1.

Thus (19) implies that 1 exceeds a which is our contradiction. Hence $W(x) < ax$ for an infinite number of positive integers.

Part 3 By this method we can also show that given any b less than 1, there exists an infinite number of x such that $W(x) > bx$. We omit the proof since it would be repetitious.

Theorem 7. If the limit, as x approaches infinity, of $L(x)/x$ exists, this limit is one.

Theorem 8. If the limit, as x approaches infinity, of $N(x) \log x/x$ exists, this limit is one.

Proof - From (6) we have $N(x) \log x > L(x)$, hence when $L(x) > ax$ we have

$$(20) \quad N(x) > \frac{ax}{\log x}$$

Using the results of theorem 7 we see that whenever a is less than 1, there is an infinity of integers for which $N(x) > \frac{ax}{\log x}$; also when a exceeds 1, there is an infinity of integers for which $N(x) < \frac{ax}{\log x}$.

Hence if $N(x) \log x/x$ converges to a limit when x becomes infinite, that limit must be one.

The Zeta- Function

Certain properties of the Riemann zeta-function are needed to prove the prime number theorem. The importance of this function in the theory of primes is that it combines two expressions, one containing the primes explicitly while the other does not. In this section we will define the zeta- function. Then we will show its relation to $A(n)$. We will state a property of Dirichlet series and use this property to prove that $Z(s)$ is analytic on the line $r = 1$. Finally we will prove several theorems concerning the distribution of the zeros of the zeta-function. The results obtained here will be used in proving the prime number theorem in the next section.

<u>Definition</u> 6 The Riemann zeta-function $Z(s)$ can be expressed by the two formulas :

(20) $Z(s) = \sum_{1}^{\infty} n^{-s}$ where $n=1, 2, 3, \ldots,$ and

(21) $Z(s) = \prod_{p} (1-p^{-s})^{-1}$ where p runs through all the primes. S is a complex variable $s = r + it$. Either of these can be taken as the definition of $Z(s)$. The infinite series (20) is convergent for $r > 1$, and uniformly convergent in any finite region for which $r > 1 + e$; where e exceeds zero. It therefore defines an analytic function $Z(s)$ regular for r greater than one.

The infinite product (21) is absolutely convergent for $r > 1$. Expand each of the factors. $(1-p^{-s}) = 1 + P^{-s} + p^{-2s} + \ldots$. Now $\sum_{p} |p^{-s}| = \sum_{p} p^{-r}$ is absolutely convergent for $r > 1$, since it is merely some of the terms from the series $\sum n^{-r}$ which we know converges for $r > 1$. Since we have absolute convergence we can multiply the series together. Each term in the resulting series will be n^{-s} where n is some integer. Each integer will appear once and only once since each integer is uniquely factorable into prime factors. Thus $(20) \equiv (21)$.

The convergence is uniform for $r \geq r' > 1$. The identity of (20) and (21) is an analytic equivalent of the theorem that the expression of an integer in prime factors is unique.[11]

One of the properties of the zeta-function is that it has no zeros for r greater than one. This can be argued as follows. Equating (20) and (21) we have

$$Z(s) = \sum_{1}^{\infty} n^{-s} = \prod_{p} (1-p^{-s})^{-1} .$$

We know that Z(s) is convergent for r greater than one. Since none of the factors of the convergent infinite product is zero the product itself cannot be zero. Thus for r greater than one, Z(s) has no zeros.[12]

<u>Theorem</u> 9. $\quad \dfrac{-Z'(s)}{Z(s)} = \sum A(n)n^{-s}$

Proof - Taking the logarithms of both sides of (21) we obtain

(22) $\quad -\log Z(s) = \sum \log (1-p^{-s})$ where the convergence is also uniform for $r \geq 1 + e$, $e > 0$.

