Letters to an Egyptian Princess

# An Essay on the Distribution of Prime Numbers, Including the Prime Number Theorem and Dirichlet's Theorem on Primes in Arithmetic Progressions

By
Chris Wuthrich

Supervisor:
W. Parry

THIRD YEAR ESSAY
AT THE MATHEMATICS INSTITUTE
UNIVERSITY OF WARWICK

# Foreword of the Editor

Times have changed since LEONARD EULER wrote his "Lettres à une princesse d'Allemagne sur divers sujets de physique et de philosophie" [18]. Princesses in the today's fast world don't have any time to learn the art of mathematics, anymore.

I decided to publish here the letters which the mathematician C. W. wrote to an Egyptian princess shortly before this country was shaken by the events in the palace. I hope that these letters will shed some light on this matter. Unfortunately the answers of the princess couldn't be found anymore.

Nothing of the original letters has been omitted. Many notes have been included which are important for the understanding of the text. Titles of the chapters, theorem and formula numbering, references and the bibliography have been added later to make it easier reading.

The letters have been written in English, although the author's native language is Bernese. For the sake of conserving the original text only a few mistakes have been corrected.

Moreover, I should say that some of the sources for the author's remarks and historical notes are known, namely [36] pp. 3 - 55; pp. 925 - 946 (appendix by PAUL T. BATEMAN), [6] pp. 132 - 138, [3] pp. 1 - 12; p. 293, [29] pp. 1 - 8, [19] pp. 452 - 454, [11] and [42].

I used `WinEdt`, $\mathcal{AMS}$-LaTeX and Mathematica.

I have the pleasure to thank the persons without whose help this essay wouldn't have been possible:

*Dina El Mehelmy*

*Sylvia Guibert*

*Olaf Dümmer*

*Alessandra Ibba*

The editor : C. M. W.

# Contents

# Part I

# The Prime Number Theorem

"Die gütige Mittheilung Ihrer Bemerkungen über die Frequenz der Primzahlen ist mir in mehr als einer Beziehung interessant gewesen. Sie haben mir meine eigenen Beschäftigungen mit demselben Gegenstande in Erinnerung gebracht, deren erste Anfänge in eine sehr entfernte Zeit fallen, ins Jahr 1792 oder 1793, wo ich mir Lambertsche Supplemente zu den Logarithmentafeln angeschafft hatte. Es war noch ehe ich mit feineren Untersuchungen aus der höhern Arithmetik mich befasst hatte eines meiner ersten Geschäfte, meine Aufmerksamkeit auf die abnehmende Frequenz der Primzahlen zu richten, zu welchen Zweck ich dieselben in den einzelnen Chiliaden abzählte, und die Resultate auf einem der angehefteten weissen Blätter verzeichnete. Ich erkannte bald, dass unter allen Schwankungen diese Frequenz durchschnittlich nahe dem Logarithmus verkehrt proportional sei, so dass die Anzahl aller Primzahlen unter einer gegebenen Grenze $n$ nahe durch das Integral

$$\int \frac{du}{\log n}$$

ausgedrückt werde, wenn der hyperbolische Logarithm. verstanden werde."

## Letter 1

# Introduction

My dear princess,
I hope I am allowed to say that I was really surprised, not only by the King's sudden decision that you should stop your studies, but even more by your letter. You asked me to continue to teach you about prime numbers, these fascinating numbers which mathematicians often talk about. Of course, I am conscious of the danger, but I will take the risk. Because it is a great honour to me that I can continue to give lessons to such a motivated and motivating student as you are. Or, how EULER wrote:[(a)]

> "Comme l'espérance de pouvoir continuer á Votre Altesse mes instruction dans la géométrie semble de nouveau être reculée, ce qui me cause un très-sensible chagrin, je souhaiterais y pouvoir suppléer par écrit, autant que la nature des objets le permet."

I would like to show you in several letters (if the King doesn't change his mind) the development of the theory of the distribution of primes. It will include the famous prime number theorem and the theorem about primes in arithmetic progression which was discovered by DIRICHLET.

Let me first give you a little explanation on the main questions we are talking about. In the first part, our interest lies in the $\pi(x)$ function, it denotes the numbers of prime which are less or equal than $x$. I think you know that there is no strict law for primes, they are spread in a chaotic way over the integers. In your country, in Alexandria, the story of primes starts when EUCLID proved that there exists infinitely many primes. Maybe, the first to pronounce the possibility of a theorem that characterizes the distribution of prime numbers was ADRIEN M. LEGENDRE in 1789.[(b)] Later in 1808, he was a bit more precise when he wrote:[(c)]

> Quoique la suite des nombres premiers soit très irrégulière, on peut cependant trouver avec une précision très-satisfaisante, combien il y a de nombres depuis 1 jusqu'à une limite donnée $x$. La formule qui résout la question est
>
> $$y = \frac{x}{\log x - 1.08366},$$
>
> $\log x$ étant un logarithme hyperbolique.

In other words he thought that $\pi(x)$ behaves like this function when $x$ is sufficiently large. LEGENDRE knew that he wasn't able to proof this conjecture.

But I will show you now what CARL F. GAUSS thought about this formula: [ ... ][(d)] So in other words: at the age of 15, GAUSS took tables of prime numbers and counted how many there are in each block of 1000. He realized that the probability for a number $n$ to be prime is about $\frac{1}{\ln n}$. I tried to do the same experiment as GAUSS. Here is a graphic showing the number of primes in the intervals of length 10'000. I also plotted the graph of the function $10'000/\ln x$. Gauss saw that there was a connection between the $\pi(x)$ function and the integral $\mathrm{Li}(x) = \int_1^x \frac{du}{\ln u}$.

---

[(a)] first letter of EULER in [18]
[(b)] see [38]
[(c)] see [39] or [36] p. 5
[(d)] the text which the author copied from [20] or [36] p. 37 is printed on the title page of this part.

But what kind of relation? It is impossible that the absolute error $\pi(x) - \mathrm{Li}(x) \to 0$ as $x \to \infty$, this is much too strong. But we may hope that the relative error tends to zero

$$\lim_{x\to\infty} \frac{\pi(x) - \mathrm{Li}(x)}{\mathrm{Li}(x)} = 0;$$

this is the same as

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1.$$

At the end of the letter, there is the plot of this fraction for $x < 10^6$.

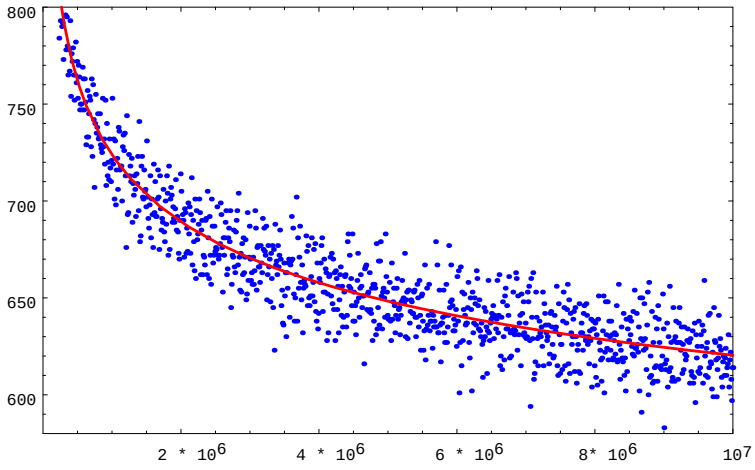



Figure 1.1: The experiment of Gauss

This makes it look really probable. But we have to be careful: The same graph give us the impression that $\mathrm{Li}(x)$ is always bigger than $\pi(x)$. Littlewood proved that this empiric conjecture is wrong,[(e)] the graph above cuts the asymptotic line infinitely many times. So, although the formulae which were given by Gauss and Legendre gives good approximations for $\pi(x)$, we should better be a little bit more careful.

I think you got an impression about the problem I will write you about, but still you are not aware of the immense difficulties we will have to face. And what a detour we will have to make to get to our aim! Your humble servant.

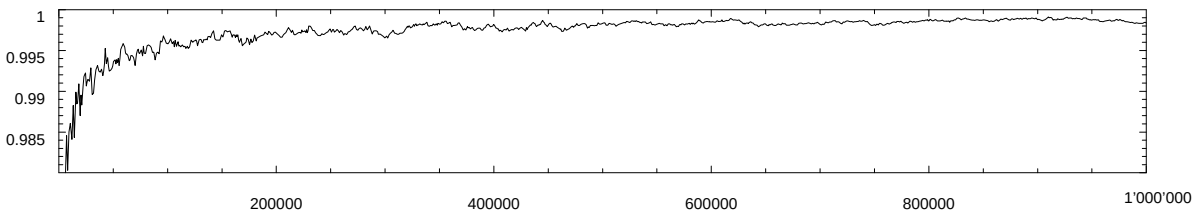



Figure 1.2: The relative error

[(e)] see [24]

## Letter 2

# The Functions of Chebyshev

My dear princess,
The King, you may know it already, told me officially that I am released from my teaching in the palace. He offered me a place at the technical college. He sounded very determined.

So I am writing you this second letter from my new flat in the city center. In the first one I was talking about $\pi(x)$ and the conjectures made by GAUSS and LEGENDRE. Both of them knew that a proof of such a formula would be difficult. CHEBYSHEV made the first step towards this theorem which ABEL described by "Følgende Theorem som findes der og som vistnok er det mærkværdigste i hele Mathematiken kan jeg [ikke] afholde mig fra at afskrive."[(a)] His idea was to consider two other functions which are easier to work with.

I first define the von Mangoldt function $\Lambda(n)$ to be $\ln p$ if $n$ is a power of a prime number $p$ and to be 0 otherwise. CHEBYSHEV's function are[(b)]

$$\vartheta(x) := \sum_{p \le x} \ln p \tag{2.1}$$

and

$$\psi(x) := \sum_{p^m \le x} \ln p = \sum_{n \le x} \Lambda(n), \tag{2.2}$$

both for $x > 0$. These two functions are connected by

$$\psi(x) = \vartheta(x) + \vartheta\left(x^{\frac{1}{2}}\right) + \vartheta\left(x^{\frac{1}{3}}\right) + \cdots,$$

the series being finite, since $\vartheta(x) = 0$ for $x < 2$. This formula can be used to write

$$\psi(x) - 2\psi(\sqrt{x}) = \vartheta(x) - \vartheta\left(x^{\frac{1}{2}}\right) + \vartheta\left(x^{\frac{1}{3}}\right) - + \cdots,$$

which give us the useful inequality

$$\psi(x) - 2\psi(\sqrt{x}) \le \vartheta(x) \le \psi(x). \tag{2.3}$$

And the first sum in the definition of $\psi(x)$ can be written as

$$\psi(x) = \sum_{p \le x} \left[\frac{\ln x}{\ln p}\right] \cdot \ln p \tag{2.4}$$

---

[(a)] It is known that the author didn't know what this meant, he copied it from [36], probably to boast !

[(b)] The princess asked the author in a letter (which was found later in her room) whether her assumption was right that this sums run over prime numbers. The author replied: "Indeed, I am so sorry for this slip of the pen, I will use throughout the series of letters $p$ to be a prime number. As well as $n$,$m$ will denote integers, $x$ a real number, and $s = \sigma + it$ a complex number. The latter notation seems a little bit strange but almost all books use it - mathematicians are bound by traditions, too."

since $\ln p$ occurs exactly $m = [\ln x / \ln p]$ times when $p^m \le x < p^{m+1}$. You can find another formula in LANDAU's Handbuch[c] (I will give your maid my copy of this book, but, please, hide it well from your father's eyes) on page 76 another:

$$\ln([x]!) = \sum_{n \le x} \psi\left(\frac{x}{n}\right)$$

The main importance of these functions is the following theorem, which states that in order to prove the prime number theorem we can as well prove $\psi(x) \sim x$ or $\vartheta(x) \sim x$.

**Theorem 2.1.**

$$\begin{aligned} \lambda &= \underline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\ln x} = \underline{\lim}_{x\to\infty} \frac{\vartheta(x)}{x} = \underline{\lim}_{x\to\infty} \frac{\psi(x)}{x} \\ \Lambda &= \overline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\ln x} = \overline{\lim}_{x\to\infty} \frac{\vartheta(x)}{x} = \overline{\lim}_{x\to\infty} \frac{\psi(x)}{x} \end{aligned} \tag{2.5}$$

PROOF. [d] From the formulae (2.3) and (2.4), I can conclude that

$$\vartheta(x) \le \psi(x) \le \sum_{p \le x} \frac{\ln x}{\ln p} \cdot \ln p = \pi(x) \ln x.$$

On the other hand, if $0 < \alpha < 1$ and $x > 1$,

$$\vartheta(x) \ge \sum_{x^\alpha < p \le x} \ln p \ge (\pi(x) - \pi(x^\alpha)) \cdot \ln(x^\alpha)$$

Thus I can write

$$\frac{\vartheta(x)}{x} \ge \alpha \left( \frac{\pi(x) \ln x}{x} - \frac{\ln x}{x^{1-\alpha}} \right).$$

If I fix $\alpha < 1$, but let $x \to \infty$, I can deduce that the limits of indetermination of $\vartheta(x)/x$ will be bigger or equal to $\alpha\, \pi(x) \ln x / x$. As this inequality holds for all $\alpha < 1$, it will be true for $\alpha = 1$ as well. □

I think you remember that $\mathrm{Li}(x)$[e] is asymptotically equal to $\frac{x}{\ln x}$, for there is the asymptotic development[f]

$$\mathrm{Li}(x) = \frac{x}{\ln x} + \frac{1!x}{\ln^2 x} + \frac{2!x}{\ln^3 x} + \cdots + \frac{q!x}{\ln^{q+1} x} + (q-1)! \int_1^x \frac{du}{\ln^{q+2} x}$$

So the proof of $\psi(x) \sim x$ would imply $\pi(x) \sim \mathrm{Li}(x)$ as well.

CHEBYSHEV's aim was to prove the postulate of Bertrand that, if $n > 6$, there always exists a prime $p$ satisfying $\frac{1}{2}n < p \le n - 2$. For this he required the inequality that $\Lambda < 2\lambda$. This result implies the

**Theorem 2.2.**

$$\pi(x) = \mathrm{O}\left(\frac{x}{\ln x}\right) \qquad \textit{as } x \to \infty. \tag{2.6}$$

[c] see [36]

[d] This proof is copied from [29] p. 13.

[e] The definition of $\mathrm{Li}(x)$ is $\int_1^x \frac{du}{\ln u}$. (Sometimes the lower limit of the integral is taken to be 2, the two functions differ then by $\mathrm{Li}(2) = 1.04516\ldots$ which doesn't change the formula in the prime number theorem.)

[f] see [36] p. 14

I won't give you the proof although it quite nice and elementary. I made some photocopies of the proof in INGHAM's book,[g] for I wouldn't know how to write it better than he did it. It is actually the proof that $\lambda \geq \ln 2$ and $\Lambda \leq 4 \ln 2$. In the Handbuch[h] you can find further inequalities such as

$$\lambda \geq a = \ln \frac{2^{\frac{1}{2}} 3^{\frac{1}{3}} 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} = 0.9213\ldots$$

and $\Lambda \leq \frac{6}{5} a = 1.1055\ldots$ or $\Lambda \leq \frac{171}{175} \cdot \frac{6}{5} a = 1.0803\ldots$. The first proof of the theorem above and the postulate can be found in [9] and [10]. It is believed that this proof should be in THE BOOK, the book where God wrote down the most beautiful mathematical proofs.[i] Still narrower boundaries for this limits were obtained by SYLVESTER in [48]. But the prime number theorem could never be proven with these ideas. The best result was a theorem of CHEBYSHEV which says that $\lambda \leq 1 \leq \Lambda$ or, in other words, that if the limit of $\frac{\pi(x) \ln x}{x}$ as $x \to \infty$ exists then it is equal to 1.[j]

Please, my princess, be careful. Your humble teacher.

