Dipartimento di Matematica

Corso di Laurea Triennale in Matematica

Tesi in Teoria dei Numeri

The Extended Riemann Hypothesis and its Consequences on Primality Tests

Relatore:
Prof.
Lars Halvard Halle

Presentata da:
Lorenzo Russi

Sessione Giugno 2025
Anno Accademico 2024/2025

Abstract

Questa tesi ha come scopo quello di fornire una introduzione al test di primalità probabilistico di Solovay-Strassen, che negli anni 60 è stato un punto di partenza fondamentale per gli algoritmi di primalità usati tutt'oggi, e studiarne la connessione con l'ipotesi estesa di Riemann. Il primo capitolo si concentrerà sul fornire al lettore alcuni strumenti fondamentali nello studio della teoria dei numeri, come i simboli di Legendre e i caratteri di Dirichlet. Questi ultimi verranno ripresi nel secondo capitolo, al fine di introdurre una definizione formale dell'ipotesi di Riemann e della sua generalizzazione che useremo per il resto della tesi. Il terzo capitolo si occuperà del test di primalità di Solovay-Strassen, mostrandone l'utilizzo e le limitazioni, e introdurrà le modifiche proposte per renderlo deterministico. Il quarto e ultimo capitolo dimostrerà che l'ipotesi estesa di Riemann rende deterministico la nuova versione del test, e stabilirà dei maggioranti per il numero di prove da eseguire.

Contents

Introduction

The Riemann Zeta function can be said to be, with no exaggeration, one of the most, if not the most, important functions in pure mathematics, and certainly the most studied one. The distribution of its zeroes is widely considered to be the greatest unsolved problem in math, with ramifications across many fields of study.
The function $\zeta(s)$ was originally defined over the real plane by Euler, who discovered that every negative even integer was a zero for it (these zeroes are called **trivial zeroes**). Later on, in a seminal 1859 article (the transcription of which you can find at [15]), the function's domain was extended to $\mathbb{C} \setminus \{1\}$ by Bernhard Riemann. Riemann had defined, in the very same article, another function $\pi(x)$, that allowed him to model the distribution of prime numbers over the real line. The use of $\pi(x)$ required calculating the zeroes of the Zeta function, which quickly became the subject of Riemann's interest.

Further work proved that every nontrivial zero could be found in $\{s \in \mathbb{C}, s : 0 \leq \mathrm{Re}(s) \leq 1\}$, often referred to as the **critical strip**. After calculating some of the first nontrivial zeroes, Riemann noticed a pattern in their distribution and came up with his famous hypothesis: that every nontrivial zero had $1/2$ as its real part. If the Riemann Hypothesis were to be conclusively proven to be true or false, it would have a profound impact on the world of math, particularly in the fields of number theory, cryptography, and complex analysis.
Despite numerous attempts, the problem remains unsolved to this day, and cracking it, or even making significant progress, would probably net you a Fields medal. Nevertheless, many brilliant mathematicians have taken their turn at expanding and building upon the original work, focusing, in particular, on the problem of generalizing the Riemann Hypothesis for entire classes of functions, similar to ζ. The two best known of such generalizations are the Generalized Riemann Hypothesis, which concerns itself with the class of Dirichlet L-functions, and the Extended Riemann Hypothesis, which was built upon Hecke L-functions.

This thesis will be focusing on the Extended Riemann Hypothesis, as it has some fascinating implications for the Solovay-Strassen primality test, which we are interested in. In 1977, Robert M. Solovay and Volker Strassen took inspiration from previous ideas of M.M. Artjuhov [3] to devise an algorithm able to discern if a number is composite or "probably prime" [17]. The Solovay-Strassen test is a probabilistic test, that is, a test which gives a result paired with the probability of that result being correct. In other words, it can give fairly accurate approximations but it can't

efficiently prove if a number is prime, only if it's not. This dissertation will focus on a modified deterministic version of the Solovay-Strassen test, and highlight why the Extended Riemann Hypothesis is required for it to work. Furthermore, it will examine an upper bound of $2\log^2 m$ for the minimum number of trials required to have a deterministic result. This upper bound was first computed by Eric Bach, albeit for different purposes [4].

The thesis will be organized as such: the first section will introduce the concept of Legendre and Jacobi Symbols, along with Dirichlet characters and their properties. The second section will discuss the Riemann Hypothesis itself, and introduce its two most commonly used generalizations. The third section will give an overview of the Solovay-Strassen test, with some example uses and observations on its limit, contrasting it with the proposed newer test. Lastly, the fourth section will introduce several results regarding nontrivial subgroups of $\mathbb{Z}/(m)^*$ under the assumption of ERH, compute the aforementioned upper bound, and prove that the new test is deterministic if the number of trials is higher than the bound. The main sources for this thesis are: an Eric Bach article based on his PhD work [4], the Keith Conrad paper on the Solovay-Strassen test [7], the Keith Conrad paper on the Miller-Rabin test [6], and the Pete L. Clark textbook on number theory [5].