We can differentiate (22) since the derived series is uniformly convergent for $r \geq 1 + e$ since the n^{th} prime exceeds n and the series is majorized by $\sum n^{-s} \log n$. We obtain

$$\frac{-Z'(s)}{Z(s)} = \sum \frac{p^{-s} \log p}{1-p^{-s}}$$

$$= \sum \frac{\log p}{p^{s}} (1 + p^{-s} + p^{-2s} + \ldots .)$$

$$= \sum \log p \sum_{m=1}^{\infty} p^{-ms}$$

Since the double series $\sum \sum p^{-ms} \log p$ is absolutely convergent for $r > 1$, it can be written as

(23) $\quad \dfrac{-Z'(s)}{Z(s)} = \sum_{p,m} p^{-ms} \log p$. Now consider the series

(24) $\sum A(n)n^{-s}$ which equals

$\sum \log p/n^{-s}$ for $n = p^{m}$ and is zero otherwise.

Hence $\sum A(n)n^{-s} = \sum_{p,m} p^{-ms} \log p$ and from (23)

(25) $\quad -Z'(s)/Z(s) = \sum A(n)n^{-s}$

11. Hardy and Wright, page 245

12. For a formal proof of this property see <u>Theory of the Riemann Zeta-Function</u>, page 2

At this point we wish to prove that $Z(s)$ is analytic for $r > 0$ except for a simple pole at $s = 1$. We will need a property of Dirichlet series.

Definition 7. A Dirichlet series is a series of the form $\sum a_n e^{-j_n s}$ where $j_1 < j_2 \ldots\ldots j_n \rightarrow \infty$. The j_n's are real numbers and s is a complex variable.

The Riemann zeta-function is defined by a Dirichlet series where $a_n = 1$ and $j_n = \log n$.

The property we need is as follows. If the Dirichlet series converges for any point s' then it converges uniformly throughout the sector for which we have $\arg(s - s') \leq \pi/2 - q$ where q is any positive number less than $\pi/2$; and therefore defines an analytic function at any point in the half plane to the right of s'. [13]

Theorem 10. $Z(s)$ is analytic for $r > 0$ except for a simple pole at $s = 1$. [14]

Proof - Consider the function

$$\begin{aligned} g(s) &= (1 - 2^{1-s})\, Z(s) \\ &= \sum n^{-s} - \sum 2/(2n)^2 \\ &= 1 - 2^{-s} + 3^{-s} - 4^{-s} + \ldots\ldots \end{aligned}$$

This series converges for any $r > 0$. Hence by the property of Dirichlet series, $g(s)$ is analytic for $r > 0$ and $Z(s) = \dfrac{g(s)}{1-2^{1-s}}$ is analytic in the right half plane except where the denominator equals zero. The denominator vanishes for $2^{s-1} = 1$, or $(s-1)\log 2 = 2\pi ki$ $(k = 0, \pm 1, \pm 2, \ldots)$ or $s = 1 + 2\pi ki/\log 2$

In a similar manner it can be shown that a second function $h(s) = (1-3^{1-s})\, Z(s)$ is analytic for any $r > 0$. Hence $Z(s)$

13. For a proof of this property see Titchmarsh, Theory of Functions, pages 288 - 289
14. Our proof follows closely that due to Bochner, pages 93-94

is analytic except where $1-3^{1-s} = 0$, i.e., where $s = 1 + \frac{2\pi ki}{\log 3}$

The only point common to these two sets of points is the point $s = 1$, or else $\log 3 / \log 2 = a/b$, i.e., $3^b = 2^a$ where a and b are integers; but this is impossible since any integer has a unique factorization into primes, Thus $Z(s)$ is analytic for $r > 0$ except for a simple pole at $s = 1$.

It was proved independently by Hadamard and Poussin in 1896 that $Z(s)$ has no zeros on the line $r = 1$. They were able to prove the prime number theorem by showing that it was a consequence of this theorem. We will present, for historical reasons, both Hadamard's argument and Poussin's proof of this property of the zeta - function.[13]

Theorem 1. $Z(1 + it) \neq 0$ for all values of t.