[g] see [29] p. 14
[h] see [36] pp. 87 - 95
[i] see [2]
[j] see [36] pp. 95 - 98.

# Letter 3

# Riemann's Zeta Function

My dear student and princess,
Thank you for your long letter. I am most grateful for your questions (I hope you received my answer) and your interest in the subject. So I won't let you wait and I will continue immediately:

The most important step towards a complete proof of the prime number theorem was made by BERNHARD RIEMANN in his brilliant paper "Über die Anzahl der Primzahlen unter einer gegebenen Grösse"[(a)] which is only 8 pages long but contains the fundamental facts about a function $\zeta(s)$, (nowadays it is called Riemann's zeta function). The first to consider this function was LEONARD EULER.[(b)] He realized the importance of analytical methods in other parts of mathematics, such as number theory and combinatorics. He used the equality

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

to show that $\sum_p \frac{1}{p}$ diverges. But before I start telling you the whole fascinating story about this function I will try to be a little bit more precise.

**Definition 3.1.** For $\sigma = \operatorname{Re} s > 1$ we define

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{3.1}$$

This is well-defined, since $\left|\sum_{n=1}^{\infty} \frac{1}{n^s}\right| \leq \sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} < \infty$ for every $\sigma > 1$.

**Theorem 3.2.**
*For $\sigma > 1$ we have*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}}. \tag{3.2}$$

PROOF. The proof is based on the fundamental theorem of arithmetic. First, we notice that $\left|\frac{1}{p^s}\right| < 1$ for all prime number p and all $\sigma > 1$. Thus the following sums converge absolutely for all positive $x$:

$$\prod_{p<x} \sum_{m=1}^{\infty} \left(\frac{1}{p^s}\right)^m = \prod_{p<x} \frac{1}{1-\frac{1}{p^s}}$$

But, on the other hand, I can rearrange the first sum to $\sum \frac{1}{n^s}$ where the sum runs over all $n$ whose prime factors are smaller than $x$. If I take $x \to \infty$ this sum approaches $\zeta(s)$, thus the product converges and the theorem is proven. □

[(a)] see [45]
[(b)] see [17]

We will have to work with the the logarithm[c] of $\zeta(s)$. For $\sigma > 1$ we have

$$\ln \zeta(s) = -\sum_p \ln(1 - p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{1}{m p^{ms}} \tag{3.3}$$

$$= \sum_p \frac{1}{p^s} + \mathrm{O}(1) \qquad \text{as } s \downarrow 1, \tag{3.4}$$

as the sums with $m \geq 2$ stay bounded. For the logarithmic derivative of $\zeta(s)$

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{d}{ds}(\ln \zeta(s))$$

$$= \sum_p \sum_{m=1}^{\infty} \frac{\ln p}{p^{ms}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \tag{3.5}$$

for $\sigma > 1$, where $\Lambda(n)$ is the Mangoldt function I defined in the beginning of my previous letter.

A hundred years after EULER, in 1859, BERNHARD RIEMANN wrote his famous paper. Inspired by the CHEBYSHEV's paper on primes, he was working on a formula related to $\pi(x)$. His new idea was to consider $\zeta(s)$ as a function on complex values of $s$. He proved the following facts about "his" function:

- The analytic continuation (see 3.3),
- the functional equation (see 4.1),
- the trivial zeros (see 4.2) on the negative real axis and the existence of non-trivial zeros in the critical strip $0 \leq \sigma \leq 1$.

This strip is really "critical", since we shall see that it contains the information about primes. Moreover he made some conjecture, but I will tell you about it later. Let us now look at the analytic continuation of the zeta function:

**Theorem 3.3.**
*$\zeta(s)$ is analytic in the half plane $\sigma > 0$ except for a simple pole at $s = 1$ with residue 1.*

There are many different ways to prove this. I advise you to have a look at the nice collection which can be found in TITCHMARSH's book on the Zeta function.[d] There is another proof which is much more general given in APOSTOL's "Introduciton"[e]

---

[c] the logarithm $\ln z$ is understood to be the main value $w$ such that $-\pi < \operatorname{Im} w \leq \pi$ and $e^w = z$, for the zeta function it can be defined by the series (3.3) and its analytic continuation

[d] see [49]

[e] see [3] pp. 249 - 255;
APOSTOL considers the Hurwitz Zeta function

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n + a)^s}$$

where $0 < a \leq 1$ and $\sigma > 1$. This generalization makes it possible to prove a similar theorem for the Riemann Zeta function $\zeta(s) = \zeta(s, 1)$ and the Dirichlet Series for characters modulo $k$, at the same time. Since there is the formula

$$L(s, \chi) = k^{-s} \sum_{r=1}^{k} \chi(r) \zeta(s, \frac{r}{k}).$$

The analytic continuation of $\zeta(s, a)$ is based on

$$\zeta(s, a)\Gamma(s) = \int_0^{\infty} \frac{x^{s-1} e^{-ax}}{1 - e^{-x}} dx \quad \text{for } \sigma > 1$$

But I will show you now the proof of the theorem as it is given in PRACHAR's book:[f]

PROOF. For $\sigma > 0$ we have

$$\int_n^{n+1} \frac{x-[x]}{x^{s+1}}dx = \int_n^{n+1} x^{-s}dx - n\int_n^{n+1} x^{-s-1}dx.$$

And if we sum up from $n = 1$ to $N-1$:

$$\begin{aligned}
s\int_1^N \frac{x-[x]}{x^{s+1}}dx &= s\int_1^N x^{-s}dx - s\sum_{n=1}^{N-1} n\left[\frac{x^{-s}}{-s}\right]_{x=n}^{x=n+1} \\
&= \frac{s}{s-1}\left(1-\frac{1}{N^{s-1}}\right) + \sum_{n=1}^{N-1}\frac{n}{(n+1)^s} - \sum_{n=1}^{N-1}\frac{1}{n^{s-1}} \\
&= \left(-1+\frac{1}{s-1}\right)\left(1-\frac{1}{N^{s-1}}\right) + \sum_{n=2}^{N}\frac{n-1}{n^s} - \sum_{n=1}^{N-1}\frac{1}{n^{s-1}} \\
&= -1 - \frac{1}{N^{s-1}} + \frac{1}{s-1}\left(1-\frac{1}{N^{s-1}}\right) + \sum_{n=1}^{N}\frac{1}{n^s} - 1 + \frac{1}{N^{s-1}} - 1 \\
&= 1 + \frac{1}{s-1}\left(1-\frac{1}{N^{s-1}}\right) - \sum_{n=1}^{N}\frac{1}{n^s} \qquad (3.6)
\end{aligned}$$

Now we let $N \to \infty$ and we get

$$\zeta(s) = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{x-[x]}{x^{s+1}}dx \qquad (3.7)$$

for $\sigma > 1$. But the last integral is an analytic function for $\sigma > 0$, since $0 \le x-[x] < 1$ and $\left|x^{-(s+1)}\right| = x^{-(\sigma+1)}$. Thus the function on the right hand side is an analytic continuation of $\zeta(s)$ for $\sigma > 0$. □

If you subtract the last two equations (3.6) and (3.7), you find that

$$\zeta(s) - \sum_{n=1}^{N}\frac{1}{n^s} = \frac{1}{(s-1)N^{s-1}} - s\int_N^\infty \frac{x-[x]}{x^{s+1}}dx \quad \text{for all } \sigma > 0, \qquad (3.8)$$

which we shall use later.

But I will stop now and tell you more in a few days in my next letter. I enclose a picture of GAUSS I found in the hills of old papers in my room. I hope you like it.

Your humble teacher.

---

which can be used to write

$$\zeta(s,a) = \Gamma(1-s)\cdot\frac{1}{2\pi i}\int_\gamma \frac{z^{s-1}e^{az}}{1-e^z}dz$$

where the contour $\gamma$ is a positive oriented loop around the negative real axis. This is a analytic function for $s \neq 1$.

[f] see [43] p. 59

# Letter 4

# Riemann's Zeta Function II

My dear princess,
Since I am sure that I enclosed the picture, I have to suppose that it fell out of the letter as your maid ran back to your room. At least it is not the letter that has been lost, for I don't want to think what would happen ...

I promised you to write about the work of BERNHARD RIEMANN. The last result we proved was only part of the truth, because

**Theorem 4.1.**
*$\zeta(s)$ is a meromorphic function with only one single pole at $s = 1$. $\zeta(s)$ satisfies the following functional equation for all $s \neq 0$:*

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\Gamma(s)\cos(\frac{\pi s}{2})\zeta(s) \tag{4.1}$$

I won't show you the proof in all details, it is well explained in TITCHMARSH's book.[(a)] One way to obtain the result is to push the domain of convergence to $\sigma > -1$ using the representation

$$\zeta(s) = \frac{1}{2} + \frac{1}{s-1} + s\int_1^\infty \frac{[x] - x + \frac{1}{2}}{x^{s+1}}dx \quad \text{for } \sigma > -1.$$

For $-1 < \sigma < 0$ this can be rewritten as

$$\zeta(s) = s\int_0^\infty \frac{[x] - x + \frac{1}{2}}{x^{s+1}}dx$$

and then use the Fourier series of the numerator:

$$\begin{aligned}
\zeta(s) &= s\int_0^\infty \sum_{n=1}^\infty \frac{\sin(2\pi nx)}{n\pi} \cdot \frac{dx}{x^{s+1}} \\
&= \frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \frac{\sin(2\pi nx)}{x^{s+1}}dx \\
&= \frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \frac{(2\pi n)^{s+1}\sin u}{u^{s+1}}\frac{du}{2\pi n} \\
&= s2^s\pi^{s-1}\sum_{n=1}^\infty n^{s-1}\cdot\int_0^\infty \frac{\sin u}{u^{s+1}}du \\
&= s2^s\pi^{s-1}\zeta(1-s)(-\Gamma(-s))\sin(\tfrac{\pi s}{2})
\end{aligned}$$

[(a)] see [49] p. 14

Of course, I left out all the justification for convergence that should be made. The last step is to use a property of the Gamma function:[(b)]

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}.$$

I know that you don't like the horrible Euler-McLaurin sum formula, but, using it, you would find the exact value of the zeta function for certain integers:

**Proposition 4.2.** *For $n \in \mathbb{N}$, we have*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1} \tag{4.2}$$

*where $B_n$ is the $n^{\text{th}}$ Bernoulli number. In particular $\zeta(-2n) = 0$ for $n \geq 1$, $\zeta(0) = -\frac{1}{2}$, $\zeta(-1) = -\frac{1}{12}$, $\zeta(-3) = \frac{1}{120}$, ... If $k$ is a positive even integer we have*

$$\zeta(k) = \frac{(2\pi)^k |B_k|}{2k!}. \tag{4.3}$$

The values of $\zeta(3)$, $\zeta(5)$, ... are still unknown. There is also the possibility to give its Laurent series around $s = 1$:

$$\zeta(s) = \frac{1}{s-1} + \sum_{k=0}^{\infty} (-1)^k \frac{\gamma_k}{k!} (s-1)^k$$

where

$$\gamma_k = \lim_{N->\infty} \left( -\frac{\ln^{k+1} N}{k+1} + \sum_{n=1}^{N} \frac{\ln^k n}{n} \right).$$

$\gamma_0 = 0.577216\ldots$ is the constant of Euler. No, please don't try to do that, the calculations are not less ugly than the formula itself.

I told you that RIEMANN made some conjectures which he didn't prove. (I used the enumeration in LANDAU's Handbuch[(c)]):

1. There are infinitely many zeros in the critical strip which lie symmetrical to the real axis and to the critical line $\sigma = \frac{1}{2}$.

2. If we denote $N(T)$ the number of zeros (counted with multiplicity) in the rectangle defined by $0 < \sigma < 1$ and $0 < t \leq T$, then

$$N(T) = \frac{1}{2\pi} T \ln T - \frac{1 + \ln(2\pi)}{2\pi} T + \mathrm{O}(\ln T) \qquad \text{as } T \to \infty. \tag{4.4}$$

3. $\sum_\rho |\rho|^{-2}$ converges and $\sum_\rho |\rho|^{-1}$ diverges, where $\rho$ runs over all non-real zeros of $\zeta(s)$.

4. There are constants $a$ and $b$ such that

$$(s-1)\zeta(s) = a e^{bs} \frac{1}{\Gamma(\frac{s}{2}+1)} \prod_\rho (1 - \frac{s}{\rho}) e^{\frac{s}{\rho}}. \tag{4.5}$$

[(b)] It is interesting to note that there exists a functional equation for the Hurwitz zeta function (see the footnote 8.(e)) as well, when $a$ is rational, it can be found in [3] p. 261:

$$\zeta\left(1-s, \frac{h}{k}\right) = \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} \cos\left(\frac{\pi s}{2} - \frac{2\pi r h}{k}\right) \zeta\left(s, \frac{r}{k}\right)$$

[(c)] see [36] pp. 31 - 36

5. The zeros of $\zeta(s)$ in the critical strip all lie on the critical line.

6.

$$f(x) = \sum_{p^m \le x} \frac{1}{m} = \mathrm{Li}(x) - \sum_{\rho} \left(\mathrm{Li}(x^{\rho}) + \mathrm{Li}(x^{1-\rho})\right) - \ln 2 + \int_x^{\infty} \frac{1}{(y^2-1)y \ln y} dy, \quad (4.6)$$

where $\rho$ runs over all zeros of $\zeta(s)$ ordered by increasing positive $\mathrm{Im}\,\rho$.

The last formula is related to $\pi(x)$ by $f(x) = \pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots$ and thus $f(x) - \pi(x) = \mathrm{O}\left(\frac{\sqrt{x}}{\ln x}\right)$. It is known as "Riemannsche Primzahlformel".

The conjectures 1, 3 and 4 were proven by JACQUES HADAMARD.[d] The second and the sixth had shown to be true by VON MANGOLDT.[e] The only one which is still unproven is the fifth, known as the Riemann hypothesis (Riemannsche Vermutung). Partial results in the general direction of the Riemann hypothesis have been of two kinds. First, there are results which demonstrate the existence of a zero-free region. Second, there are results showing that a large proportion of the complex zeros of $\zeta(s)$ lie on or near the critical line. Although results of the latter type are somewhat more striking, many are of no use in prime-number theory, whereas those of the first-mentioned kind have a direct influence on the error term in the prime number theorem.

In 1915 HARDY proved there are infinitely many zeros on the critical line. In 1921 HARDY and LITTLEWOOD showed that the number of zeros on the critical line from $\frac{1}{2}$ until $\frac{1}{2}+iT$ is at least $AT$ for some positive constant $A$, if $T$ is sufficiently large. SELBERG improved this to $AT \ln T$ in 1942; this means that a positive fraction of all zeros lie on the critical line. In 1974 LEVISON showed that 7 of 10 zeros lie on the critical line.

Using computers the first 1.5 millions of zeros have been proved to lie on the critical line.[f]

You may wonder why I tell you so much about this conjecture. It is because it is one of the most famous unproven "hypothesis", and that's what it makes so fascinating for mathematicians. I remember that it was one of the prime reason why I wanted to study this subject, and to see what influences it has on the prime numbers. I will show you later what the truth of the Riemann hypothesis would imply on the error term in the prime number theorem. At the end of this letter I include a graphic showing the image of the critical line in the complex plane.