1 Basic Concepts and Notation

This section aims to go over some basic definitions that are commonly used in number theory, along with specifying some quirks of the notation that will be used henceforth. Throughout this thesis, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$,and $\mathbb{C}$ will denote, respectively, the integers, the rational numbers, the real numbers, and the complex numbers. We'll use the notation $\mathbb{Z}^+$ to mean every non negative integer (including 0).
The reader might remember that, if $a = k + np$ for some integers k, p, n, then we define $a \mod p = k$. k is called a **residue** and, if $a \mod p = b \mod p$, we say that a and b are **congruent**.

1.1 Legendre and Jacobi Symbols

As a general reminder, $a \in \mathbb{Z}$ is said to be a **perfect square** if there exist $b \in \mathbb{Z}$ such that $b^2 = a$. Similarly, a is said to be a **perfect square modulo p** if there exist $b \in \mathbb{Z}$ such that $b^2 \mod p \equiv a$.

Definition 1.1 (Quadratic residue modulo p)**.**
Let a be a positive integer and let p be an odd prime. We say that a is a ***quadratic residue modulo*** *p if a is congruent to a perfect square modulo p.*

Keep in mind that a perfect square modulo p is not necessarily a perfect square.

Example 1.2.
For example, 3 *and* 5 *are not perfect squares, but they are perfect squares modulo* 11*, because* $3 = 5^2 \mod 11$ *and* $5 = 7^2 \mod 11 = 4^2 \mod 11$*.*

This example also shows that perfect squares modulo p can be the square of more than one integer.

Example 1.3.
The following table shows the residues for all a, $p \leq 15$, the bolded cells represent the quadratic residues.

a	a(mod 3)	a(mod 5)	a(mod 7)	a(mod 11)	a(mod 13)
2	2	2	**2**	2	2
3	**0**	3	3	**3**	3
4	**1**	**4**	**4**	**4**	**4**
5	2	**0**	5	**5**	5
6	**0**	**1**	6	6	6
7	**1**	2	**0**	7	7
8	2	3	**1**	8	8
9	**0**	**4**	**2**	**9**	**9**
10	**1**	**0**	3	10	**10**
11	2	**1**	**4**	**0**	11
12	**0**	2	5	**1**	12
13	**1**	3	6	2	**0**
14	2	**4**	**0**	**3**	**1**
15	3	**0**	**1**	**4**	2

As recounted by Gauss [10], Legendre was working on modular arithmetics towards the end of the 18th century, when he conjectured what became known as the law of quadratic reciprocity. While attempting to prove it, he brought forth his own notation, the so-called Legendre symbols. This particular notation proved to be quite appropriate not only for the problem at hand, but for the broader field, and was thus widely adopted.

Definition 1.4 (Legendre Symbols)**.**
Let a be positive integer and p be an odd prime, ***Legendre symbols*** *are functions with values in $\{0, 1, -1\}$ defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \mod p \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}.$$

To understand why Legendre symbols became commonplace notation in this field, let's take a look at some of their first uses. Consider this famous Euler result, which we won't prove:

Theorem 1.5 (Euler's Criterion)**.**
Let $p > 2$ be prime and a be an integer coprime to p. Then:

$$a^{(p-1)/2} \equiv \begin{cases} 1 \mod p & \text{if there is an integer } k \text{ such that } k^2 \equiv a \mod p \\ -1 \mod p & \text{otherwise} \end{cases}.$$

This theorem is extremely useful because it gives us a way to verify whether an integer a is a quadratic residue modulo p. However, this formulation is a bit clunky, as the condition to be examined is not clear at a first glance. But thanks to Legendre symbols, we can express the previous theorem in a more compact and elegant manner:

Theorem 1.6 (Criterion with Legendre symbols)**.**
Let $p > 2$ be prime and a be an integer coprime to p. Then:

$$\left(\frac{a}{p}\right) \equiv a^{(n-1)/2} \mod p.$$

For similar reasons the law of quadratic reciprocity is most commonly expressed through Legendre symbols. In this thesis we won't provide a proof for it, but it's interesting to note that the earliest known one is found in Gauss's Disqvisitiones arithmeticae [9]. This shows how, at the dawn of the 19th century, number theory, and more specifically the study of number fields, had a central role in math discussions.

Theorem 1.7 (Law of quadratic reciprocity)**.**
Let p, q be distinct odd primes, then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

As useful as Legendre symbols are, they can only be properly defined under a strict condition: that p has to be prime! Unfortunately, in the context of prime testing, the primality of p is impossible to assure (after all, that's what we are testing for). Therefore, in this thesis, we'll be using a generalization by Jacobi [12], which does not have such a restriction. For the next definition, $\left(\frac{a}{p_i}\right)^{a_i}$ is to be interpreted as the standard Legendre Symbol

Definition 1.8 (Jacobi Symbols)**.**
Let a and n be positive integers and $n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ be the prime factorization of n. Then we define the ***Jacobi Symbol*** *as:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1}\left(\frac{a}{p_2}\right)^{a_2}\dots\left(\frac{a}{p_n}\right)^{a_n}.$$

It's easy to verify that, if n is prime, the previous definition is equivalent to the standard Legendre symbol. Legendre and Jacobi symbols aren't completely interchangeable, but they do share many common properties. In this thesis we'll refer to the following 5:

1. $a \equiv b \mod n \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$,
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$,
3. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$,
4. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$,
5. $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)(-1)^{((m-1)/2)*((n-1)/2)}$.