A. Hadamard's argument.

If we integrate (23) we have for $r > 1$

$$\log Z(s) = \sum_p \sum_{m=1}^{\infty} p^{-ms}/m .$$

This can be written as equal to $\sum_p p^{-s} + f(s)$ where $f(s)$ is regular for $r > \frac{1}{2}$. Since $Z(s)$ has a simple pole at $s = 1$, then as $r \to 1$

(26) $\sum p^{-r} \sim -\log(r-1)$. This is because

$$(1-2^{1-s})\, Z(s) = (1^{-s} + 2^{-s} + 3^{-s} + \dots\dots) - 2(2^{-s} + 4^{-s} + 6^{-s} \dots)$$

$$= 1^{-s} - 2^{-s} + 3^{-s} - \dots\dots,$$ and this series converges to log 2 for $s = 1$. Hence

$$(s-1)\, Z(s) = (1-2^{1-s})\, Z(s) \frac{(s-1)}{1-2^{1-s}} \to \frac{\log 2}{\log 2} = 1 \quad \text{and}$$

$$Z(s) \sim 1/s-1$$

Now let us assume that $s = 1 + it'$ is a zero of $Z(s)$ and hope for a contradiction. If $s = 1 + it'$, then as $r \to 1$

(27) $\sum_p \cos(t' \log p)/p^r = \log |Z(s)| - R\,(f(s) \sim \log(r-1)$

13. Both will be similar to those in The <u>Theory of the Riemann Zeta-Function</u>, pages 39 - 41

This is because $\sum_p p^{-r} p^{-it} = \sum_p p^{-r}\,(e^{-it\log p})$.
Comparing (26) and (27) we see that cos(t' log p) must be approximately -1 for most values of p. But then cos(2t'log p) is approximately 1 for most values of p, and
$\log\left|Z(r+2it')\right| \sim \sum_p \cos(2t'\log p)/p^r \sim \sum_p p^{-r} \sim -\log(r-1)$.
Thus 1 + 2it' is a pole of Z(s) which is our contradiction.

B. Poussin's Proof that $Z(1+it) \neq 0$

His proof also makes use of a relation between Z(r+it) and Z(r+ 2it). The following identity is also used:

(28) $3 + 4\cos t + \cos 2t = 2(1+\cos t)^2 \geq 0$ for all values of t.

Proof - Integrating (23) we have

$$\log Z(s) = \sum_p \sum_{m=1}^{\infty} p^{-ms}/m$$
$$= \sum_p \sum_{m=1}^{\infty} p^{-mr} e^{-it\log p}/m. \quad \text{Hence}$$

(29) $Z(s) = \exp \sum_p \sum_{m=1}^{\infty} p^{-mr} e^{-it\log p}/m$, thus

(30) $|Z(s)| = \exp \sum_p \sum_{m=1}^{\infty} m^{-1} p^{-mr} \cos(mt\log p)$.

Now let $B = |Z(1+e)|^3\,|Z(1+e+it)|^4\,|Z(1+e+2it)|$ and using (30) we have

$$B = \exp \sum_p \sum_{m=1}^{\infty} \frac{3 + 4\cos(mt\log p) + \cos(2mt\log p)}{mp^{m(1+e)}}$$

Since each term in this sum is positive or zero we obtain

(31) $B \geq 1$ for $r > 1$.

From part A we have $Z(s) \sim 1/s-1$, thus

$Z(s) = O(1/s-1)$ and $Z(1+e) = O(e^{-1})$

Let us assume that Z(s) does have a zero at the point s = 1 + it. Then we will have

$Z|(1+e)|^3 = O(e^{-3})$

$Z|(1+e+it)| = O(e^4)$

$Z|(1+e+2it)| = O(1)$. Hence $B = O(e)$ which is a contradiction of (31) if e is sufficiently small. Thus Z(1+it) vanishes for no value of t.

Landau's Proof of the Prime Number Theorem

In this section we will demonstrate Landau's proof of the prime number theorem assuming the validity of his lemma on asymptotic expansions. Before we state Landau's Lemma we will prove that $W(x) \sim x$ is equivalent to the prime number theorem. Proving this theorem is the starting point for several other proofs of the prime number theorem as well as for Landau's.

<u>Theorem</u> 12. $W(x) \sim x$ is equivalent to $N(x) \sim x/\log x$, i.e., to prove the prime number theorem it is sufficient to prove that $W(x) \sim x$.[14]

Proof - From definition 4 we have

$L(x) = \sum_{p \leq x} \log p$. Now this can be written as

(32) $L(x) = \sum_{n \leq x} \left[N(n) - N(n-1)\right] \log n$ since the value within the bracket is 1 or 0 depending on whether n is prime.