Your humble servant.

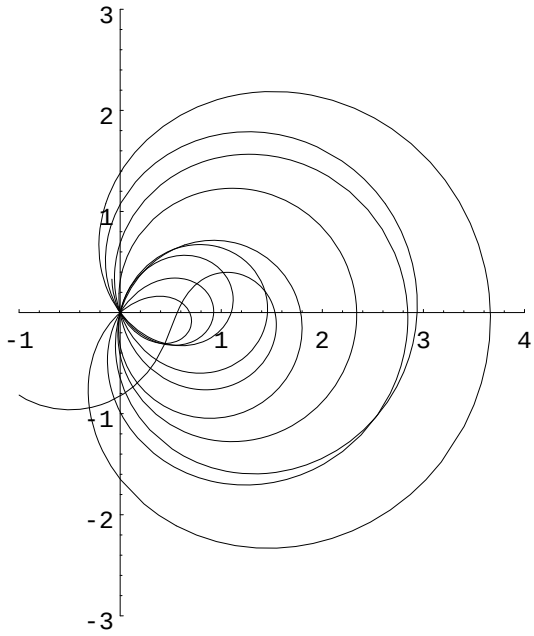



Figure 4.1: $\zeta(\frac{1}{2}+it)$ for $0 < t < 50$

[d] see [21]
[e] see [51] and [52]
[f] see [19] p. 454

# Letter 5

# Zeta and the Primes

Dearest princess,
Thank for your letter. It is true that I talked a lot about the zeta function, but not how it is connected to prime numbers (apart from the product formula of EULER). It is a mysterious fact that a special function characterized by infinite sums or integrals with very complicated behavior should give us information about natural numbers which represent our first contact with mathematics. I will give you now some formulae to illustrate this better.

**Proposition 5.1.** *For $\sigma > 1$ we can write*

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx \tag{5.1}$$

PROOF. [a]

$$\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= \sum_{n=1}^{\infty}\frac{\psi(n)-\psi(n-1)}{n^s} \\
&= \lim_{N->\infty}\left(\sum_{n=1}^{N-1}\psi(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)+\frac{\psi(N)}{N^s}\right) \\
&= \sum_{n=1}^{\infty}\psi(n)\int_n^{n+1}\frac{s}{x^{s+1}}dx \\
&= s\sum_{n=1}^{\infty}\int_n^{n+1}\frac{\psi(x)}{x^{s+1}}dx \\
&= s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx
\end{aligned}$$

□

In INGHAM's book[b] there is a section called "the fundamental formula". I am going to show you this formula that is the key to the prime number theorem. We need the following

**Lemma 5.2.** *For any integer $k \geq 1$ and for $c > 0$ we have*

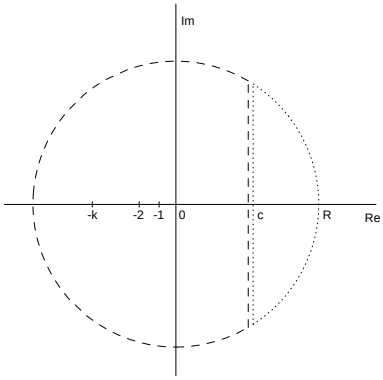
$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{a^s}{s(s+1)\cdots(s+k)}ds = \begin{cases} 0 & \text{for } 0 < a \leq 1 \\ \frac{1}{k!}\left(1-\frac{1}{a}\right)^k & \text{for } 1 \leq a \end{cases}$$

The notation $\int_{c-i\infty}^{c+i\infty}$ stands for the integral along the vertical line $\sigma = c$, provided it exists.

[a] see [34]
[b] see [29]; but the author used [44] and [19] for the proof

PROOF. Let

$$f(s) = \frac{a^s}{s(s+1)\cdots(s+k)}.$$




The poles of this function are 0,-1,-2, ... $-k$. In the first case when $0 < a \leq 1$, the integral along the dotted way vanishes and $a^s$ is uniformly bounded on the arc, thus

$$\int_{c-i\infty}^{c+i\infty} f(s)ds = 0.$$

In the second case when $a > 1$, we use the dashed contour. Once again $a^s$ is uniformly bounded, and the theorem of residues yields

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f(s)ds = \sum_{\nu=0}^{k} \mathrm{Res}_{s=-\nu} f(s) = \sum_{\nu=0}^{k} \frac{(-1)^\nu a^{-\nu}}{\nu!(k-\nu)!} = \frac{1}{k!}\left(1-\frac{1}{a}\right)^k.$$

□

Let

$$\Psi(x) = \int_0^x \psi(u)du = \sum_{n\leq x}(x-n)\Lambda(n). \tag{5.2}$$

The equality of the last two expressions can be seen by

$$\begin{aligned}
\int_0^x \psi(u)du &= (x-[x])\psi([x]) + \sum_{k=1}^{[x]-1}\psi(k) \\
&= (x-[x])\sum_{n=1}^{[x]}\Lambda(n) + \sum_{k=1}^{[x]-1}\sum_{n=1}^{k}\Lambda(n) \\
&= \sum_{n=1}^{[x]}(x-[x])\Lambda(n) + \sum_{n=1}^{[x]}\sum_{k=n}^{[x]-1}\Lambda(n) \\
&= \sum_{n=1}^{[x]}\big((x-[x]) + ([x]-1-n+1)\big)\Lambda(n)
\end{aligned}$$

Finally we get to our fundamental formula

**Theorem 5.3.**

$$\Psi(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\cdot\frac{x^{s+1}}{s(s+1)}ds \tag{5.3}$$

*for $c > 1$ and $x > 1$.*

PROOF.

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\cdot\frac{x^{s+1}}{s(s+1)}ds &= \frac{x}{2\pi i}\int_{c-i\infty}^{c+i\infty}\sum_{n=1}^{\infty}\Lambda(n)\left(\frac{x}{n}\right)^s\frac{ds}{s(s+1)}\\ &= \sum_{n=1}^{\infty}\Lambda(n)x\,\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{\left(\frac{x}{n}\right)^s}{s(s+1)}ds\\ &= \sum_{n=1}^{[x]}\Lambda(n)x\left(1-\frac{1}{x/n}\right)\\ &= \sum_{n\le x}\Lambda(n)(x-n)=\Psi(x)\end{aligned}$$

Where I used the lemma 5.2 for $k=1$ and the integration and the summation may be interchanged, since

$$\sum_{n=1}^{\infty}\int_{c-i\infty}^{c+i\infty}\left|\frac{\Lambda(n)(x/n)^s}{s(s+1)}ds\right| < x^c\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^c}\int_{-\infty}^{\infty}\frac{dt}{c^2+t^2}$$

is finite. □

The formula we just proved and the formula in 5.1 are connected in a more general way by Mellin's transformation. Actually with a bit more of annoying limit checks one could find directly[(c)]

$$\psi(x)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\cdot\frac{x^s}{s}ds \tag{5.4}$$

for $c>1$ and for all where $\psi(x)$ is continuous, and otherwise the integral takes the value in the middle of the step, i.e. $\psi(x)-\frac{1}{2}\Lambda(x)$.

I wonder if you are able to prove[(d)] the

**Proposition 5.4.**

$$\ln\zeta(s)=s\int_2^{\infty}\frac{\pi(x)}{x\cdot(x^s-1)}dx \quad \textit{for } \sigma>1 \tag{5.5}$$

I remember you (3.3): $\ln\zeta(s)=\sum_p\frac{1}{p^s}+\sum_p\sum_{m=2}^{\infty}\frac{1}{mp^{ms}}$, and that it is the first sum that make that the function has a pole at $s=1$. And this sum can be expressed as

$$\sum_p\frac{1}{p^s}=s\int_2^{\infty}\frac{\pi(x)}{x^{s+1}}dx \tag{5.6}$$

(this can be proved in the same way.)[(e)]

Late at night, as I write this letter, I raise my eyes to the palace which can be seen from my tiny room. And I see the light in your window which is shining over the city. Might it be that some numbers are stealing your sleep ? Magdalene[(f)] told me that the only time you could do mathematics was the nights when your father had to rest.

Your grateful teacher.

---

[(c)] see [11] p. 105

[(d)] a proof can be found in [49]

[(e)] see [5] p. 31

[(f)] the lady-in-waiting who used to bring the letters

# Letter 6

# Estimations for Zeta

Dear Princess,
I think that it was not very prudent to take the picture found by your father in the garden. What if he finds out that it is a mathematician and that you didn't stop doing maths ? But I am maybe too anxious.

I will show you some things about the zeta function (again !!!) that we will use to prove the prime number theorem. Firstly, that there are no zeros on the vertical line $\sigma = 1$. This is essential to all analytic proofs (which I know). The graph (figure 6) will never pass through the origin.

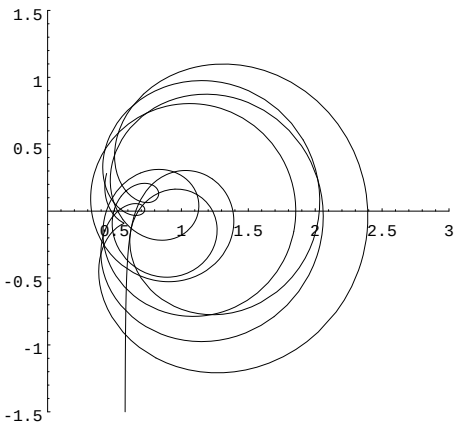



Figure 6.1: $\zeta(1+it)$ for $0 < t < 50$

**Proposition 6.1.**

$$\zeta(s) \neq 0 \quad \textit{for all } \sigma \geq 1$$

PROOF. [(a)] This elegant proof was found by MERTENS.[(b)] If $\sigma > 1$ the fact follows from 3.2. So we have to look at $s = 1 + it$ for $t \neq 1$. Let

$$\begin{aligned}
\varphi_\varepsilon(t) &= |\zeta(1+\varepsilon)|^3 \cdot |\zeta(1+\varepsilon+it)|^4 \cdot |\zeta(1+\varepsilon+2it)| \\
&= \prod_p \left|1 - \frac{1}{p^{1+\varepsilon}}\right|^{-3} \left|1 - \frac{1}{p^{1+\varepsilon+it}}\right|^{-4} \left|1 - \frac{1}{p^{1+\varepsilon+2it}}\right|^{-1} \\
\ln \varphi_\varepsilon(t) &= \sum_p \left(-3\ln\left(1 - \frac{1}{p^{1+\varepsilon}}\right) - 4\ln\left(1 - \frac{1}{p^{1+\varepsilon+it}}\right) - \ln\left(1 - \frac{1}{p^{1+\varepsilon+2it}}\right)\right) \\
&= \sum_p \sum_{m=1}^{\infty} \frac{1}{m} p^{-(1+\varepsilon)m} (3 + 4\cos(mt\ln p) + \cos(2mt\ln p))
\end{aligned}$$

From $3 + 4\cos\theta + \cos 2\theta = 2(1+\cos\theta)^2 \geq 0$ we can conclude $\varphi_\varepsilon(t) \geq 1$. I suppose that $\zeta(1+it) = 0$ for some $t \neq 0$. Hence $\zeta(1+\varepsilon+it) = \int_1^{1+\varepsilon} \zeta'(\sigma+it)d\sigma = \mathrm{O}(\varepsilon)$ if $\varepsilon \to 0$. We get a contradiction:

$$1 \leq \varphi_\varepsilon(t) = \left(\frac{1}{\varepsilon} + \mathrm{O}(1)\right)^3 \cdot \mathrm{O}(\varepsilon)^4 \cdot |\zeta(1+\varepsilon+2it)| = \mathrm{O}(\varepsilon) \qquad \text{as } \varepsilon \to 0$$

since the last factor converges to $\zeta(1+2it)$. □

We will need some estimations of our zeta function, although it is not necessary for the proof of the weak form of the prime number theorem. But we need it to make estimations of the error term.

[(a)] The notation of [28] are used.
[(b)] see [41]

**Theorem 6.2.**
*Let $a > 0$. There exists a constant $c$ such that*

$$|\zeta(s)| < c \ln t \tag{6.1}$$

*for $\sigma > \frac{1}{2}$, $1 - \frac{a}{\ln|t|} \leq \sigma \leq 2$ and $t \geq 3$.*

PROOF. Using (3.8):

$$|\zeta(s)| \leq \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{1}{|s-1| \cdot N^{\sigma-1}} + |s| \int_N^\infty \frac{dx}{x^{\sigma+1}}$$

Hence

$$\begin{aligned}
|\zeta(s)| &\leq \sum_{n=1}^{N} \frac{1}{n \cdot n^{-\frac{a}{\ln t}}} + \frac{1}{tN^{\frac{a}{\ln t}}} + (t+3)\frac{1}{\sigma \cdot N^\sigma} \\
&\leq \sum_{n=1}^{N} \frac{e^{a\frac{\ln n}{\ln t}}}{n} + \frac{e^{a\frac{\ln N}{\ln t}}}{t} + 2t \cdot \frac{1}{1 - \frac{a}{\ln t \cdot N}} e^{a\frac{\ln N}{\ln t}} \\
&\leq e^{a\frac{\ln N}{\ln t}} \sum_{n=1}^{N} \frac{1}{n} + \frac{e^{a\frac{\ln N}{\ln t}}}{t} + 2\frac{1}{1 - \frac{a}{\ln t}} \cdot \frac{t}{N} \cdot e^{a\frac{\ln N}{\ln t}}
\end{aligned}$$

I choose a $N$ to be $[t]$

$$|\zeta(s)| < e^a(\ln t + 1) + \frac{e^a}{t} + 2\frac{1}{1 - \frac{a}{\ln 3}} \cdot \frac{3}{2} < c \ln t$$

since $t \geq 3$. □

**Theorem 6.3.**
*Let $b > 0$. There exists a constant $c$ such that*

$$\left|\zeta'(s)\right| < c \ln^2 t \tag{6.2}$$

*for $t \geq 3$ and $1 - \frac{b}{\ln t} \leq \sigma \leq 2$.*

PROOF. [(c)] Let $a > b$. Every point in the region $\left\{s \mid 1 - \frac{b}{\ln t} \leq \sigma \leq \frac{3}{2}\right\}$ is the center of a circle of radius $r = \frac{b'}{\ln t}$ which is completely contained in the region $\left\{s \mid 1 - \frac{a}{\ln t} \leq \sigma \leq 2\right\}$. Using Cauchy formula, we get

$$\left|\zeta'(s)\right| \leq \frac{1}{2\pi} \cdot 2\pi r \cdot \frac{\max|\zeta(s)|}{(s+r)^2},$$

where the maximum on the circle is taken. The estimation for $\zeta(s)$ and $t \geq 3$ leads us to

$$\begin{aligned}
\left|\zeta'(s)\right| &\leq \frac{b'}{\ln t} \cdot \frac{c' \ln(t+r)}{(3 + \frac{b'}{\ln t})^2} \\
&\leq c'' \frac{\ln^2 t}{3 \ln^2 3 + b'}
\end{aligned}$$

□

[(c)] see [5] p. 55

At this point I should show you a proof of the following

**Proposition 6.4.** *There exist constants $a > 0$, $c_1$, $c_2$ and $\beta > 0$ such that*

$$\frac{\zeta'(s)}{\zeta(s)} \leq c_1 \ln t \cdot \ln\ln t \qquad \textit{and} \qquad \frac{1}{\zeta(s)} \leq c_2 \ln^\beta t \tag{6.3}$$

*for all $t \geq 3$ and $1 - \frac{a}{\ln t} \leq \sigma \leq 2$.*

*In particular $\zeta(s)$ has no zero in this region.*

But I know that you are interested in the prime number theorem and not in these annoying estimations. I indicate to you that you can find in the Handbuch on the pages 176 to 180 a proof for a weaker estimation on a smaller region.[(d)] These kind of estimations are derived from the proof of the non-vanishing of $\zeta(s)$ on the line $\sigma = 1$. So I leave it to you to read it in some book, I will use it in the next letter when I shall finally explain to you the prime number theorem. Your teacher.