1.2 Notation and Auxiliary Functions

We'll start this subsection with the introduction of some of the notation. In general, K will indicate an algebraic number field with degree n, and r_1, r_2 will denote its embedding in $\mathbb{R}$, and half of its embedding in $\mathbb{C}$, respectively (so that n=$r_1 + 2r_2$). The symbol Δ will denote the absolute value of K's discriminant.
We'll use the letter O for the ring of integers of K, and U to indicate an ideal of O. For each nonzero ideal U, NU is to be interpreted as the order of the quotient ring O/U, that is, the number of cosets in O/U. Moreover, we'll make use of some important auxiliary functions for the purpose of computation. Henceforth $\Lambda(n)$ will denote a function equal to $\log p$ if n can be expressed as a power of a certain prime p, and 0 otherwise. The Gamma function Γ is the most widely used extension of the factorial function on $\mathbb{C}$ and was first derived by Bernoulli in the 18th century.

Definition 1.9 (Gamma function)**.** *Let $z \in \mathbb{C}$ be such that $\mathrm{Re}(z) > 0$, the **gamma function** is defined as the analytic continuation of the following integral:*

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}.$$

Exactly as we expect, we have that the Gamma function follows the same recursive property of the standard factorial: for all positive integers z, $\Gamma(z) = (z-1)!$. Lastly, this thesis will use the Digamma function (also known as the psi function):

Definition 1.10 (Digamma function)**.**
*We define the **digamma function** ψ as the logarithmic derivative of the Gamma function:*

$$\psi(z) = \frac{\Gamma'}{\Gamma}(z).$$

The function ψ has several remarkable properties [2]. We'll use some of the following:

1. ψ follows the recurrence relation $\psi(z) = \psi(z+1) - 1/z$,
2. ψ satisfies the duplication formula $\psi(z/2) + \psi((z+1)/2) = 2(\psi(z) - \log 2)$,
3. Over the range $(0, \infty)$, ψ has derivatives that alternate in sign. Thus ψ is increasing, ψ' is decreasing, and in general all derivatives are monotone,
4. As a consequence of the first property, the first derivative of ψ follows the relation $\psi'(z) = \psi'(z+1) + 1/z^2$.

In anticipation of the functions we'll be using later on, let's refresh our memory on some specific function classes. For most of this section, we'll mostly be using the definitions provided in chapter 16 of Pete Clark's "Number Theory: A Contemporary Introduction" [5]. As a reminder, an **arithmetic** function is a function whose domain is $\mathbb{Z}$ and whose range is included in $\mathbb{C}$.

Definition 1.11 (Completely multiplicative function)**.**
*Let $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ be an arithmetic function, f is said to be **completely multiplicative** if $f(1) \neq 0$ and for all $a, b \in \mathbb{Z}$, $f(ab) = f(a)f(b)$.*

Definition 1.12 (Periodic function)**.**
*For $N \in \mathbb{Z}^+$, a function is called N-**periodic** if for all $n \in \mathbb{Z}^+$, $f(n+N) = f(n)$. An arithmetic function is **periodic** if it's N-periodic for some $N \in \mathbb{Z}^+$.*

Most people will be familiar with periodicity in the context of sine and cosine. However, while those functions are often referred to as periodic, going by the above definition, they aren't, since their period is 2π which is not an integer. So let's examine what some of our periodic functions actually look like:

Example 1.13.
The parity function is defined as:

$$f(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}.$$

In this case, $f(n)$ is 2-periodic, as n always has the same parity as $n+2$. Moreover, $f(n)$ is also completely multiplicative, since the product of two even numbers is still even and the product of two odd numbers is still odd.

Example 1.14.
*The **sawtooth wave** is a periodic function:*

$$x(t) = 2\left(\frac{t}{p} - \left\lfloor \frac{1}{2} + \frac{t}{p} \right\rfloor\right).$$

Given p, we have that

$$x(t+p) = 2\left(\frac{t+p}{p} - \left\lfloor \frac{1}{2} + \frac{t+p}{p} \right\rfloor\right) = 2\left(\frac{t}{p} + 1 - \left\lfloor \frac{1}{2} + \frac{t}{p} \right\rfloor - 1\right) = x(t).$$

This function is therefore p-periodic!

Counterintuitively, a function can have more than one period. An intriguing example of this is :

Example 1.15.
This is the famous Dirichlet function, a very poorly behaved function often used in textbook counterexamples:

$$\mathbf{1}_{\mathbb{Q}}(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \notin \mathbb{Q} \end{cases}.$$

It just so happens that for any $y \in \mathbb{Z}$, $\mathbf{1}_{\mathbb{Q}}(x+y) = \mathbf{1}_{\mathbb{Q}}(x)$, and thus the function can be said to be y-periodic.