Now adding and subtracting $N(n-1)\log(n-1)$ in (32) we have

(33) $$L(x) = \sum_{n \leq x} \left\{N(n) \log n - N(n-1)\log(n-1)\right\} - \sum_{n \leq x} N(n-1) \left[\log n - \log(n-1)\right]$$

Hence setting $R(m) = \sum_{n \leq x} N(n-1) \log\left(1 + \frac{1}{n-1}\right)$ and noting that

$\sum_{n \leq x} N(n) \log n - N(n-1) \log (n-1) = N(m) \log m$, where $m = [x]$

then (33) becomes

(34) $L(x) = N(m) \log m - R(m)$. Thus

(35) $L(m)/m = N(m) \log m/m - R(m)/m$ and if we can show that

a. $L(m)/m \to 1$ and

b. $R(m)/m \to 0$ we will have proved the prime number theorem.

First consider proving a. Rewrite

$$R(m) = \sum_{0 < v \leq x-1} N(v) \log (1 + 1/v)$$

Since for $v > 0$, $\log (1 + 1/v) < 1/v$ we have

14. Our proof will follow closely that in <u>Fourier Analysis</u>, 90-92

(36) $R(m)/m \leq 1/m \sum_{0<v\leq x-1} N(v)/v < 1/(m-1) \sum_{0<v\leq x-1} N(v)/v$

From theorem 2 we know that as $v \to \infty$, $N(v)/v \to 0$. The last term in (36) is an arithmetic mean. We know that if a sequence of real numbers converges to a limit, then the sequence of arithmetic means converges to the same limit. Hence $R(m)/m \to 0$ as $m \to \infty$.

To prove b let us rewrite (5) as

$W(n) = \sum_{p\leq n} \log k + \sum_{p^2\leq n} \log k + \ldots\ldots$, where

the series breaks off for $x^{1/m} < 2$ or $n > \log n / \log 2$.

The number of primes such that $p^k \leq n$ is $N(\sqrt[k]{n})$ which is less than $\sqrt{n}$. Thus

$$W(n)/n - L(n)/n = 1/n \sum_{p^k\leq n} \log p \qquad (k \geq 2)$$

Hence
$$W(n)/n - L(n)/n < \frac{1}{n}\left[\sqrt{n}\log n + \sqrt[3]{n}\log n + \ldots \sqrt[k]{n}\log n\right]$$
$$< \frac{1}{n} \log n\left[\sqrt{n} + \sqrt{n} + \ldots \sqrt{n}\right]$$
$$< \frac{1}{n} \log n \frac{\log n}{\log 2} \sqrt{n} = \frac{1}{\log 2} \frac{\log^2 n}{\sqrt{n}} .$$

Now $\frac{\log^2 n}{\sqrt{n}} \to 0$ as $n \to \infty$. Thus if $W(n)/n \to 1$ so will $L(n)/n$ and the proof of the prime number theorem will be completed. Hence proving $W(n) \sim n$ is equivalent to proving the prime number theorem.

Note that from (3) $W(x) = \sum_{n\leq x} A(n)$. Hence $\sum_{n\leq x} A(n) \sim x$ is also equivalent to the prime number theorem.

<u>Landau's Lemma</u> [15]

(37) Let $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ for $r > 1$. Suppose

(1) $a_n \geq 0$ for $n = 1,2,\ldots\ldots$

(2) $F(s)$ is analytically continuable on to $r = 1$ and has no singularities there except for a pole of order one

15. The work of the remainder of this section will closely parallel the work of Wiener in <u>Fourier Integral</u>, pg.125

at $r = 1$, with principal part $A/(x-1)$

(3) There exists a finite c for which

(38) $F(s) = O(|s|^c)$ for $r > 1$. Then

(39) $A = \lim_{n\to\infty} \frac{1}{m} \sum_1^n a_k$.

Landau's Proof of the Prime Number Theorem

Proof - From (25) we have

$- Z'(s)/Z(s) = \sum_1^\infty A(n)n^{-s}$. We wish to show that

$-Z'(s)/Z(s)$ satisfies the conditions of the previous lemma.

First of all $A(n)$ is by definition not less than zero.

From theorem 10 we know that $Z(s)$ is analytic for $r > 0$ except for a simple pole at $s = 1$. Hence a constant k exists such that

(40) $Z(s) - k/(s-1)$ is analytic at $s = 1$. (the actual value of k turns out to be one)

$Z'(s) + k/(s-1)^2$ is also analytic at $s = 1$.