[(d)] the author didn't indicate that there are further better estimations in [36]: pp. 318 - 324. The proposition above is on the pages 610 - 616 or better presented in [5] pp. 56 - 62

# Letter 7

# The Prime Number Theorem

O($h$), my princess,
All this long work on the zeta function will bear fruits, today. I am going to show you the proof of the Prime Number Theorem.

Inspired by the famous work of RIEMANN that I described in one of the previous letter, independently, HADAMARD[a] and DE LA VALLÉE POUSSIN[b] finally could prove the prime number theorem at the end of the nineteenth century. The latter showed in [13] that the asymptotic function $\mathrm{Li}(x)$ approximates $\pi(x)$ better than $\frac{x}{\ln x}$. It follows from his work that

$$\pi(x) = \mathrm{Li}(x) + \mathrm{O}\Big(xe^{-\alpha\sqrt{\ln x}}\Big)$$

for some positive constant $\alpha$.

There has been a lot of progress made on the different methods of proving the prime number theorem. LANDAU[c] simplified the proof and showed a possibility to prove it without any knowledge about $\zeta(s)$ for $\sigma < 1$. Further simplification are due to HARDY and LITTLEWOOD, as well as KARAMATA, they used a Tauberian theorem for power series. WIENER's work on general Tauberian theorems led to several proofs which require nothing more than the non-vanishing of $\zeta(s)$ on the vertical line $\sigma = 1$. IKEHARA, BOCHNER and LANDAU made some further simplification. Now, I won't show you such proofs, using the Wiener-Ikehara theorem, (you can find them at the end of the Handbuch.[d]) They are very elegant and short. "So", you may ask me, "why don't you take such a proof? For you often tell me that one reason why you're studying mathematics is your aesthetic sense." Because these proofs hide certain things. You can't generalize them, and you wouldn't see what hard work it is to find better estimations.

In 1948 SELBERG and ERDÖS found an "elementary" proof. It is based on a elementary asymptotic relation obtained by SELBERG. But I won't tell you anything about it, the proof is long, but it assumes the least knowledge.[e]

On the other hand there has been progress made on the order of the error term. In 1922 LITTLEWOOD announced a proof of the existence of a larger zero-free region for the zeta-function, namely a region whose width is of order $(\ln\ln t)/\ln t$. Such results give immediately better error terms. In 1936 CHUDAKOV improved this using the methods for dealing with exponential sums due to VINOGRADOV.

I will use the same function as integrand as in [4], [29] or [5]. The Handbuch[f] uses a slightly different function, namely $-\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s^2}$.

I will denote $-\frac{\zeta'(s)}{\zeta(s)}\frac{x^s+1}{s(s+1)}$ by $f(s)$. Furthermore I use the complex contour $\gamma$ shown in the figure 7.1.

---

[a] see [22]
[b] see [12]
[c] see [33] or [36] pp. 258
[d] see [34] and [6]
[e] "elementary" proofs can be found in [43] and [7]
[f] see [36] pp. 183 - 193

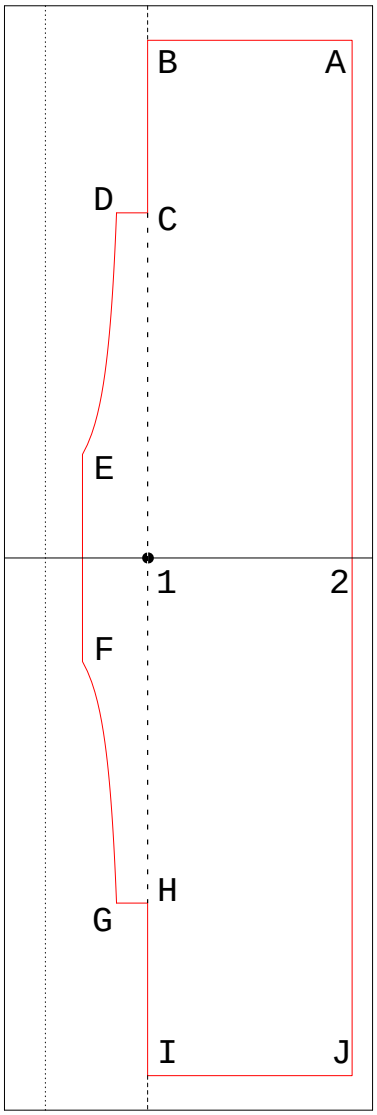



Figure 7.1: A good contour

The letters are denoting the following points:

$$\begin{aligned} A &= 2 + x^4 i & J &= \overline{A} = 2 - x^4 i \\ B &= 1 + x^4 i & I &= \overline{B} = 1 - x^4 i \\ C &= 1 + Ti & H &= \overline{C} = 1 - Ti \\ D &= 1 - \frac{c}{\ln T} + Ti & G &= \overline{D} = 1 - \frac{c}{\ln T} - Ti \\ E &= 1 - \frac{c}{\ln 3} + 3i & F &= \overline{E} = 1 - \frac{c}{\ln 3} - 3i \end{aligned}$$

and the curve from $E$ to $D$ (similar for $F$ to $G$) is parameterized by $t \mapsto 1 - \frac{c}{\ln t} + it$ for $t \in [3, T]$.

$f(s)$ has only one pole in the interior of $\gamma$ at $s = 1$, with residue $\frac{x^2}{2}$, (that's why we looked for a zero-free region of the zeta function), thus

$$\frac{1}{2\pi i} \oint_\gamma f(s)ds = \frac{x^2}{2} \tag{7.1}$$

Therefore, if you remember the formula (5.3) in my fifth letter,

$$\Psi(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} f(s)ds = \frac{x^2}{2} + \frac{1}{2\pi i} \int_{\gamma'} f(s)ds, \tag{7.2}$$

where $\gamma'$ is the path $2 - i\infty$, $J$, $I$, $H$, ..., $A$, $2 + i\infty$. I now have to show you that this last integral is small. What means small ? - You will see: (All O's are used for $x \to \infty$.)

First, (remember the estimation (6.3), I didn't prove)

$$\begin{aligned} \frac{1}{2\pi i} \int_A^{2+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \frac{x^{s+1}}{s(s+1)} ds &= \mathrm{O}\left(x^3 \int_{x^4}^{\infty} \frac{\ln t \cdot \ln\ln t}{t^2} dt\right) \\ &= \mathrm{O}\left(x^3 \int_{x^4}^{\infty} \frac{\sqrt{t}}{t^2} dt\right) \\ &= \mathrm{O}\left(\frac{x^3}{(x^4)^{\frac{1}{2}}}\right) = \mathrm{O}(x) \end{aligned}$$

The same must hold for $\int_{2-i\infty}^{J}$. As next we look at the horizontal segment:

$$\begin{aligned} \int_A^B f(s)ds &= \mathrm{O}\left(x^3 \frac{\ln x^4 \cdot \ln\ln x^4}{(x^4)^2}\right) \\ &= \mathrm{O}\left(\frac{1}{x^4}\right) \end{aligned}$$

and this is about nothing, the same for $\int_I^J$. Now we are going down on the line $\sigma = 1$.

$$\begin{aligned} \int_C^B f(s)ds &= \mathrm{O}\left(x^2 \int_T^{x^4} \frac{\ln t \cdot \ln\ln t}{t^2} dt\right) \\ &= \mathrm{O}\left(\frac{x^2}{T^{1-\delta}}\right), \end{aligned}$$

for all $\delta > 0$, and this holds for $\int_H^I$ as well.

$$\begin{aligned}\int_C^D f(s)ds &= \mathrm{O}\left(x^2\frac{\ln T\cdot\ln\ln T}{T^2}\right)\\ &= \mathrm{O}\left(\frac{x}{T}\right)\end{aligned}$$

On the remaining part $\int_C^G$, $\frac{\zeta'(s)}{s(s+1)\zeta(s)}$ is bounded for all $x$, thus

$$\int_C^G f(s) = \mathrm{O}\left(x^{1-\frac{c}{\ln T}+1}\right).$$

So we can write

$$\begin{aligned}\Psi(x) - \frac{x^2}{2} &= \mathrm{O}\left(\frac{x^2}{T^{1-\delta}}\right) + \mathrm{O}\left(x^{2-\frac{c}{\ln T}}\right)\\ &= \mathrm{O}\left(x^2e^{-(1-\delta)\ln T}\right) + \mathrm{O}\left(x^2e^{-c\frac{\ln x}{\ln T}}\right)\end{aligned}$$

Now, since we can still choose $T$, let us make a wise choice, let it satisfy

$$(1-\delta)\ln T = c\frac{\ln x}{\ln T}, \qquad \text{i.e.} \qquad \ln T = \sqrt{\frac{c\ln x}{1-\delta}}$$

I will denote the constant $\sqrt{c/(1-\delta)}$ by $2\alpha$. And we can formulate[g] the

**Theorem 7.1.**
*There exists a constant $\alpha > 0$ such that*

$$\Psi(x) = \frac{x^2}{2} + \mathrm{O}\left(x^2e^{-2\alpha\sqrt{\ln x}}\right). \tag{7.3}$$

Do you feel how close we are to the result? I think you won't be surprised by the following

**Lemma 7.2.** *Let $\omega$ be a function $[0,\infty[\to[0,\infty[$ which is increasing such that $x/\omega(x)$ is increasing, too. For every increasing function $g$ such that*

$$\int_0^x g(u)du = \frac{x^2}{2} + \mathrm{O}\left(\omega(x)^2\right),$$

*then we have $f(x) = x + \mathrm{O}(\omega(x))$.*

The uninteresting but tricky proof is in BLANCHARD's book.[h] So, let us apply it to $\Psi(x) = \int_0^x \psi(u)du$:

**Theorem 7.3.**
*With the same $\alpha > 0$:*

$$\psi(x) = x + \mathrm{O}\left(xe^{-\alpha\sqrt{\ln x}}\right) \tag{7.4}$$

This theorem together with 2.1 shows already that

$$\lim_{x\to\infty}\frac{\pi}{x/\ln x} = 1.$$

[g] this theorem and its deduction (slithly modified) are taken from [5]
[h] see [5] pp. 65 - 66

But we want more. We transport the error term to $\pi(x)$, passing by $\vartheta(x)$. First, we use (2.3) to see that

$$\vartheta(x) = x + \mathrm{O}\Big(xe^{-\alpha\sqrt{\ln x}}\Big).$$

On the one hand

$$\begin{aligned}
\pi(x) &= \sum_{n=2}^{[x]} \frac{\vartheta(n)-\vartheta(n-1)}{\ln n} \\
&= \frac{\vartheta(x)}{\ln([x])} + \sum_{n=2}^{[x]-1} \vartheta(n)\left(\frac{1}{\ln n} - \frac{1}{\ln(n+1)}\right) \\
&= \frac{\vartheta(x)}{\ln x} + \vartheta(x)\left(\frac{1}{\ln x} - \frac{1}{\ln[x]}\right) + \int_2^{[x]} \vartheta(u)\, d\Big(\frac{-1}{\ln u}\Big) \\
&= \frac{\vartheta(x)}{\ln x} + \int_2^{x} \vartheta(u)\, d\Big(\frac{-1}{\ln u}\Big)
\end{aligned}$$

and on the other hand, using partial integration

$$\mathrm{Li}(x) = \mathrm{Li}(2) + \Big[\frac{u}{\ln u}\Big]_{u=2}^{x} + \int_2^x u\, d\Big(\frac{-1}{\ln u}\Big),$$

thus

$$\begin{aligned}
\pi(x) - \mathrm{Li}(x) &= \frac{\vartheta(x)-x}{\ln x} + \mathrm{O}(1) + \int_2^x (\vartheta(u)-u)\, d\Big(\frac{-1}{\ln u}\Big) \\
&= \mathrm{O}\left(\frac{xe^{-\alpha\sqrt{\ln x}}}{\ln x}\right) + \mathrm{O}(1) + \mathrm{O}\left(xe^{-\alpha\sqrt{\ln x}} \cdot \int_2^x d\left(\frac{-1}{\ln u}\right)\right) \\
&= \mathrm{O}\Big(xe^{-\alpha\sqrt{\ln x}}\Big),
\end{aligned}$$

since $\int_2^x d(-1/\ln u) < \ln 2$.

And this means that we have proven[i] the

**Prime Number Theorem 7.4.**
*There exists a constant $\alpha > 0$ (the same as in the previous theorem) such that*

$$\pi(x) = \mathrm{Li}(x) + \mathrm{O}\Big(x e^{-\alpha\sqrt{\ln x}}\Big). \tag{7.5}$$

Although this letter is already much too long, I add that under the assumption of the truth of the Riemann hypothesis the error term would have the form $\mathrm{O}(\sqrt{x}\cdot\ln x)$. This was found by VON KOCH.[j]

There is the possibility to push the left part of the path used in the proof to $-\infty$. One can find like this the explicit formula, valid for all $x$ where $\psi(x)$ is continuous,

$$\psi(x) = \sum_{p^m \le x} \ln p = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\ln\left(1 - \frac{1}{x^2}\right) \tag{7.6}$$

where the sum runs over the complex zeros $\rho$ of $\zeta$. The second term comes from the pole at $s = 0$ of $f(s)$ and the last one from the trivial zeros of the zeta function. This is essentially the same as (4.6). This gives a direct connection between the numbers of the form $p^m$ and the zeros in the critical strip.

Leaving you a with a lot of work, yours, C. W.

[i] see [5] pp. 66 - 67
[j] see [50] or [5] p. 90

# Part II

# Dirichlet's theorem

"Say they so ? Oh, believe them not. Or if it indeed be so, that this other Space is really Thoughtland, then take me to that blessed Region where I in Thought shall see the inside of all solid things."
A SQUARE[a]

[a] quoted from [1]

## Letter 8

# Characters of an Abelian Group

My dear princess,
Yesterday, I was in the palace, the King had asked for me. My boldest dreams that I would be allowed to teach you again, were quickly destroyed, when he offered me a job as a cryptographer. He heard that one uses big prime numbers to code messages ... Sigh, politician and their obsession for usefulness! I refused as I don't want to soil the pure prime numbers, for all use may be criminal. May others take the responsibility.[a]

Now, that we finished the first part, when we looked at the distribution of the set of primes in the set of integers, we could ask about certain subsets. I would like to show you the famous theorem of Gustav Lejeune-Dirichlet. He proved that there are infinitely many primes in every arithmetic progression if the first element and the common difference are relatively prime. Adrien M. Legendre made the conjecture in 1788 that this should be true.[b] He published several proofs, but all of them were incomplete.

Dirichlet had the idea to generalize a proof of the existence of infinitely many primes due to Euler (by his product formula for the zeta function)[c]. His success established a new field in mathematics, analytic number theory, before there was still a clear separation of pure, elementary arithmetic (in the Greek tradition) and the new, complicated calculus. And this wouldn't have been possible if there wasn't, at the same time, the development of a strict foundation of calculus.