1.3 Dirichlet Characters

As we saw with the parity example, being periodic and being completely multiplicative are not mutually exclusive properties! In fact, during this dissertation, we'll be mostly discussing functions that belong to both classes. As a lot of the groundwork regarding them was done by Dirichlet, these special functions take after his name:

Definition 1.16 (Dirichlet character)**.**
A N-periodic arithmetic function χ that is also completely multiplicative is called a ***Dirichlet character*** *of modulus N. The character $\chi_1 = 1$ is referred to as the* ***trivial*** *Dirichlet character. Every other χ is said to be* ***nontrivial****.*

Example 1.17 (Principal character)**.**
The simplest possible nontrivial Dirichlet Character is called the ***principal character*** *and exists for all moduli m:*

$$\chi_0(a) = \begin{cases} 0 & \text{if } gcd(a,m)>1 \\ 1 & \text{if } gcd(a,m)=1 \end{cases}.$$

It's not always easy to imagine what a nontrivial nonprincipal Dirichlet character looks like from the definition alone. Luckily, we have already introduced one such function previously: the Legendre symbol.

Proposition 1.18 (Legendre Symbols are characters)**.**
For any odd prime p, the transformation that associates the Legendre symbol to a number n, $L_p : \mathbb{Z}^+ \longrightarrow \mathbb{C}$, defined as $L_p(n) = \left(\frac{n}{p}\right)$, is a nonprincipal nontrivial Dirichlet character of modulus p.
Proof
For any n, $m \in \mathbb{Z}$, we can use the second property of 1.4 to infer that

$$L_p(nm) = \left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = L_p(n)L_p(m),$$

which proves that $L_p(n)$ is indeed completely multiplicative.
Furthermore, by definition $L_p(n + p) = L_p(n)$ and thus $L_p(n)$ is also p-periodic. Lastly, we notice that $L_p(n) = 0$ if and only if $gcd(n, p) > 1$. However, since the image of Legendre symbols includes -1, we know for a fact that L_p is a distinct character from χ_0 and is thus nonprincipal (and obviously also nontrivial). □

1.4 Conductors and Primitive Characters

In discussing the subject of Dirichlet characters, one more distinction is needed: whether a character is primitive or not. To explain what that means, we introduce the concept of quasiperiod:

Definition 1.19 (Quasiperiod and Conductors)**.**
Let χ be a Dirichlet Character of modulus k, we say that χ has a ***quasiperiod*** *of d if $\chi(m) = \chi(n)$ for all m, n coprime to k such that $m \equiv n \mod d$. The smallest possible integer for which χ is quasiperiodic is called the* ***conductor*** *of χ.*

As a reminder, if we take $K = \mathbb{Q}$ as the number field and $\mathbb{Z}$ as the ring of integers, every ideal will be generated by an integer r, and denoted with (r), in which case we have $Nr = r$, where Nr is to once again be interpreted as the size of the quotient ring $\mathbb{Z}/(r)$. Recalling that Δ indicates the absolute value of the discriminant of K, if χ a primitive character with conductor r, we'll thus use the notation $A_\chi = Nr\Delta = r\Delta$.

Example 1.20. *Let's consider the principal character of modulus 2:*

$$\chi_{0,2}(a) = \begin{cases} 0 & \text{if } a \text{ is even} \\ 1 & \text{if } a \text{ is odd.} \end{cases}.$$

When considering the integers modulo 2, 1 is the only odd number, and thus $\chi_{0,2}(a)$ trivially has a quasiperiod of 1, which is also the conductor. However, note that the period of $\chi_{0,2}(a)$ is actually 2!

Example 1.21. *Consider instead the following characters of modulus 16:*

$$\chi_{16,3}(a) = \begin{cases} 1 & \text{if a=1 mod 16 or a=7 mod 16} \\ -i & \text{if a=3 mod 16 or a=5 mod 16.} \\ i & \text{if a=11 mod 16 or a=13 mod 16.} \\ -1 & \text{if a=9 mod 16 or a=5 mod 15.} \\ 0 & \text{otherwise} \end{cases},$$

and

$$\chi_{16,9}(a) = \begin{cases} 1 & \textit{if a=k mod 16 with k in \{1,7,9,15\}} \\ -1 & \textit{if a=k mod 16 with k in \{3,5,11,13\}} \\ 0 & \textit{otherwise} \end{cases}.$$

We find out that the conductor of $\chi_{16,3}$ is 16, and so is its period, while the conductor of $\chi_{16,9}$ is 8.

Definition 1.22 (Primitive Characters)**.**
A character χ of modulus m is said to be ***primitive*** *if its conductor is equal to m. Otherwise, it is said to be* ***imprimitive*** *[8].*

Example 1.23.
As we saw above, $\chi_{0,2}$ is imprimitive because it has a quasiperiod lower than 2,and so is $\chi_{16,9}$, since it has a quasiperiod lower than 16. However, $\chi_{16,3}$'s conductor is indeed the same as its period and thus $\chi_{16,3}$ is a primitive character.