Hence $- Z'(s) / Z(s) - 1/(s-1)$ is analytic at $s = 1$ so that

$- Z'(s) / Z(s)$ has a pole of order one at $s = 1$ with principal part $1/(s-1)$. In applying (39) to $- Z'(s)/Z(s)$ we have $A = 1$.

The final condition is that (38) be satisfied. We can show that $Z'(s)/Z(s) = o(\log^9 t)$.[16]

Since the hypothesis of the Lemma is satisfied the conclusion is that

$$1 = \lim_{n\to\infty} \frac{1}{n} \sum A(n).$$

But this is merely $\sum A(n) \sim n$ which we have shown is equivalent to the prime number theorem.

16. See Titchmarsh, The Theory of the Riemann Zeta-Function, pg. 44

Bochner's Proof of the Prime Number Theorem

We will now present, in much greater detail, another proof of the prime number theorem. This section will follow closely the work on pages 84 - 94 of Bochner's Fourier Analysis. We will state a theorem of Bochner's concerning asymptotic expansions which is essential to his proof of the main theorem. Since the proof of this auxiliary theorem is rather lengthy we will just outline its main points so as to indicate the level of mathematics needed to prove the prime number theorem. Finally, making use of the theorem on asymptotic expansions and the property of Dirichlet series stated after definition 7, we will prove the prime number theorem.

Theorem 13. Bochner's Theorem on the asymptotic behavior of the partial sums of the coefficients of a Dirichlet series.

Let $F(s) = \sum a_n e^{-j_n s}$. Suppose

(1) j_n is not less than zero for $n = 1, 2, \ldots, j_i < j_{i+1}, j_n \to \infty$.

(2) a_n is not less than zero for $n = 1, 2, \ldots$.

(3) The series converges to $F(s)$ for $r > 1$ and $F(s)$ is analytic for $r \geq 1$, except at the point $s = 1$.

(4) At the point $s = 1$, $F(s)$ has a simple pole with residue A.

Then, as $n \to \infty$, $A_n = \sum_1^n a_v \sim Ae^{j_n}$, i.e.,

$$\lim_{n\to\infty} A_n e^{-j_n} = A$$

Proof - Denote by Λ the sector for which we have $\arg(s-s') \leq \frac{\pi}{2} - q$, where q is any positive number less than $\pi/2$.

The partial sums of $F(s)$ at point s in Λ are

$$(41) \quad S_n(s) = \sum_{v=0}^{n} a_v e^{-j_v s} = \sum_{v=0}^{n} (A_v - A_{v-1}) e^{-j_v s}$$
$$= \sum_{v=0}^{n-1} A_v (e^{-j\ s} - e^{-j\quad s}) + A_n e^{-j_n s}.$$

(42) $F(s)$ can be written as $F(s) = \sum_{v=1}^{\infty} A_n (e^{-j_n s} - e^{-j_{n+1} s})$ if

$\left| A_n e^{-j_n s} \right| \to 0$ as $n \to \infty$. To show this consider

$$\left| A_n e^{-j_n s} \right| = \sum_{\nu=1}^{n} a_\nu e^{-j_n r'} e^{-j_n (r-r')}$$
$$\leq \sum_{\nu=1}^{n} a_\nu e^{-j_\nu r'} e^{-j_n (r-r')}$$
$$= S_n(r')\, e^{-j_n (r-r')}$$ which goes to zero as n goes to infinity.

Substituting $e^{-j_n s} - e^{-j_{n+1} s} = s \int_{j_n}^{j_{n+1}} e^{-us}\,du$ in (42) we have

$$(43) \quad F(s) = \sum_{1}^{\infty} A_n s \int_{j_n}^{j_{n+1}} e^{-us}\,du.$$

Now introduce the step function

$A(u) = A_n$. $\quad j_n \leq u \leq j_{n+1}$ and (43) becomes

$$(44) \quad F(s) = \sum_{n=0}^{\infty} s \int_{j_n}^{j_{n+1}} A(u)\, e^{-us}du$$
$$= s \int_0^\infty A(u)\, e^{-us} du\ .$$

We will prove that $A(u)\, e^{-u} \to A$ as $u \to \infty$ which is at least as strong a statement as the statement of the theorem.