Dirichlet wasn't able to prove the other conjecture of Legendre that the primes would lie equally distributed in the invertible classes modulo a natural number. It was de la Vallée Poussin who proved a more precise result, namely that

$$\lim_{x\to\infty} \frac{{}_m\pi_a(x)}{x/\ln x} = \frac{1}{\varphi(k)},$$

where ${}_m\pi_a(x)$ denotes the number of primes in the arithmetic progression $\{a+nm \mid n \in \mathbb{N}\}$ ($a$ and $m$ two relatively prime positive integers) which are smaller than or equal to $x$. And $\varphi(x)$ is Euler's phi-function. This implies

$$\lim_{x\to\infty} \frac{{}_m\pi_a(x)}{{}_m\pi_{a'}(x)} = 1. \tag{8.1}$$

where $a'$ is another positive integer relatively prime to $m$. These proofs, partly simplified by Landau, use a lot of calculus and complex analysis.

As I think you had enough of this O's, I will choose another way which is closer to the original one. So we leave the more analytic part and we come to a more algebraic part. I will include a second generalization as well, we will work over any number field. Of course, as a lot of their number rings are not unique factorisation domains, we can't look at the prime numbers anymore. But as the ideals have a unique factorisation we can try to look for asymptotic formulas for the prime ideals.

[a] The author didn't write more about this conversation with the king. It is unknown whether the author had a good relation with the king.
[b] see [36] p. 7
[c] see [15]

In a first part, I will tell you something about characters of finite abelian group, then about Dirichlet series. Finally we start working in the number field. I shall prove the Unit Group Theorem and the formula for the density of ideals in the ideal classes. Then I will introduce the Dedekind zeta function and show you some of its properties. As a corollary we'll get the theorem of Dirichlet.

I hope, my dear Princess, you remember the theory of characters of groups. I shall recall you briefly the part we will need. A very elegant introduction can be found in SERRE's book.[(d)] This is were I have taken most of the following statements:

Let $G$ be a finite abelian group written multiplicatively. The *dual of a group* $G$ is the set $\mathrm{Hom}(G;\mathbb{C}^*)$, denoted by $\hat{G}$. Its elements are called *characters*, they are homomorphisms of abelian groups between $G$ and $\mathbb{C}^*$. (This is a special case of the representation theory of finite groups, irreducible representations of abelian groups have dimension 1.[(e)]) For any group $G$ there is the *principal character* $\chi_1$ which takes only the value 1 for all elements in $G$.

The dual group $\hat{G}$ is (not canonically) isomorphic to $G$ itself. (You can find the proof when you decompose the group into a direct product of cyclic groups.[(f)]) There are the orthogonality relations:[(g)]

**Proposition 8.1.** *Let* $\chi \in \hat{G}$,

$$\sum_{x\in G} \chi(x) = \begin{cases} |G| & \text{if } \chi = \chi_1 \\ 0 & \text{if } \chi \neq \chi_1 \end{cases} \tag{8.2}$$

*and let* $x \in G$,

$$\sum_{\chi\in \hat{G}} \chi(x) = \begin{cases} |G| & \text{if } x = 1 \\ 0 & \text{if } x \neq 1 \end{cases} \tag{8.3}$$

You may have guessed that, for the theorem of Dirichlet, our $G$ will be the group of invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$, I will denote it by $\mathbb{Z}_m^*$. A character of $\mathbb{Z}_m^*$ is called a *character modulo* $m$. Such a character $\chi$ can be viewed as a function $\mathbb{Z} \to \mathbb{C}^*$ by putting $\chi(n) = 0$ if $n$ is not relatively prime to $m$, and to be the value of $\chi$ of the class of $n$ modulo $m$. This function is then strictly multiplicative, i.e. $\chi(nn') = \chi(n)\chi(n')$ for all $n, n' \in \mathbb{Z}$, and periodic with period $m$.

I suppose that I should give you some examples of such characters tables. For the first seven integers this is printed in [3] on page 139. If $m$ is a prime number, then $\mathbb{Z}_m^*$ is cyclic (since $\mathbb{Z}/m\mathbb{Z}$ is a finite field). If $g$ is a generator then the characters are simply

$$\chi_b(g^c) = \omega^{(b-1)c}, \quad \text{where } \omega = e^{\frac{2\pi i}{m-1}}$$

is a primitive $(m-1)^{\text{th}}$-root of unity, $1 \leq b \leq m-1$ and $0 \leq c < m-1$. For $m$ equals 9, 14 or 18, there are six elements in the group, thus they are also cyclic (the only abelian group of order six). The group $\mathbb{Z}_{10}^*$ is cyclic of order 4. But the groups $\mathbb{Z}_8^*$ and $\mathbb{Z}_{12}^*$ are Kleinian groups. This means that their characters are real (all elements have order 2).

**Lemma 8.2.** *Let* $x$ *be an element of an abelian group* $G$. *Let* $H$ *be the subgroup generated by* $x$. *Let* $\lambda$ *be the order of* $x$, *and* $\mu$ *the index of* $H$ *in* $G$. *Then*

$$\prod_{\chi\in\hat{G}} (1 - \chi(x)T) = (1 - T^\lambda)^\mu \in \mathbb{C}[T]. \tag{8.4}$$

---

[(d)] see [47] pp. 61 - 76
[(e)] see [30] pp. 81 - 82
[(f)] see [30]
[(g)] for a proof see [47]

PROOF. Every character of $G$ restricted to $H$ gives a character of $H$. There are $\lambda$ characters in the cyclic subgroup $H$. While $\chi$ runs once over every character of $G$, $\chi(x)$ runs $\mu$ times over every $\lambda$-th root of unity. And the formula is a consequence of the factorisation of $(1-T^\lambda)$. □

In particular, if $p$ is prime to $m$, then

$$\prod_\chi (1-\chi(p)T) = (1-T^{\lambda(p)})^{\mu(p)} \tag{8.5}$$

where $\lambda(p)$ is the order of $p$ in $\mathbb{Z}_m^*$ and $\lambda(p) = \varphi(m)/\mu(p)$.

I hope this more algebraic part I have started today will please you even more than what we have done before. Your teacher.

# Letter 9

# Dirichlet series

My dearest princess,
I am glad to hear that you agree with me on what I said about my reason and aim of mathematics. So let us go on, on our way through the kingdom of primes, walking in the garden of numbers without knowing why. Our interest in the bricks of the house of integers shall be our only guide.

Today I am going to tell you what Dirichlet series are, and what $L$-series are. But first, let me take any multiplicative[(a)] function $f\colon \mathbb{Z} \to \mathbb{C}$. I hope you remember that these function form a group under the Dirichlet multiplication:

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{de=n} f(d)g(e)$$

The inverse of the function $\iota$ which is identically 1 is called the Möbius function $\mu(n)$. $\mu(n)$ is equal to 0 if $n$ not square-free, and it is equal to $(-1)^k$, where $n$ has $k$ prime factors.[(b)]

Now, I will come back to what I would like to do: A *Dirichlet series* is a formal series of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}, \qquad \text{with } a(n) \in \mathbb{C}, s \in \mathbb{C}. \tag{9.1}$$

The first definition of the zeta function is an example of such a series. If a Dirichlet series converges for some $s_0$, it converges for all $s$ such that $\sigma > \sigma_0$.[(c)] So there exists a maximal half plane $\{s \mid \sigma > \sigma_0\}$ where the series converges. $\sigma_0$ is called the *abscissa of convergence*. There is also a half plane $\{s \mid \sigma > \sigma_1\}$ where the series converges absolutely. $\sigma_1$ is called the *abscissa of absolute convergence*. It can be shown that $\sigma_1 < \sigma_0 + 1$.[(d)] It easy to prove that the function

$$D_a(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \tag{9.2}$$

---

[(a)] a definition is in [3] p. 33:
$f$ is multiplicative if $f$ is not identically zero and if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.

[(b)] for more details on this subject see [3]

[(c)] It isn't clear why the author didn't include the proof of this fundamental fact (see [47] or [5] p. 27): Let $s, s_0 \in \mathbb{C}$ such that $\sigma_0 < \sigma$ and such that the series converges. Let $\varepsilon > 0$. There exists $N > 0$ such that $\left|\sum_{n=m}^{r} a(n) n^{-s_0}\right| < \varepsilon$ for all $m > r > N$. Using Abel's lemma we can write

$$\sum_{n=m}^{r} \frac{a(n)}{n^s} = \sum_{n=m}^{r} \frac{a(n)}{n^{s_0}} \cdot n^{s_0 - s} = r^{s_0 - s} \sum_{n=m}^{r} \frac{a(n)}{n^{s_0}} + \sum_{n=m}^{r-1} \left( \sum_{k=m}^{n} \frac{a(k)}{k^{s_0}} \right) \cdot \left(n^{s_0 - s} - (n+1)^{s_0 - s}\right)$$

$$\left|\sum_{n=m}^{r} \frac{a(n)}{n^s}\right| \leq r^{\sigma_0 - \sigma} \varepsilon + \sum_{n=m}^{r-1} \varepsilon \left| (s_0 - s) \int_n^{n+1} u^{s_0 - s - 1} du \right|$$

$$\leq \varepsilon + \varepsilon \left| (s_0 - s) \right| \int_m^r u^{\sigma_0 - \sigma - 1} du \leq \varepsilon \left(1 + \frac{|s_0 - s|}{\sigma_0 - \sigma}\right)$$

Moreover, the convergence is uniform in every angular domain of the form $\sigma_0 < \sigma$ and $|\arg(s - s_0)| \leq \alpha < \pi/2$.

[(d)] The Dirichlet series for $a(n) = (-1)^n$ gives an example that $0 = \sigma_0 \neq \sigma_1 = 1$. In fact $D_a(s) = (1 - 2^{1-s})\zeta(s)$, for $\sigma > 0$ and $s \neq 1$.

representing the Dirichlet series is a analytic function in its half plane of convergence. The sum converges uniformly in every compact set it. Moreover the series with different coefficients $a(n)$ which converge on a common half plane represent different functions.

If we have two multiplicative functions $f$ and $g$, such that the functions representing their series $D_f(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ and $D_g(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ converges absolutely in a common half plane $\sigma > \sigma_1$, then

$$D_f(s) \cdot D_g(s) = D_{f*g}(s) \quad \text{for } \sigma > \sigma_1.$$

You can check this if you do just once a multiplication of two Dirichlet series.[(e)] This gives us some formulas:

$$\frac{1}{\zeta(s)} = D_\mu(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \qquad \text{for } \sigma > 1$$

$$\frac{\zeta(s-1)}{\zeta(s)} = D_\varphi(s) = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} \qquad \text{for } \sigma > 2$$

The latter formula is derived from $\varphi * \iota = \mathrm{id}$. The first one is important in the theory of the Riemann zeta function. The Riemann hypothesis is equivalent to the statement that this Dirichlet series has $\sigma_0 = \frac{1}{2}$.

Moreover, if the multiplicative function $f$ is strictly multiplicative, i.e. $f(nn') = f(n)f(n')$ for all $n, n' \in \mathbb{N}$. then we have the equality

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1} \qquad \text{for } \sigma \geq \sigma_1. \tag{9.3}$$

The proof is the same as for the case of the Riemann zeta function (theorem 3.2) adding the $f(n)$'s everywhere.

I will need the following[(f)]

**Lemma 9.1.** *Suppose an arithmetic function $a(n)$ satisfies $\sum_{n \leq t} a(n) = \mathrm{O}(t^r)$ for some $r \geq 0$ as $t \to \infty$. Then the series $D_a$ converges for all $\sigma > r$, i.e. $\sigma_0 \leq r$.*

Proof. Let $S(k) = \sum_{n=1}^{k} a(n)$. By the assumption there exists a $B > 0$ such that $|S(k)| \leq Bk^r$. Using this and Abel's lemma we get

$$\begin{aligned}
\left|\sum_{n=m}^{k} \frac{a(n)}{n^s}\right| &\leq \left|\frac{S(k)}{k^s} - \frac{S(m-1)}{m^s}\right| + \left|\sum_{n=m}^{k-1} S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \\
&\leq B \cdot \left(\frac{k^r}{k^\sigma} + \frac{(m-1)^k}{m^\sigma} + \sum_{n=m}^{k-1} n^r \left| s \int_n^{n+1} \frac{dt}{t^{s+1}} \right|\right) \\
&\leq B\left(k^{r-\sigma} + m^{r-\sigma} + |s| \sum_{n=m}^{k-1} n^r \cdot \frac{1}{n^{\sigma+1}}\right)
\end{aligned}$$

Letting $m$ and $k$ go to infinity this expression goes to 0 for any $\sigma > r$, as the sum is bounded by

$$\int_{m-1}^{\infty} t^{r-\sigma-1} dt = \frac{(m-1)^{r-\sigma}}{r-\sigma}.$$

□

[(e)] see [3] p. 228 or [5] p. 26

[(f)] see [40] p. 182

There is another interesting result of LANDAU, this is almost at the end of what you called the "bible of prime".[g]

**Theorem 9.2.**
*Let $\sum_{n=1}^{\infty} a(n)n^{-s}$ be a Dirichlet series with $a(n) \geq 0$. Let $\sigma_0 = \sigma_1 < \infty$ be the abscissa of convergence. The analytic function $D_a(s)$, represented by the Dirichlet series for $s > \sigma_0$, has a pole at $s = \sigma_0$.*

I am afraid I didn't give you the proof behind it, although it is rather nice. But we will not need this theorem for our purpose. Later we will connect the Dirichlet series with the characters, but first we leave on a journey in the number fields.
The one who has the immense pleasure to walk through the field of numbers with you. C.W.

[g] she meant [36], see p. 880;
LANDAU is more general, he looks at the series of the form

$$\sum_{n=1}^{\infty} a(n)e^{-\lambda_n z}.$$

# Letter 10

# The Unit Group

Come with me, my dear princess, to other fields than the rational.