Lastly, we'll use the letter β to measure how much a character "depends on signs". To understand what that means, first consider that if $\chi(m)$ is a character with conductor f, there exists numbers $a_1 \in \{0, 1\}$, with $1 \leq i \leq r_1$, such that for any $n \equiv 1 \mod f, \chi(m) = \prod(sign\ m_i)^{a_i}$. We define β as the number of 1's that are present in the list a_1,a_2, ..., a_{r_1} and α as $r_1 - \beta$. By construction, we have that $0 \leq \alpha$, $\beta \leq n$. That being said, most of the results of this thesis are pertinent to $\mathbb{Q}$, which greatly simplify our work. In fact, in that number field, we have that $r_1 = 1$, $\beta = 0$, and thus $\alpha = 1$. To understand why Dirichlet characters are so important to the subject of this thesis we need to familiarize ourselves with the Riemann Hypothesis. The next section will discuss a formal definition of it, along with some of the its generalizations.

2 Dirichlet series and generalizations of RH

As this thesis revolves around the Extended Riemann hypothesis it's necessary to introduce some of the concepts upon which the hypothesis is built. We'll start by reintroducing the Riemann Zeta function as a special case of a generic Dirichlet Series. We'll then follow it with the introduction of the standard Riemann Hypothesis and its first generalization; the aptly named Generalized Riemann Hypothesis. This will serve as a contrast for the second part of the section, following the same structure, but providing a different way of generalizing RH, involving Hecke L-functions. The final section contains a formal definition of the Extended Riemann Hypothesis, which will be the one used in the rest of this thesis.

2.1 The Standard Riemann Hypothesis and the Generalized Riemann Hypothesis

Definition 2.1 (Dirichlet series)**.**
Let $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ be an aritmetic function and let $s \in \mathbb{C}$. We define the ***Dirichlet series*** *of f as:*

$$D(f, s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Dirichlet series are of fundamental importance in number theory, providing a crucial analytic interpretation of certain problems. Most notably, the Riemann Zeta function is, in fact, a special case of a Dirichlet series:

Definition 2.2 (Riemann Zeta function)**.**
The Riemann Zeta function is the Dirichlet series of the constant unit function. In other words, let $s \in \mathbb{C} \setminus \{1\}$ and let $u(n) = 1$ for every n, we define $\zeta_R(s) : \mathbb{C} \longrightarrow \mathbb{C}$ as:

$$\zeta_R(s) = \sum_{n=1}^{\infty} \frac{u(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The line of $\{s \in \mathbb{C} \setminus \{1\} : \mathrm{Re}(s) = 1/2\}$ is called **the critical line**. During his work, Riemann started suspecting this to be the line where all nontrivial zeroes resided, and thus formulated:

Conjecture 2.3 (Riemann Hypothesis)**.**
Let $s \in \mathbb{C} \setminus \{1\}$ be a nontrivial zero of ζ, then $\mathrm{Re}(s) = \frac{1}{2}$.

As we've discussed, the Riemann Zeta function can be seen as a particular case of a Dirichlet series. Could Dirichlet series based on other functions also share the same properties? And what kind of functions would even produce interesting results? Well, it just so happens that the function $u(n)$ is actually the trivial Dirichlet character χ_0! It thus becomes worthwhile to study what happens to other characters when they are transformed into Dirichlet series. The character's particular properties make them uniquely suitable for a specific transformation:

Definition 2.4 (Dirichlet L-Series)**.**
A ***Dirichlet L-series*** *is the Dirichlet series associated to a Dirichlet character:*

$$L_D(\chi, s) = D(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

These L-Series are a great generalization for functions that behave somewhat similarly to the Riemann Zeta function. The question of where their zeroes lie thus becomes relevant when discussing the original RH. In 1884, this realization led Adolf Plitz to first formulate the Generalized Riemann Hypothesis [14]; an extension of Riemann's standard conjecture:

Conjecture 2.5 (GRH)**.**
For every Dirichlet character χ and for every $s \in \mathbb{C}$, such that $L_D(\chi, s) = 0$, if s is not a real negative number then $\mathrm{Re}(s) = 1/2$.

Note that choosing the trivial Dirichlet Character $\chi_0 = 1$ yields the ordinary Riemann hypothesis. The Generalized Riemann Hypothesis is a powerful result that already allows us to find the bounds for the specific case of K=$\mathbb{Q}$. However, as this thesis will establish several results that are generally true for all number fields, we need a even more general result.