By definition F(s) is analytic except for a simple pole with residue A at s = 1. We may choose A = 1 and then write

$F(s) = 1/(s-1) + H(s)$, where $H(s)$ is analytic for $r > 1$.

We now need the identity $1/(s-1) = \int_0^\infty e^{-(s-1)u} du$.

Combining the last two equations we have

$F(s) - s/(s-1) = s \int_0^\infty \left[A(u) - e^{u}\right] e^{-us} du = s\, g(s).$

This function is analytic for $r > 1$.

Let $e^{-u}A(u) = B(u)$. (Note, now all we have to prove is that $B(u) \to 1$.)

(45) Now $g(s) = \int_0^\infty \left[B(u) - 1\right] e^{-(s-1)u}$.

It can be shown that

$g(1 + e + it) = g_e(t) = \int_0^\infty \left[B(u) - 1\right] e^{-eu} e^{-itu}$ converges uniformly to $g(1+it)$ in any finite interval $-2k \leq t \leq 2k$.

We now introduce the Fejer kernel[17] and form the transform

$$\frac{1}{2}\int_{-2K}^{2K} e^{iyt}\left(1 - \frac{|t|}{2k}\right) g_e(t)\,dt$$

$$(46)\qquad = \frac{1}{2}\int_{-2K}^{2K} e^{iyt}\left(1 - \frac{|t|}{2K}\right)dt \int_0^\infty \left[B(u) - 1\right] e^{-eu} e^{-itu}du.$$

Now for a fixed y and a finite t-interval and an infinite u-interval we wish to change the order of integration. This can be done since we can show that

$\int_0^\infty \left[B(u) - 1\right] e^{-eu}e^{-itu}du$ converges uniformly in t.

Interchanging the order of integration we have

$$(47)\qquad \frac{1}{2}\int_{-2K}^{2K} e^{iyt}\left(1 - \frac{|t|}{2k}\right) g_e(t)\,dt =$$

$$\frac{1}{2}\int_0^\infty \left[B(u) - 1\right] e^{-eu}\,du\int_{-2K}^{2K} e^{i(y-u)t}\left(1 - \frac{|t|}{2k}\right) dt$$

It can be shown that

$$\frac{1}{2}\int_{-2K}^{2K} e^{-ict}\left(1 - \frac{|t|}{2k}\right)dt = \frac{\sin^2 kc}{kc^2}$$

Thus we may write (47) as

$$\frac{1}{2}\int_{-2K}^{2K} e^{iyt}\left(1 - \frac{|t|}{2k}\right) g_e(t)dt = \int_0^\infty \left[B(u) - 1\right] e^{-eu}\frac{\sin^2 k(y-u)}{k(y-u)^2}du$$

Now let $k(y-u) = v$, with k fixed. Then by theorems concerning monotone convergence we may obtain the result

$$(48)\qquad \lim_{y\to\infty}\int_{-\infty}^{Ky} B(y - v/k)\,\sin^2 v/v^2 = \pi \text{ for every k.}$$

We will make use of this result to prove that $\lim_{u\to\infty} B(u) = 1$ and hence prove theorem 13.

We will use two steps and show

(1) $\overline{\lim}_{u\to\infty} B(u) \leq 1$ and (2) $\underline{\lim}_{u\to\infty} B(u) \geq 1$.

17. For a discussion of the Fejer kernel $\left(1 - \frac{|t|}{2k}\right)$ see Bochner, pages 36-37

For (1) we choose a fixed a such that $0 < a < ky$. Then

$$(49)\ \pi \geq \overline{\lim_{y\to\infty}} \int_{-a}^{a} B(y-v/k)\sin^2 v/v^2\,dv.$$