Let $K$ be a number field.[(a)] Denote by $\mathfrak{o}$ its number ring[(b)] and by $d$ its discriminant.[(c)] I will use the symbol $\sigma_1$, $\sigma_2$, ... $\sigma_r$ for the real embeddings of $K$ in $\mathbb{C}$ (if there are some) and $\tau_1$, $\tau_2$, ... $\tau_{\hat{r}}$, $\overline{\tau_1}$, $\overline{\tau_2}$, ... $\overline{\tau_{\hat{r}}}$ for the none real embeddings. Denote $n = r + 2\hat{r} = [K\colon \mathbb{Q}]$ and $N\colon K \to \mathbb{R}$ the norm[(d)] over $\mathbb{Q}$, i.e.

$$N(\omega) = \prod_{j=1}^{r} \sigma_j(\omega) \cdot \prod_{k=1}^{\hat{r}} |\tau_k(\omega)|^2 .$$

And so on, I think you still remember the definitions from the lessons last year, when I was still allowed to teach you. Our aim in this first letter about number fields is the determination of the structure of the unit group. The first who considered units of an algebraic number field was probably Gauss in the case $K = \mathbb{Q}[i]$. The main theorem 10.1 was discovered by Dirichlet, not in excatly the same form, because he used another definition of algebraic integer. According to Minkowski the idea of the proof occured to Dirichlet as he was listening to the Eastern concert in the Sistine Chapel.[(e)]

I will have to jump between different spaces. Firstly, we look at $K$ as its image under the injection

$$\begin{aligned} K &\rightarrowtail \mathbb{R}^r \times \mathbb{C}^{\hat{r}} \\ \omega &\mapsto (\sigma_1(\omega), \ldots, \sigma_r(\omega), \tau_1(\omega), \ldots, \tau_{\hat{r}}(\omega)) \end{aligned}$$

Under this identification $\mathfrak{o}$ and its ideals[(f)] $\mathfrak{a}$ become lattices[(g)] of rank $n$. To see this we will show that the volume of a fundamental parallelotope is nonzero. Let $\alpha_1$, $\alpha_2$, ... , $\alpha_n$ be the $\mathbb{Z}$-basis[(h)] of an ideal $\mathfrak{a}$ in $K$. Using elementary column transformations,

$$\begin{aligned} \operatorname{vol}(F_{\mathfrak{a}}) &= \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \operatorname{Re}\tau_1(\alpha_1) & \operatorname{Im}\tau_1(\alpha_1) & \ldots & \operatorname{Re}\tau_{\hat{r}}(\alpha_1) & \operatorname{Im}\tau_{\hat{r}}(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & & \ddots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \operatorname{Re}\tau_1(\alpha_n) & \operatorname{Im}\tau_1(\alpha_n) & \ldots & \operatorname{Re}\tau_{\hat{r}}(\alpha_n) & \operatorname{Im}\tau_{\hat{r}}(\alpha_n) \end{pmatrix} \right| \\ &= \left| \frac{1}{(2i)^{\hat{r}}} \det \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1(\alpha_1)} & \ldots & \tau_{\hat{r}}(\alpha_1) & \overline{\tau_{\hat{r}}(\alpha_1)} \\ \vdots & \ddots & \vdots & \vdots & & \ddots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1(\alpha_n)} & \ldots & \tau_{\hat{r}}(\alpha_n) & \overline{\tau_{\hat{r}}(\alpha_n)} \end{pmatrix} \right| \end{aligned}$$

[(a)] this is a finite dimensional algebraic field extension of $\mathbb{Q}$ embedded in $\mathbb{C}$.
[(b)] this is the integral closure of $\mathbb{Z}$ in $K$, see [37] p. 5
[(c)] see [26] §23, p. 73
[(d)] see [26] §22, p. 71
[(e)] see [42] p.130
[(f)] ideal are always ordinary ideals of $\mathfrak{o}$ as a ring, not fractional ideals.
[(g)] this is a $\mathbb{Z}$-span in a real vector space.
[(h)] see [35] Satz 99, p. 29

and the formula for this determinant[(i)], we get

$$\mathrm{vol}\,(F_{\mathfrak{a}}) = \frac{1}{2^{\hat{r}}} N(\mathfrak{a})\sqrt{|d|} \neq 0. \tag{10.1}$$

The norm can be defined for the whole $\mathbb{R}^r \times \mathbb{C}^{\hat{r}}$ by

$$N(x,z) = \prod_{j=1}^{r} x_j \cdot \prod_{k=1}^{\hat{r}} |z_k|^2 \tag{10.2}$$

Secondly, as we are interested in the multiplicative structure of $\mathfrak{o}$, we jump to another space, the *logarithmic space* $V$. Look at the group homomorphism

$$\begin{aligned} \log\colon (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^{\hat{r}} &\to V = \mathbb{R}^{r+\hat{r}} \\ (x_1,\ldots,x_r,z_1,\ldots,z_{\hat{r}}) &\mapsto (\ln|x_1|,\ldots,\ln|x_r|,2\ln|z_1|,\ldots,2\ln|z_{\hat{r}}|) \end{aligned}$$

where $\mathbb{R}^\times$ and $\mathbb{C}^\times$ is $\mathbb{R}\setminus\{0\}$, and $\mathbb{C}\setminus\{0\}$ respectively, with its multiplicative group structure. In this space the norm can be written as

$$\epsilon(\log(x,z)) = \ln|N(x,z)|, \qquad \text{where } \epsilon(t) = \sum_{j=1}^{r+\hat{r}} t_j. \tag{10.3}$$

The kernel of log restricted to $\mathfrak{o}$ is the group of all roots of unity, denoted by $W$. It is a cyclic group of finite order, say $w$.[(j)] Let $U$ be the group of unites in $\mathfrak{o}$. We see that $\log U = H \cap \log(\mathfrak{o}\setminus\{0\})$ where $H = \ker\epsilon$ is a hyperplane in $V$, since an element of $\mathfrak{o}$ is a unit if and only if its norm is $\pm 1$.[(k)] For all other elements $\epsilon(\log\omega)$ is positive. As $\log U$ has the property that every bounded subset is finite, it is a lattice in $H$.[(l)] It remains just to show that its dimension is $r+\hat{r}-1$ and we will have proven the

**Unit Group Theorem 10.1.**
*The unit group $U$ is a direct product of $W$ with a free abelian group of rank $r+\hat{r}-1$.*

In other words: There exist units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+\hat{r}-1}$, called a *fundamental system of units*, such that the expression

$$\zeta^l \varepsilon_1^{k_1}\varepsilon_2^{k_2}\cdots\varepsilon_{r+\hat{r}-1}^{k_{r+\hat{r}-1}}$$

($\zeta$ is a primitive root of unity in $\mathfrak{o}$) represents exactly once every unit when $l$ runs from 0 to $w-1$ and the $k_j$'s vary in $\mathbb{Z}$.

In order to prove it we need a lemma, which is a corollary of Minkowski's theorem for linear forms:

**Lemma 10.2.** *Let $\mu \in V$ such that $\epsilon(\mu) = \ln\sqrt{|d|}$. Then there exists an $\alpha \in \mathfrak{o}$ such that $\log\alpha$ has smaller coordinates than $\mu$ in the standard basis, i.e. lies in the $r+\hat{r}$-simplex formed by $\mu$ and all its standard projection onto $H$.*

[(i)] see [35] Satz 103, p.31
[(j)] see [42] proposition 3.4
[(k)] see [35] Satz 46, p. 16
[(l)] see [40] exercise 5.31, p. 151 or see [37] p. 69

Figure 10.1: The simplex of lemma 10.2

PROOF. Let $\varkappa_j = e^{\mu_j} > 0$ for $j = 1, \dots r$ and $\varkappa_{r+k} = \varkappa_{r+\hat{r}+k} = e^{\frac{1}{2}\mu_{r+k}}$ for $k = 1, \dots \hat{r}$. Thus $\prod_{j=1}^{r+2\hat{r}} \varkappa_j = e^{\epsilon(\mu)} = \sqrt{|d|}$. Use the matrix

$$\begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_r(\omega_1) & \tau_1(\omega_1) & \overline{\tau_1(\omega_1)} & \dots & \tau_{\hat{r}}(\omega_1) & \overline{\tau_{\hat{r}}(\omega_1)} \\ \vdots & \ddots & \vdots & \vdots & & \ddots & & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_r(\omega_n) & \tau_1(\omega_n) & \overline{\tau_1(\omega_n)} & \dots & \tau_{\hat{r}}(\omega_n) & \overline{\tau_{\hat{r}}(\omega_n)} \end{pmatrix},$$

($\omega_1, \dots, \omega_n$ a $\mathbb{Q}$-basis of $K$ in $\mathfrak{o}$), whose absolute value is by definition $\sqrt{|d|}$, in Minkowski's theorem[m] to get $x_1, \dots, x_n \in \mathbb{Z}$ such that $\alpha = \sum_{l=1}^{n} \omega_l x_l \in \mathfrak{o}$ satisfies

$$|\sigma_j(\alpha)| = \left| \sum_{l=1}^{n} \sigma_j(\omega_l) x_l \right| \leq \varkappa_j \qquad |\tau_k(\alpha)| = \left| \sum_{l=1}^{n} \tau_k(\omega_l) x_l \right| \leq \varkappa_{r+k}$$

$$(\log \alpha)_j = \ln |\sigma_j(\alpha)| \leq \ln \varkappa_j = \mu_j \qquad (\log \alpha)_{r+k} = 2 \ln |\tau_k(\alpha)| \leq 2 \ln \varkappa_{r+k} = \mu_{r+k}$$

Which finishes the proof. □

PROOF OF THE UNIT GROUP THEOREM. The theorem is proven if we show that $\log U$ is not completely contained in a subspace of H of codimension 1 So let $0 \neq \gamma \in V^*$ be a form on $V$ whose kernel is not equal to $H$. We have to find an $\varepsilon \in U$ who is sent in the kernel of $\gamma$.

I denote by $H' \subset V$ the affine hyperplane parallel to $H$ defined by the equation $\epsilon(t) = \ln \sqrt{|d|}$. Let $A > 0$ be a parameter. For every $h \in \mathbb{N}$, let $\mu_h \in H'$ such that $\gamma(\mu_h) = Ah$. So $\mu_h$ lies somewhere on an affine subspace $l_h$ of $H'$ of codimension 1, parallel to $\ker \gamma$. By the lemma, there exists for every $h$ an $\alpha_h \in \mathfrak{o}$ with its image in the $r + \hat{r}$-simplex between $H$ (see picture below) and $\mu_h$. $A$ can be chosen sufficiently big to guarantee that these simplices don't intersect. ($A$ is a parameter for the distance between the rungs of the ladder in the picture.) So we have a sequence $\alpha_1, \alpha_2, \dots$ with $N\big((\alpha_j)\big) = |N(\alpha_j)| \leq \sqrt{|d|}$ (since they lie between $H$ and $H'$). But we can only have finitely many ideals with norm smaller than $\sqrt{|d|}$.[n] So two of these $\alpha$'s must be associated, say $\alpha_h$ and $\alpha_{h'}$. Hence there exists a unit $\varepsilon$ with $\alpha_h = \varepsilon \alpha_{h'}$. As $\log \alpha_h = \log \varepsilon + \log \alpha_{h'}$ means that $\log \varepsilon$ is a vector pointing form the simplex beneath $\mu_h$ to the one beneath $\mu_{h'}$, $\log \varepsilon$ can not lie in the kernel of $\gamma$. □

This is all I've got to tell you today. You may ask why we are interested in units. I hope you will understand this better in my next letter when we will count ideals. So we are going to switch some more between these two spaces. Yours faithfully, C.W. .

Figure 10.2: The ladder

[m] see [26] Theorem 95, §33, p. 104
[n] see [35] Satz 34, §34, p. 33

## Letter 11

# Density of Ideals in a Class

My dearest princess,
I would like to dance with you, once more, through the spaces. For this time, our goal is to count the ideals in a class.[a] We will calculate a certain limit of a fraction which we will call later the "density" of the prime ideals in the class and we will see that this is closely connected to the zeta function of the number field.

Let $e_1, \dots, e_{r+\hat{r}-1}$ be a $\mathbb{Z}$-basis of the lattice $\log U$. I define the *regulator* of the field $K$ to be the volume of the fundamental parallelotope of $\log U$ in $H$ divided by the constant $\sqrt{r+\hat{r}}$.[b]

**Theorem 11.1.**
*Let $C$ be a class of ideals. Let $Z_C(t)$ denote the number of ideals in $C$ with norm smaller than $t$. Then*

$$\lim_{t\to\infty} \frac{Z_C(t)}{t} = \kappa = \frac{2^{r+\hat{r}}\,\pi^{\hat{r}}\,R}{w\sqrt{|d|}} \tag{11.1}$$

Proof. Fix an ideal $\mathfrak{a}$ in the inverse class of $C$. There is a bijection between the ideals $\mathfrak{b}$ in $C$ and the principal ideals $(\omega)$ contained in $\mathfrak{a}$, given by $\mathfrak{a}\mathfrak{b} = (\omega)$.[c] So $Z_C(t)$ is the number of non-associated $\omega$'s in $\mathfrak{a}$ with

$$|N(\omega)| = N\big((\omega)\big) \le tN(\mathfrak{a}). \tag{11.2}$$

Complete $e_1, \dots, e_{r+\hat{r}-1}$ to a basis of $V$, by adding $v = (1, 1, \dots, 1) \in H^{\perp}$. Every $\omega \in \mathfrak{a}$ can be written as

$$\log\omega = \sum_{j=1}^{r+\hat{r}-1} c_j e_j + c_{r+\hat{r}} v \tag{11.3}$$

We can multiply a given $\omega$ with units (adding a $\mathbb{Z}$-linear combination of $e_j$ to $\log\omega$) in order to get the $0 \le c_j < 1$ for all $j = 1, \dots r+\hat{r}-1$. Every set of associated $\omega$'s as a representative with the first $r+\hat{r}-1$ coordinates smaller than 1. The condition on the norm our $\omega$'s in (11.2) becomes

$$\ln|tN(\mathfrak{a})| \ge \ln|N(\omega)| = \epsilon(\log\omega) = c_{r+\hat{r}}\epsilon(v) = c_{r+\hat{r}} \cdot (r+\hat{r}).$$

So if we define the parallelotope $P_b$ in $V$ by

$$P_b = \Big\{ c_{r+\hat{r}} v + \textstyle\sum_{j=1}^{r+\hat{r}-1} c_j e_j \mid 0 \le c_j < 1, 0 \le c_{r+\hat{r}-1} \le b \Big\} \qquad \text{with } b = \frac{\ln|tN(\mathfrak{a})|}{r+\hat{r}}.$$

we have simply $Z_C(t) = \#(\log\mathfrak{a} \cap P_b)$. Now we go back to $\mathbb{R}^r \times \mathbb{C}^{\hat{r}}$, remembering that the $\ker\log = W \subset U$ has $w$ element, we can write $w \cdot Z_C(t) = \#(\mathfrak{a} \cap \log^{-1} P_b)$. Since $\mathfrak{a}$ is a lattice, this will be approximately

$$w \cdot Z_C(t) \sim \frac{\operatorname{vol}\left(\log^{-1} P_b\right)}{\operatorname{vol}\left(F_{\mathfrak{a}}\right)} \tag{11.4}$$

[a] for the definition of a class see [26] §33, pp. 105 - 108
[b] see [40] Theorem 41, p. 175
[c] see [35] Satz 68, §5, p.21

Let us have a look at the preimage of a point in the logarithmic space.

$$\log(x_1, \dots, x_r, \rho_1 e^{i\theta_1}, \dots, \rho_{\hat{r}} e^{i\theta_{\hat{r}}}) = (t_1, \dots, t_{r+\hat{r}})$$

gives the conditions

$$\begin{aligned} x_j &= \pm e^{t_j} && j = 1, \dots, r \\ \rho_k &= e^{\frac{1}{2} t_{r+k}} && k = 1, \dots, \hat{r} \\ \theta_k &\in [0, 2\pi) && k = 1, \dots, \hat{r} \end{aligned} \tag{11.5}$$

So the preimage of $P_b$ splits into $2^r$ disjointed set (according to the choice of signs for the $x$'s). Fixing a $\theta \in [0, 2\pi)^{\hat{r}}$, we get a set $U_\theta$ which is diffeomorophic to $P_b$. Thus

$$\operatorname{vol}\left(\log^{-1} P_b\right) = 2^r \int_0^{2\pi} \cdots \int_0^{2\pi} \operatorname{vol}(U_\theta)\, d\theta_1 \cdots d\theta_{\hat{r}} \tag{11.6}$$

Let us calculate

$$\operatorname{vol}(U_\theta) = \int_{U_\theta} \rho_1 \cdots \rho_{\hat{r}} \cdot dx_1 \cdots dx_r d\rho_1 \cdots d\rho_{\hat{r}}$$

using the transformation (11.5):

$$\begin{aligned} \operatorname{vol}(U_\theta) &= \int_{P_b} e^{\frac{1}{2} t_{r+1}} \cdots e^{\frac{1}{2} t_{r+\hat{r}}} \cdot e^{t_1} \cdots e^{t_r} \cdot \frac{1}{2} e^{\frac{1}{2} t_{r+1}} \cdots \frac{1}{2} e^{\frac{1}{2} t_{r+\hat{r}}} \cdot dt_1 \cdots dt_{r+\hat{r}} \\ &= \frac{1}{2^{\hat{r}}} \int_{P_b} e^{\epsilon(t)} dt_1 \cdots dt_{r+\hat{r}} \end{aligned}$$