2.2 Hecke L-functions and the Extended Riemann Hypothesis

The Dirichlet L-series are not the only possible transformations that are compatible with Dirichlet characters! The one we'll mostly use during this thesis is actually the following:

Definition 2.6 (Hecke L-function)**.**
A ***Hecke L-function*** *associated with a character χ is:*

$$L(s, \chi) = \sum_U \frac{\chi(U)}{(NU)^s}.$$

We can then derive the equivalent of the Riemann Zeta function by choosing the trivial character once again:

Example 2.7 (Dedekind Zeta function)**.**
The ***Dedekind Zeta function*** *of K is the special case in which we take the Hecke L-function associated with the trivial character $\chi = 0$:*

$$\zeta(s) = \sum_U \frac{1}{(NU)^s}.$$

In general, Hecke L-functions are analytic on the whole plane, except for the ones associated with principal characters, which have a simple pole at s=1. They also have infinitely many zeroes in the critical strip as well as extra zeroes at specific non negative integers. We'll use the notation ρ to indicate the zeroes that lie in the critical strip. This leads us to yet another possible generalization of RH, the Extended Riemann hypothesis:

Conjecture 2.8 (ERH)**.**
If s is a nontrivial zero of ζ, then $\mathrm{Re}(s) = \frac{1}{2}$.

Note that the ordinary Riemann Hypothesis follows from ERH if we take $K = \mathbb{Q}$ as the number field, and $O = \mathbb{Z}$ as the ring of ideals. Due to the way we defined the Dedekind Zeta function, ERH is a conjecture compatible with a generic field K, unlike GRH. This is the reason we chose to use ERH over GRH.

2.3 Properties of the Dedekind Zeta function and Hecke L-functions in general

Before we start using ERH, let's take a look at some properties of the functions we discussed so far. We begin with some absolutely convergent representations of their logarithmic derivatives in the half plane $\mathrm{Re}(s) > 1$:

$$\frac{\zeta'}{\zeta}(s) = -\sum_U \frac{\Lambda(U)}{(NU)^s}$$

and

$$\frac{L^{'}}{L}(s) = -\sum_{U} \frac{\Lambda(U)\chi(U)}{(NU)^{s}}$$

.
As before, $\Lambda(U) = \log Np$ if U is a power of a prime ideal p, and 0 otherwise.
We'll also use the notation

$$\psi_{\zeta}(s) = \frac{r_1 + r_2}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2}{2}\psi\left(\frac{s+1}{2}\right) - \frac{nlog\pi}{2}$$

,

$$\psi_{L}(s) = \frac{r_2 + \alpha}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta}{2}\psi\left(\frac{s+1}{2}\right) - \frac{nlog\pi}{2}.$$

With this in mind, for any s we have that:

$$\frac{\zeta^{'}}{\zeta}(s) = B + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log\Delta - \frac{1}{s} - \frac{1}{s-1} - \psi_{\zeta}(s).$$

Moreover, if we choose χ to be a generic primitive nonprincipal character, we can also generalize it into:

$$\frac{L^{'}}{L}(s) = B_{\chi} + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log A_{\chi} - \psi_{L}(s).$$

You can find the proof of the latter on page 433 of [13]. Note that due to the structures of ζ and L, taking the sum in a symmetric order will result in having $B + \sum \rho^{-}1 = B_{\chi} + \sum \rho^{-1} = 0$. Therefore there's no need for a specific estimation of B or B_{χ}.
Having familiarized ourselves with ERH, it's now time to discuss primality tests, specifically the one that this thesis is discussing: The Solovay-Strassen primality test.

3 Euler Witnesses and Solovay-Strassen

In the first section we had introduced the famous Euler Criterion while discussing some uses for Legendre symbols. Following that, we highlighted one of their main limitations, that being the requirement for p to be prime, and argued in favour of using Jacobi's symbols instead. However, we have never considered if the criterion was one of the properties that the two types of symbols shared.

3.1 A first look at the test

It turns out that Euler's formula doesn't hold if we generalize p to be composite. This might seem disappointing, but it's actually the key fact that was used by Solovay and Strassen to develop their 5 steps test, which is done as follows:

Let n be the number whose primality we are interested in finding out.

1. Choose a number $t \geq 1$ to be the number of trials to be done during the test.
2. Randomly select t integers ranging from 2 to $n-2$.
3. For each randomly selected integer, check the Euler Criterion (this is called a trial).
4. If the Euler Criterion does not hold for at least one integer thus chosen, the test confirms that n is composite.
5. Otherwise the test gives us the following result: "n is prime with probability P".

We'll discuss the various values that P can take later. For now, let's focus on step 4: on what basis does that passage hold? As discussed before, the criterion doesn't hold for nonprime p, and more specifically, for odd composite numbers, the congruence tends to have a lot of counterexamples. We call those counterexamples Euler Witnesses and we define them more formally as follows:

Definition 3.1 (Euler Witnesses)**.**
Let $n > 1$ be an odd integer and let a be such that $1 < a < n-1$.
*We say that a is a **Euler Witness** if either of the following conditions hold:*

1. $gcd(a, n) > 1$,

2. $gcd(a, n) = 1$ *and* $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$.

We say that a is a ***Euler Nonwitness*** *otherwise.*

Observe that calculating $\left(\frac{a}{n}\right)$ is enough to check for both conditions at the same time, as the first condition is equivalent to $\left(\frac{a}{n}\right) = 0$, due to the properties we discussed in section one.

Example 3.2.
Let n=8073, we quickly find out that $2^{4036} \mod 8037 = 2473 \neq \pm 1$.
Thus 2 is a Euler Witness for 8073 and we can conclude that 8073 is composite.