By definition $B(u) = A(u)e^{-u}$. Since $A(u)$ is monotonically increasing

$$e^{y-a/k}B(y-a/k) \leq e^{y-v/k}B(y-v/k)\ .$$ Then

$$B(y-v/k) \geq e^{(v-a)/k}B(y-a/k).$$ Substituting this in (49) we have

$$\pi \geq \overline{\lim_{y\to\infty}} \int_{-a}^{a} e^{(v-a)/k}\sin^2 v/v^2 dv.\ B(y-a/k) \quad \text{and}$$

$$\pi \geq \int_{-a}^{a} e^{-2a/k}\sin^2 v/v^2\,dv.\overline{\lim_{y\to\infty}} B(y-a/k)$$

$$(50) \qquad = e^{-2a/k}\int_{-a}^{a}\sin^2 v/v^2 dv.\overline{\lim_{y\to\infty}} B(y)\ .$$

Now let $a \to \infty$ and $k \to \infty$ in such a way that $a/k \to 0$. Then from (50) we have

$$\pi \geq \overline{\lim_{y\to\infty}} B(y) \text{ or } \overline{\lim_{y\to\infty}} B(y) \leq 1 \quad \text{which is (1)}$$

By means of similar inequalities we can show that (2) holds, i.e., $\underline{\lim_{y\to\infty}}\ B(y) \geq 1$.

Hence from (1) and (2) we have $\lim_{v\to\infty} B(u) = 1$. This is $\lim_{v\to\infty} A(u)\,e^{-u} = 1$ and our proof of theorem 13 is complete.

<u>Theorem</u> 14 <u>Bochner's Proof of the Prime Number Theorem</u>

We will now use the preceding theorem together with the zeta-function, the arithmetical function $A(n)$, and the convergence property of Dirichlet series to prove the prime number theorem.

Proof - Form the Dirichlet series

$$(51) \quad F(s) = \sum A(n)n^{-s}$$

Suppose $F(s)$ satisfies the conditions of theorem 13 with $A = 1$. The conclusion of that theorem will then be

$\sum_{n\leq x} A(n) \sim n$ which we have proven is equivalent to the prime number theorem. Hence to prove theorem 14 we only have to show that $F(s)$ satisfies the hypothesis of theorem 13.

Conditions 1 and 2 are clearly satisfied. We have only to prove that the series converges to $F(s)$ for $r > 1$, and that $F(s)$ is analytic for $r \geq 1$ except at the point $s = 1$ where $F(s)$ has a simple pole with residue 1.

From theorem 9 we have $-Z'(s)/Z(s) = \sum A(n)n^{-s}$ and the series converges for $r = 1$. Hence by the convergence property of Dirichlet series it defines an analytic function for $r \geq 1$. We proved, while demonstrating Landau's proof of the prime number theorem, that $-Z'(s)/Z(s)$ has a simple pole with residue 1 at $s = 1$. Also, from theorem 11 we know that $Z(s)$ vanishes at no point on the line $s = 1$. Hence $F(s)$ satisfies all the conditions of theorem 13 and our proof is complete.

Bibliography

In addition to the texts cited in the thesis this list includes several other books which contain material relevant to the subject. Since this material differs, for the most part, from that which was included merely in method of approach and not in content, it was omitted.

E.T.Bell, The Development of Mathematics, (New York, McGraw - Hill Book Company, Inc., 2nd edition, 1945)

S.Bochner, Fourier Analysis, (Princeton University, 1937)

F.Cajori, A History of Mathematics, (New York, Macmillan Company, 1919)

R.Courant and H.Robbins, What is Mathematics, (New York, Oxford University Press, 1941)

T.Estermann, Introduction to Modern Prime Number Theory, (Cambridge University Press, 1952)

G.H.Hardy and E.M.Wright, The Theory of Numbers, (Oxford, At the Clarendon Press, 1938)

G.B.Mathews, Theory of Numbers, Part 1, (New York, G.E.Stechert and Co., Reprint 1927)

J.R.Newman, The World of Mathematics, Vol. 1, (New York, Simon and Schuster, 1956)

D.E.Smith, A Source Book in Mathematics, (New York, McGraw - Hill Book Company, Inc., 1927)

E.C.Titchmarsh, The Theory of the Riemann Zeta - Function, (Oxford, At the Clarendon Press, 1951)

E.C.Titchmarsh, The Theory of Functions, (Oxford, At the Clarendon Press, 1932)

D.V.Widder, The Laplace Transform, (Princeton University Press, 1946)

N.Wiener, The Fourier Integral and Certain of its Applications, (New York, Dover Publications, Inc., 1933)