We'd like to change basis to $e_1, \dots, e_{r+\hat{r}-1}, v$. As $v$ is orthogonal to $H$, the volume of the parallelotope spanned by the basis is just $R\sqrt{r+\hat{r}} \cdot |v| = R(r+\hat{r})$ by definition of the regulator. Hence

$$\begin{aligned} \operatorname{vol}(U_\theta) &= \frac{1}{2^{\hat{r}}} \int_{P_b} e^{c_{r+\hat{r}} \epsilon(v)} R(r+\hat{r}) dc_1 \cdots dc_{r+\hat{r}} \\ &= \frac{1}{2^{\hat{r}}} R(r+\hat{r}) \int_0^b \int_0^1 \cdots \int_0^1 e^{c_{r+\hat{r}}(r+\hat{r})} dc_1 \cdots dc_{r+\hat{r}} \\ &= \frac{1}{2^{\hat{r}}} \frac{(r+\hat{r})\, R\, (e^{b(r+\hat{r})} - 1)}{r+\hat{r}} \\ &= \frac{1}{2^{\hat{r}}} R\, (tN(\mathfrak{a}) - 1) \end{aligned}$$

Now we can stick together all the pieces we found. First we use (11.6), and we obtain

$$\operatorname{vol}\left(\log^{-1} P_b\right) = 2^r\, (2\pi)^{\hat{r}}\, \frac{1}{2^{\hat{r}}}\, R\, (tN(\mathfrak{a}) - 1)$$

Hence, by (11.4) and (10.1),

$$\begin{aligned} Z_C(t) &\sim \frac{2^r\, \pi^{\hat{r}}\, R\, (tN(\mathfrak{a}) - 1)}{w\, 2^{-\hat{r}}\, N(\mathfrak{a})\, \sqrt{|d|}} \\ &\sim \frac{2^{r+\hat{r}}\, \pi^{\hat{r}}\, R\, N(\mathfrak{a})}{w\, \sqrt{|d|}\, N(\mathfrak{a})} t \end{aligned}$$

□

From Theorem 11.1, we can deduce at once

**Theorem 11.2.**
*Let $Z(t)$ denote the number of ideals whose norm is smaller than $t$. Then*

$$\lim_{t\to\infty} \frac{Z(t)}{t} = \kappa\, h,$$

*where $h$ is the class number of the field.*

MARCUS proves in his book[(d)] that the error term in the last two theorems has order $O\left(t^{1-\frac{1}{n}}\right)$. The proof is based on the fact that the boundary of $\log^{-1} P_b$ is $(n-1)$-Lipschitz-parametrizable. I will use this without proof.

You may get tired of this long way we are traveling to get to the result I promised you at the beginning, the theorem of Dirichlet. But you realize that from the window of our train that brings us there, we can see much more other beautiful landscapes of our Numberland.

Your traveling companion.

[(d)] see [40] theorem 39, p.158

# Letter 12

# Dedekind's Zeta Function

Oh, my princess,
Your letter really surprised me, and Magdalene told me more about your project. Be advised that I will support it and try to help you with all means. The guardian that your father has put in front of your room will be "well primed". But its too dangerous to write about it, I will discuss everything with Magdalene.

We come to the application of what we did the last two letters. I define the Dedekind zeta function, this function was introduced by DEDEKIND:[(a)]

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \tag{12.1}$$

where the sum runs over all nonzero ideals $\mathfrak{a}$ in $\mathfrak{o}$. If I denote the number of ideal with norm $n$ by $j(n)$ then I can rewrite it as

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j(n)}{n^s} \tag{12.2}$$

which is a Dirichlet series $D_j$ with a multiplicative function $j$.[(b)]

**Lemma 12.1.**

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} \tag{12.3}$$

*(the sum running over all nonzero prime ideals of $\mathfrak{o}$) converges absolutely in the half plane $\sigma > 1$.*

PROOF. Every $\mathfrak{p}$ can divide at most one prime number $p \in \mathbb{Z}$. Conversely, every prime splits in at most $n$ distinct prime ideal.[(c)] So the partial sum in (12.3) for the $\mathfrak{p}$ dividing $p$ is smaller than $\frac{n}{p^s}$, as $N(\mathfrak{p}) = p^f$ for some $f \geq 1$.[(d)] And the statement follows from the fact that $\sum \frac{1}{p^s}$ converges for $\sigma > 1$ and $N(\mathfrak{p}) > 0$. □

The following theorem was proved by LANDAU in [32].

**Theorem 12.2.**
*Let $n = [K : \mathbb{Q}]$. $\zeta_K(s)$ can be extended to an analytic function of the half plane $\sigma > 1 - \frac{1}{n}$ except for a simple pole at $s = 1$ with residue $h \cdot \kappa$. Moreover we have*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \tag{12.4}$$

*converges absolutely for all $\sigma > 1$. (The product runs over all nonzero prime ideals of $\mathfrak{o}$.)*

---

[(a)] see [14]
[(b)] see [26] §41, p. 144
[(c)] see [40] theorem 65, p.65
[(d)] $f$ is the inertial degree of $\mathfrak{p}$ over $\mathbb{Q}$.

PROOF. For $\sigma > 1$ I can write

$$\zeta_K(s) = h\,\kappa\,\zeta(s) + \sum_{n=1}^{\infty} \frac{j(n) - h\,\kappa}{n^s}$$

Well, as $\sum_{n\le t}(j(n) - h\,\kappa) = Z(t) - [t]\,h\,\kappa = \mathrm{O}\big(1 - \frac{1}{n}\big)$, by the last remark in the previous letter, we can apply the lemma 9.1 to prove that the series in the equation above converges for $\sigma > 1 - \frac{1}{n}$. So the first statement in the theorem is a consequence of the properties of the Riemann zeta function, see theorem 3.3.

The proof of the second statement is essentially the same as the Euler's product formula (3.2) using the unique prime ideal factorisation in the number ring $\mathfrak{o}$.[(e)] The convergence follows form the previous lemma. □

Of course, there is, similar to the rational case, a meromorphic continuation of $\zeta_K(s)$ for the whole plane and, using a formula for theta functions, HECKE proved a functional equation.[(f)] But this is rather complicated: The function

$$\left(2^{-\hat{r}}\pi^{-\frac{n}{2}}\sqrt{|d|}\right)^s \cdot \Gamma\left(\frac{s}{2}\right)^r \cdot \Gamma(s)^{\hat{r}} \cdot \zeta_K(s)$$

doesn't change when $s$ is replaced by $1 - s$.[(g)] There are similar formulas for $N(T)$ and there are explicit formulas as well for the generalized zeta functions. Using an integration with a contour as for the prime number theorem, LANDAU proved[(h)] that the number of prime ideals with norm smaller than $t$ is

$$\mathrm{Li}(t) + \mathrm{O}\left(x\,e^{-\frac{\alpha}{\sqrt{n}}\sqrt{\ln t}}\right).$$

This leads to the surprising fact[(i)] that any two number fields have asymptotically the same number of prime ideals of norm less then $t$ (as $t \to \infty$).

One can also define the zeta function just for a subset $A$ of prime ideals in $\mathfrak{o}$: Let $\langle A\rangle$ be the free abelian semigroup of ideals generated by $A$. Consider the function

$$\zeta_K(s; A) = \sum_{a\in\langle A\rangle} \frac{1}{N(\mathfrak{a})^s} \tag{12.5}$$

And once again, $\zeta_K(s, A)$ is a analytic function for $\sigma > 1$ and

$$\zeta_K(s; A) = \prod_{\mathfrak{p}\in A} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \tag{12.6}$$

Now we look at the logarithm of this zeta functions

$$\ln\zeta_K(s; A) = \sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}\in A}\sum_{m=2}^{\infty} \frac{1}{m\,N(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s} + \mathrm{O}(1) \tag{12.7}$$

as $s \downarrow 1$, similar to (3.4). We could ask what the prime ideals in $A$ contributes to the divergence of the zeta function for $s \downarrow 1$. This defines a "density" of $A$ in the set of all prime ideals, namely the *Dirichlet density* defined as

$$\delta(A) = \lim_{s\downarrow 1} \frac{\sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s}}{\sum_{\text{all } \mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}} \tag{12.8}$$

---

(e) see [26] §25, theorem 72, p. 85
(f) see [25]
(g) see [35] Satz 155, p. 75
(h) see [35] Satz 191, p. 113
(i) see [35] Satz 193, p. 114

If the function $\zeta_K(s;A)$ can be extended around the point $s=1$, then this density equals

$$\delta(A) = \frac{\operatorname{Res}_{s=1}\zeta_K(s;A)}{\operatorname{Res}_{s=1}\zeta_K(s)}$$

as $\ln\zeta_K(s;A) \sim \ln\frac{\text{residue}}{s-1}$.

We will try to calculate some densities: What about an ideal class $C$? You can easily convince yourself that the residue of $\zeta_K(s;C)$ at $s=1$ is equal to $\kappa$. (Generalize theorem 12.2, using $Z_C(t)$ and the theorem 11.1.) So we found

$$\delta(C) = \frac{\kappa}{h\,\kappa} = \frac{1}{h} \tag{12.9}$$

which is independent of the class. It doesn't imply that there are asymptotically the same number of prime ideals in each class. This fact would need a bit more work. For example, this means that about half of the prime ideals in $\mathbb{Z}[\sqrt{-5}]$ are principal (the class number is 2).

What is the density of the prime ideals of degree one? Using the same arguments as in the proof of lemma 12.1 we can show that the density of the prime ideals with degree $f$ greater than one is 0:

$$1 \le \prod_{\mathfrak{p}\text{ with }f\ge 2}(1-\frac{1}{N(\mathfrak{p})^s})^{-1} \le \prod_p (1-\frac{1}{p^{fs}})^{-n} = \zeta(fs)^n$$

Thus as $s$ tends to 1, the zeta function of those prime ideals stays bounded. So the prime ideals of degree one have density 1, in particular there exists infinitely many.

Or more general, we can prove the following[j]

**Theorem 12.3.**
*Let $L$ be a normal extension of $K$ of degree $n=[L:K]$. The set of prime ideals in $\mathfrak{o}$ which split completely*[k] *in the number ring of $L$ has density $\frac{1}{n}$.*

Proof. Let $A$ be the set of such prime ideals in $\mathfrak{o}$ and $B$ the set of prime ideals in the number ring of $L$ lying over elements in $A$. For every $\mathfrak{p}\in A$ we have $N_K(\mathfrak{p}) = N_L(\mathfrak{q})$ for all $\mathfrak{q}$ lying over $\mathfrak{p}$ (as $nN_K(\mathfrak{p}) = N_L(\mathfrak{p}) = nN_L(\mathfrak{q})$ by normality of $L:K$); and there are exactly $n$ such $\mathfrak{q}$. Thus

$$\sum_{\mathfrak{p}\in A}\frac{1}{N_K(\mathfrak{p})^s} = \frac{1}{n}\sum_{\mathfrak{q}\in B}\frac{1}{N_L(\mathfrak{q})^s}$$

So we are done if we prove that $B$ has density 1 in the prime ideals of the number ring of $L$. But $B$ contains all prime ideals $\mathfrak{q}$ for which $N_L(\mathfrak{q})$ is a prime number, and these are all but finitely[l] many which are ramified over $K$. □

Having flown high in the clouds we come back to earth:

**Corollary 12.4.** *Let $m\ge 2$ be an integer. The prime numbers which are congruent to 1 modulo $m$ have density $\frac{1}{\varphi(m)}$.*[m] *In particular there are infinitely many.*

Proof. Consider the normal extension $\mathbb{Q}[e^{\frac{2\pi i}{m}}]:\mathbb{Q}$ of degree $\varphi(m)$. Those prime number who split completely in the $m^{\text{th}}$ cyclotomic field are exactly those who are congruent to 1 modulo $m$, except for finitely many.[n] □

And we proved Dirichlet's theorem for a special case $a=1$.

And now I will prime myself for the battle. Yours, C.W.

---

[j] for all definitions of prime decomposition see [40] chapter 3

[k] this is a prime ideal whose decomposition as a ideal in $L$ splits in $n$ distinct prime ideals, see [40] p. 105

[l] see [40] theorem 24, p. 72

[m] Without indicating the author meant the Euler phi-function here

[n] see [26] theorem 92, p.99

# Letter 13

# The Theorem of Dirichlet

My dearest prime-cess,
Since you left the country of your ancestors, a lot has happened. Your father, the King is beside himself and the prime minister as well, for he believed to be your prime favorite when they found a lot of primes in your room. But you, being in the prime of your youth, followed your prime mover, and left the prison, your father's palace.

This shall be my last letter, because we will finally come to the proof of the theorem of Dirichlet. But I would like to formulate it a little bit more general,[a] in order to prove the same result for the Gaussian numbers $\mathbb{Q}[i]$, for instance.

So let $K$ be a number field whose ring of numbers $\mathfrak{o}$ is a unique factorisation domain, i.e. a principal ideal domain.[b] We can choose a system of representatives $\mathcal{N}$ of generators of the nonzero ideals. (For the special case $\mathbb{Q}$ and $\mathbb{Q}[i]$ we have $\mathcal{N} = \mathbb{N} = \{1, 2, \dots\}$ and $\mathcal{N} = \mathbb{N} + \mathbb{N}i$ respectively.) Let $m$ be an element of $\mathcal{N}$. I denote the ideal $(m)$ by $\mathfrak{m}$. I would like to look at the group $\tilde{G} = (\mathfrak{o}/\mathfrak{m})^*$, the group of invertible cosets of $\mathfrak{m}$. This group has order[c]

$$|\tilde{G}| = \varphi(\mathfrak{m}) = N(\mathfrak{m}) \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{N(\mathfrak{p})}\right) = |N(m)| \prod_{p|m} \left(1 - \frac{1}{|N(p)|}\right), \tag{13.1}$$

where $p$ runs through the prime numbers in $\mathcal{N}$ dividing $m$.

Unfortunately, if we choose two different generators for an ideal, $p$ and $-p$ in the rational case, they would not come to lie in the same coset modulo $\mathfrak{m}$. We have thus to factor out the units, I hope you forgive me this complification. So let $G = \tilde{G}/\tilde{U}$, where $\tilde{U}$ is the subgroup generated by units modulo $\mathfrak{m}$. Let $\chi \in \hat{G}$ be a character of $G$. It can be extended to all $n \in \mathfrak{o}$ by putting $\chi(n) = 0$ if $(n, m) = 1$. This isn't a character anymore, but it is still strictly multiplicative. It can be interpreted as a multiplicative function from the set of ideals in $\mathfrak{o}$ to $\mathbb{C}$, simply defining $\chi(\mathfrak{a})$ by the value of $\chi$ on one of its generators. (That's why we killed the units.)

We are able to define now the Dirichlet $L$-series:

$$L(s, \chi) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{n \in \mathcal{N}} \frac{\chi(n)}{|N(n)|^s} = \prod_p \left(1 - \frac{\chi(p)}{|N(p)|^s}\right)^{-1} \tag{13.2}$$

($p$ running through the primes in $\mathcal{N}$.) Using the same idea as for the Dedekind zeta function, this is a Dirichlet series. The second formula is a consequence of (9.3). What is its abscissa of convergence? If $\chi \neq \chi_1$, then the orthogonality relation (8.2) provides that the sum $\sum_{|N(n)| \leq t} \chi(n)$ stays bounded as $t \to \infty$. Thus, applying lemma 9.1 shows that $\sigma_0 = 0$. Now

[a] the idea of the following generalisation was found in [27], page 178, there is even the proof of 13.2 for any number field

[b] see [42] theorem 1.16

[c] see [42] theorem 1.8

we have a look at the $L$-series of the principal character:

$$\begin{aligned} L(s,\chi_1) &= \prod_p \left(1 - \frac{\chi_1(p)}{|N(p)|^s}\right)^{-1} \\ &= \prod_{p\nmid m} \left(1 - \frac{1}{|N(p)|^s}\right)^{-1} \\ &= \zeta_K(s) \cdot \prod_{p\mid m} \left(1 - \frac{1}{|N(p)|^s}\right) \end{aligned} \tag{13.3}$$

Thus in particular, $L(s,\chi_1)$ can be extended to an analytic function $\sigma > 1 - \frac{1}{[K:\mathbb{Q}]}$ except for a simple pole at $s = 1$ with residue $h\,\kappa\,\varphi(\mathfrak{m})$.