Note that 2 is **not** a factor of 8073, proving that the test does not give any information on the factorization of the number, only on its primality.

Example 3.3.
Let n=2011

a	$a^{(2010)/2}$ *(mod 2011)*	$\left(\frac{a}{2011}\right)$
2	*-1*	*-1*
3	*-1*	*-1*
4	*1*	*1*
5	*1*	*1*
6	*1*	*1*

We have not found any Euler Witness, giving us a certain degree of confidence in the primality of 2011 (Which is indeed prime). However, with no further information,we would still have to check every a up to $\sqrt{2011}$ *to be absolutely certain.*

Euler's criterion only assures us that finding an Euler witness for n confirms that n is not prime, but seemingly says nothing about situations where we don't find any witnesses. That's where Solovay and Strassen come in! By retracing the steps the pair originally took, in their groundbreaking 1977 article [17], we arrive at a very powerful result: that every composite integer MUST have at least one Euler witness.

Theorem 3.4 (Solovay-Strassen)**.**
Let n be an odd composite positive integer. Then there exists an integer a such that $1 < a < n-1$, $gcd(a,n) = 1$, and $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$.

Proof
We'll divide the proof in two cases, depending on whether or not n has a repeated prime factor:
1) If n does not have a repeated prime factor then $n = p_1 p_2 \dots p_k$ with $k > 2$ and $p_1 \dots p_k$ distinct odd primes. Considering p_1, it is always possible to find a integer b that is not a square modulo p_1. Therefore there's always at least one $b \in \mathbb{Z}$ such that $\left(\frac{b}{p_1}\right) = -1$. By the Chinese Remainder Theorem, this implies that, for each i in {2,. . . ,n-1}, there exists an $a \in$ {2,. . . ,n-1} such that

$$a \equiv b \mod p_1 \text{ and } a \equiv 1 \mod p_i$$

. Note that a is such that $gcd(a,n) = 1$ and

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) = -1 \cdot 1 \cdot \dots \cdot 1 = -1, \text{ since } \left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$$

. Moreover, since $b \not\equiv 1 \mod p_1$, it follows that $a \neq 1$. Suppose $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \mod n$, then we would have that $a^{(n-1)/2} = -1 \mod n$.
Due to the fact that p_2 divides n, we can reduce the equation to modulo p_2, keeping in mind that by definition $a^{(n-1)/2} = 1 \mod p_2$, to obtain that $1 = -1 \mod p_2$. This is a contradiction since p_2 is a odd prime and thus $p_2 > 2$. From this we can conclude that a is such that $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$ and $gcd(a,n) = 1$, and thus a is a Euler Witness.
2) If n has a repeated prime factor, for example p, then we can write n as $n = p^k m$ with $k \geq 2$ and $gcd(p,m) = 1$. By the chinese remainder theorem there exists an $a \in \{1, \dots, n-1\}$ such that

$$a \equiv (1+p) \mod p^2 \text{ and } a \equiv 1 \mod m$$

.
Note that $a \equiv 1 \mod m$ implies that $a \neq 1$. Once again we suppose that $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \mod n$ holds and we square both sides, thus obtaining that $1 \equiv a^{(n-1)}$

mod n. *Since* p^2 *divides* n *we can reduce the equation modulo* p^2*:* $1 \equiv a^{(n-1)} \mod p^2$. *But* $a \equiv (1+p) \mod p^2$ *and thus* $1 \equiv (1+p)^{(n-1)} \mod p^2$. *The binomial theorem tells us that*

$$(1+p)^{(n-1)} = 1 + (n-1)p \mod p^2 \text{ and thus } 1 + (n-1)p = 1 \mod p^2.$$

This implies that $(n-1)p = 0 \mod p^2$ *and therefore* $(n-1) = 0 \mod p$ *. Since* p *divides* n *by construction,* p *can't divide n-1, so we have a contradiction.*
It must then be that a *is such that* $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$ *and* $gcd(a,n) = 1$*, and thus* a *is a Euler Witness.*

□

The obvious corollary is that a number without witnesses is prime. This theorem is the basis upon which the Solovay-Strassen test is built! Together with the original criterion, it highlights a 1 to 1 correspondence between primes and numbers without witnesses. This means that checking for Euler witnesses for an integer n is indeed equivalent to checking its primality.

3.2 What does it mean to be a probabilistic primality test?

Having now established that the test does indeed work, we are now presented with the issue of efficacy. When thinking about that a question comes to mind: "How many of such witnesses are there? And how are they distributed?".
If it were the case that the witnesses are rare and far apart, then the test, while still technically accurate, would be computationally inefficient, as you'd have to check a vast quantity of numbers. Luckily for us, the next result tells us that these witnesses are rather abundant! In this thesis, if A is a set, $|A|$ will denote its cardinality.