The crucial fact to prove Dirichlet's theorem is the fact that the $L$-series don't vanish at $s = 1$. I am going to give you two proofs, the first, more general, analytic one right now (using a result without proof), the other one (only for the rational case) at the end of the letter.

**Lemma 13.1.** *If $\chi \neq \chi_1$ then $L(1,\chi) \neq 0$*

PROOF. First I want to introduce another function

$$Z(s) := \prod_{\chi\in\hat{G}} L(s,\chi) \tag{13.4}$$

Putting $T = |N(p)|^{-s}$ in (8.5) gives

$$Z(s) = \prod_{p\nmid m} \left(1 - \frac{1}{|N(p)|^{\lambda(p)s}}\right)^{-\mu(p)} \qquad \text{for } \sigma > 1 \tag{13.5}$$

where $\lambda(p)$ is the order of $p$ in $G$ and $\mu(p)$ equals $\frac{|G|}{\lambda(p)}$. I will use now (without proof) that $L(1,\chi_1)$ can be extended to an analytic function for $\sigma > 0$ except for the simple pole at $s = 1$. (For the rational case this is clear, by (13.3), and for the general case it follows from the continuation of the Dedekind zeta function found by HECKE.)

Now, we are ready to prove the lemma: If there were a character $\chi \neq \chi_1$ such that $L(1,\chi) = 0$, then $Z(s)$ would be an analytic function for $\sigma > 0$. (The zero would kill the pole of $L(s,\chi_1)$ at $s = 1$.) The product (13.5) would converge for all $\sigma > 0$, in contradiction to the fact that

$$\begin{aligned} (1 - |N(p)|^{-\lambda(p)s})^{-\mu(p)} &= (1 + |N(p)|^{-\lambda(p)s} + |N(p)|^{-2\lambda(p)s} + \cdots)^{\mu(p)} \\ &\geq (1 + |N(p)|^{-|G|s} + |N(p)|^{-2|G|s} + \cdots) \\ Z(s) = \prod_p (1 - |N(p)|^{-\lambda(p)s})^{-\mu(p)} &\geq \prod_p (1 - |N(p)|^{-s\,|G|})^{-1} = \zeta_K(s\ |G|) \end{aligned}$$

diverges for $s = 1/|G| > 0$. □

And the moment you have been waiting for so long time:

**Dirichlet's Theorem 13.2.**
*The density of the prime numbers in every invertible coset modulo $\mathfrak{m}$ is equal to $\frac{1}{\varphi(\mathfrak{m})}$.*

Note that we can speak of "density of prime numbers" as the prime ideals correspond to $p \in \mathcal{N}$ in a principal ideal domain.

PROOF. Denote by $A$ the set of prime ideal whose generator in $\mathcal{N}$ belongs to the a given class in $G$. Let $a \in A$, so $(m, a) = 1$. We are interested in the behaving of the sum

$$\sum_{\mathfrak{p} \in A} \frac{1}{N(\mathfrak{p})^s} = \sum_{p \equiv a} \frac{1}{|N(p)|^s}$$

as $s$ decreases to 1, with $p \equiv a$ if they are projected on the same element in $G$.

For $\sigma > 1$, I can write

$$\ln L(s, \chi) = -\sum_p \ln \left(1 - \frac{\chi(p)}{|N(p)|^s}\right) = \sum_p \sum_{\nu=1}^{\infty} \frac{\chi(p)}{\nu p^{\nu s}}. \tag{13.6}$$

And, I think you guessed it already,the sum for $\nu \geq 2$ is bounded when $s \to 1$. Since $(a, m) = 1$ there exists an integer $b$ such that $ab \equiv 1$. I will multiply the last equation by $\chi(b)$ and sum over all characters $\chi \in \hat{G}$.

$$\sum_{\chi \in \hat{G}} \chi(b) L(s, \chi) = \sum_p \sum_{\chi \in \hat{G}} \frac{\chi(bp)}{|N(p)|^s} + \mathrm{O}(1) \quad \text{as } s \downarrow 1$$

Using the orthogonality (8.2), $\sum_\chi \chi(bp)$ is equal to $|G|$ if $bp \equiv 1$ and vanishes otherwise, we get

$$\ln L(s, \chi_1) + \sum_{\chi \neq \chi_1} \chi(b) \ln L(s, \chi) = |G| \sum_{p \equiv a} \frac{1}{|N(p)|^s} + \mathrm{O}(1) \quad \text{as } s \downarrow 1 \tag{13.7}$$

By the previous lemma, the second term on the left hand side will stay bounded if $s$ approaches 1. Hence we can conclude that

$$\delta(A) = \lim_{s \downarrow 1} \frac{\frac{1}{|G|} \ln L(s, \chi_1)}{\ln \zeta_K(s)} = \frac{1}{|G|},$$

since $L(s, \chi_1)$ differs from $\zeta_K(s)$ only by a finite number of factors which stay bounded as $s \downarrow 1$, as we have seen in (13.3).

It remains to note that the generators of prime ideals which are sent to a given class in $G$ are equally distributed over $\tilde{G} = (\mathfrak{o}/\mathfrak{m})^*$, since $\tilde{U}$ is subgroup. Hence the density of prime numbers in a given coset modulo $\mathfrak{m}$ is

$$\frac{1}{|G|} \cdot \frac{1}{[\tilde{G} \colon G]} = \frac{1}{|\tilde{G}|} = \frac{1}{\varphi(\mathfrak{m})}.$$

□

**Corollary 13.3.** *In every arithmetic progression* $\{m\,n + a \mid n \in \mathbb{N}\}$ *there exists an infinity of prime numbers.*

The fact that the density is the same for all $a$ makes it looks probable that

$$\lim_{x \to \infty} \frac{{}_m\pi_a(x)}{{}_m\pi_{a'}(x)} = 1,$$

see (8.1), meaning that the primes are equally distributed between the invertible classes modulo $a$. But unfortunately this would need a little more work.[(d)]

Oh, I almost forgot: I still owe you the proof of the lemma in the rational case without the use of the continuation beyond $\sigma = 1$:

[(d)] see [47] p. 73 and p. 76

Look at the equation (13.7) for the special case $a = b = 1$:

$$\ln Z(s) = \sum_{\chi \in \hat{G}} \ln L(s, \chi) = \frac{\varphi(m)}{2} \sum_{p \equiv \pm 1 \bmod m} \frac{1}{p^s} + \mathrm{O}(1) \quad \text{as } s \downarrow 1$$

We have seen in 12.4 that the sum on the right hand side must diverge for $s \to 1$, hence $Z(s)$ cannot be bounded for $s = 1$.

This proof is much more elegant than the other I showed you before. So we would like to try to do this for the general case. We should find a field extension $L$ of $K$ such that the primes which split completely over $L$ are among those who are congruent to 1 modulo $\mathfrak{m}$. Such a field exists, it's the class field[(e)] ... Alas, here we are standing together at the door to a new world, which is unknown to me as well. They speak about class field theory, cohomology of groups, $\mathfrak{p}$-adic numbers, valuation, Artin maps, ... all things waiting to be discovered by us. Specially TATE's idea of Fourier analysis in number theory seems to me something for a next series of letters, once I will have understood it myself.

By the way, you may have heard that your father, believing you left with a man who turned your head, published the picture of GAUSS in all newspaper. "The one who finds this person will receive 1999 ducats."

Take care of yourself. Your prime minstrel.

[(e)] see [31] proposition 10.2

# Bibliography


[1] Edwin A. Abbott, *Flatland, A Romance of Many Dimension*, Basil Blackwell, Oxford, 1944.

[2] Martin Aigner and Günter M. Ziegler, *Proofs from The Book*, Springer, 1998.

[3] Tom M. Apostol, *Introduction to Analytic Number Theory*, UTM, Springer, 1976.

[4] ———, *Modular Functions and Dirichlet Series in Number Theory*, GTM, Springer, 1976.

[5] A. Blanchard, *Initiation á la théorie analytique des nombres premiers*, Dunod, Paris, 1969.

[6] Komaravolu Chadrasekharan, *Introduction to Analytic Number Theory*, Die Grundlehren der Mathematischen Wissenschaften, Springer, 1968.

[7] ———, *Arithmetical Functions*, Die Grundlehren der Mathematischen Wissenschaften, Springer, 1970.

[8] P. L. Chebyshev, *Œuvre de P. L. Tchebychef*, vol. 1, Chelsea Publishing Co., ?

[9] ———, *Mémoire sur les nombres premiers*, Journal de Mathématiques pures et appliquées **17** (1852), 366–390, Reprinted in [8] pp. 49 - 70.

[10] ———, *Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée*, Journal de Mathématiques pures et appliquées **17** (1852), 341–365, Reprinted in [8] pp. 25 - 48.

[11] Harold Davenport, *Multiplicative Number Theory*, Lectures in Advanced Mathematics, Markham Publishing Co., 1967.

[12] Charles Louis Xavier Joseph de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Annales de la Société scientifique de Bruxelles **20** (1896), 183–256 and 281–397.

[13] ———, *Sur la fonction $\zeta(s)$ de Riemann et le nombres premiers inférieus à une limite donnée*, Mémoires couronnés et autres mémoires publiés par l'Académie royal des Sciences, des Lettres et des Beaux-Arts de Belgique **59** (1899-1900), no. 1, 74.

[14] Richard Dedekind, *Über die Theorie der ganzen algebraischen Zahlen*, Vorlesungen über die Zahlentheorie [16], Friedrich Vieweg und Sohn, Braunschweig, 1879.

[15] Gustav P. Lejeune Dirichlet, *Über den Satz: dass jede arithmetische Progression, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viel Primzahlen enthält*, Bericht der Akademie der Wissenschaften zu Berlin (1837), 108–110.

[16] ———, *Vorlesungen über Zahlentheorie*, Friedrich Vieweg und Sohn, Braunschweig, 1879.

[17] Leonard Euler, Introductio in analysin infinitorum, vol. 1, 235, Bousquet, Lausanne, 1748, p. 235.

[18] ———, *Lettres à une princesse d'Allemagne sur divers sujets de physique et de philosophie*, Concorcet, Paris, 1789.

[19] Eberhard Freitag and Rolf Busam, *Funktionentheorie*, Springer, 1995.

[20] Carl F. Gauss, Werke, vol. 2, 444–447, Königliche Gesellschaft der Wissenschaften zu Göttingen, 1863, pp. 444–447, Brief von Gauss an Encke.

[21] Jacques Hadamard, *Études sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann*, Journal de Mathématiques pures et appliquées **9** (1893), no. 4, 171–215, Reprinted in [23] pp. 103 -149.

[22] ———, *Sur la distribution des zéro de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bulltin de la Société mathématique de France **24** (1896), 199–220, Reprinted in [23] pp. 189 -210.

[23] ———, *Œuvre de Jacques Hadamard*, vol. 1, Edition du centre National de la Recherche Scientifique, Paris, 1968.

[24] Godfrey H. Hardy and John E. Littlewood, *Contributions to the theory of the Riemann zeta-function and the theory of the distribution of primes*, Acta Mathematica **41** (1918), 119–196.

[25] Erich Hecke, *Über die Zetafunktion beliebiger algebraischer Zahlkörper*, Nachrichten der Akademie der Wissenschaften (1917), 77–89.

[26] ———, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981, Orgininal Edition: Vorlesung über die Theorie der algebraische Zahlen. Akademische Verlagsgesellschaft, Leipzig, 1923.

[27] ———, *Mathematische Werke*, Vandenhœk and Ruprecht, Göttingen, 1983.

[28] Loo Kang Hua, *Introduction to Number Theory*, Springer, 1982.

[29] A. E. Ingham, *The Distribution of Prime Number*, Cambridge University Press, 1932.

[30] Grodon James and Martin Liebeck, *Representations and Characters of Groups*, Cambridge Mathematical Textbooks, Cambrigde University Press, 1993.

[31] Gerald J. Janusz, *Algebraic Number Fields*, Academic Press, New York and London, 1973.

[32] Edmund G. H. Landau, *Ueber die zu einem algebraischen Zahlenkörper gehörige Zetafunction und die Ausdehnung der Tschebyscheffschen Primzahltheorie auf das Problem der Verteilung der Primideale*, Journal für reine und angewandte Mathematik **125** (1904), 64 – 188.

[33] ———, *Zwei neue Herleitungen für die asymptotische Anzahl der Primzahlen unter einer gegenbenen Grösse*, Sitzungsbericht der Preussischen Akademie der Wissenschaften (1908), 746–764.

[34] ———, *Über der Wienerschen neuen Weg zum Primzahlsatz*, Sitzungsbericht der Preussischen Akademie der Wissenschaften (1932), 514–521.

[35] ———, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Chelsea Publishing Company, 1949.

[36] ———, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea Publishing Company, 1953.

[37] Serge Lang, *Algebraic Numbers*, Addison-Wesley Publishing Company, Reading, Mass., 1964.

[38] Adrien M. Legendre, *Essai sur la théorie des nombres*, first ed., Duprat, Paris, 1798.

[39] ———, *Essai sur la théorie des nombres*, second ed., Courcier, Paris, 1808.

[40] Daniel A. Marcus, *Number fields*, Springer, 1977.

[41] A. Mertens, *Über eine Eigenschaft der Riemannschen ζ-Function*, Sitzungsbericht der kaiserlichen Akademie der Wissenschaften in Wien **108** (1898), no. 2a, 1429–1434.

[42] Władysław Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990, Include the longest bibliography I have ever seen (168 pages!).

[43] Karl Prachar, *Primzahlverteilung*, Die Grundlehren der Mathematischen Wissenschaften, Springer Verlag, 1957.

[44] Hans Rademacher, *Topics in analytic number theory*, Die Grundlehren der Mathematischen Wissenschaften, Springer, 1973.

[45] Bernhard Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der Königlichen Preussischen Akademie der Wissenschaften zu Berlin (1859), 671–680, Reprinted in [46] pp. 145 - 155.

[46] ———, *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, Dover Publications, New York, 1953.

[47] Jean Pierre Serre, *A Course in Arithmetic*, Springer, 1973.

[48] J. J. Sylvester, *On Tchebycheff's theory of the totality of prime numbers comprised whitin given limits*, American Journal of Mathematics **4** (1881), 230–247.

[49] Edward C. Titchmarsh, *The Theory of Riemann's Zeta Function*, Clarendon Press, 1951.

[50] H. von Koch, *Sur la distribution des nombres premiers*, Acta Mathematica **24** (1901), 159–182.

[51] H. von Mangoldt, *Zu Riemanns Abhandlung 'Über die Anzahl der Primzahlen unter einer gegebenen Grösse'*, Journal für die reine und angewandte Mathematik **114** (1895), 255–305.

[52] ———, *Zur Verteilung der Nullstellen der Riemannschen Funktion* $\xi(t)$, Mathematische Annalen **60** (1905), 1–19.