Theorem 3.5 (Ratio of Euler Witnesses)**.**
Let $n > 1$ *be an odd composite number. Then:*

$$\frac{\left|1 \leq a \leq n-1 : (a,n) = 1 \text{ and } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \mod n\right|}{n-1} < \frac{1}{2}.$$

In other words, given n*, more than 50% of the numbers in* $\{1, 2, \ldots, n-1\}$ *are Euler Witnesses.*

Proof
We divide the numbers between 1 and n-1 in three disjoint non empty sets as follows: Let $1 \leq a \leq n-1$,

$$\begin{aligned} A = \{a : (a,n) = 1 \text{ and } \left(\frac{a}{n}\right) &\equiv a^{(n-1)/2} \mod n\} \\ &= \{a : a \text{ is Euler Nonwitness}\}, \\ B = \{a : (a,n) = 1 \text{ and } \left(\frac{a}{n}\right) &\not\equiv a^{(n-1)/2} \mod n\} \\ &= \{a : a \text{ is Euler Witness with gcd(a,n)=1}\}, \end{aligned}$$

$$C = \{a : (a,n) > 1\} = \{a : a \text{ is not relatively prime to } n\}.$$

Since n is composite, C is nonempty. Moreover, due to the previous theorem, B is also nonempty. Finally, we notice that A contains 1 and n-1. What we are trying to prove is equivalent to proving that $|A| < (n-1)/2$. *Let* b_0 *be a number in B, and consider the set* $Ab_0 = \{ab_0 \mod n : a \in A\}$. *Our goal will be to prove that* Ab_0 *is actually a subset of B.*
We do this by observing that ab_0 *is relatively prime to n and that:*

$$(ab_0)^{(n-1)/2} = a^{(n-1)/2} b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \mod n.$$

By construction, $gcd(ab_0, n) = 1$. *If it were that* $ab_0 \mod n \in A$ *then we would have that:*

$$(ab_0)^{(n-1)/2} \equiv \left(\frac{ab_0}{n}\right) \mod n \equiv \left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \mod n.$$

So it would follow from the previous equations:

$$\left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \mod n \equiv (ab_0)^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \mod n.$$

Furthermore $gcd(a,n) = 1$ *implies that* $\left(\frac{a}{n}\right) = \pm 1$, *allowing us to cancel the* $\left(\frac{a}{n}\right)$ *on both sides, to obtain that* $\left(\frac{b_0}{n}\right) \mod n \equiv (ab_0)^{(n-1)/2}$ *and therefore* $b_0 \in A$.
We arrive at a contradiction, since we chose b_0 *in B, which is disjoint from A. It*

must then be that, for any given $b_0 \in B$, $ab_0 \in B$, which implies $Ab_0 \subset B$, which is what we originally wanted to prove. The number of elements in Ab_0 is $|A|$, which implies that $|A| = |Ab_0| \leq |B|$. Therefore:

$$n-1 = |A|+|B|+|C| \geq |A|+|A|+1 = 2|A|+1 > 2|A|\text{, and thus } |A| < (n-1)/2.$$

□

Now that we have shown that the test is both accurate and somewhat efficient, it's time to discuss what results we get from it. We are specifically interested in elaborating on what exactly the statement "n is prime with probability P" means. After all, as previously discussed, with a sufficiently large amount of trials ($t > n/2$), we are able to know whether n is prime or not with absolute certainty. As we'll see later on with some explicit calculations, the problem is that that amount of trials is so computationally expensive, relative to even the most naive of prime tests, to not be worth it. However, this is where the Solovay-Strassen test shines, as knowing that a number is "almost certaintly" prime is good enough for a variety of uses. In other words, there is a delicate game being played here: to find the lowest t such that the probability $P(t)$ of n being prime is acceptable. The problem of calculating the precise value of P(t) is a complex one, but a good estimation by K. Conrad [7] (p. 10) gives us the result of $P(t) > 1 - \frac{\log n}{2^t}$, with an appropriate choice of $2^t > \log n$. Let's use this to see how the probability changes as the number of trials rises:

Example 3.6. *For example, let $n = 75913$. A test run with $t = 10$ yields $P = 98.9\%$, as shown below:*

a	$a^{(75912)/2} \mod 75913$	$\left(\frac{a}{75913}\right)$
2	*1*	*1*
3	*1*	*1*
4	*1*	*1*
5	*-1*	*-1*
6	*1*	*1*
7	*-1*	*-1*
8	*1*	*1*
9	*1*	*1*
10	*-1*	*-1*

If we further evaluate up to $t = 15$, we will get $P = 99,96\%$:

a	$a^{(75912)/2} \mod 75913$	$\left(\frac{a}{75913}\right)$
11	*-1*	*-1*
12	*1*	*1*
13	*-1*	*-1*
14	*-1*	*-1*
15	*-1*	*-1*

This approximation of P gives us a strong degree of certainty in the results of the test, especially with the choice of a large t, but it is by no means perfect. Due to us not knowing the precise distribution of Euler Witnesses, only checking at least half of the numbers from 1 to n would guarantee that the result is accurate.
As an example of how inefficient that would be, let's compare it to the most naive form of primality testing, checking whether or not every number up to $\sqrt{n}$ is a divisor of n:

Example 3.7. *Referring to the previous example, if we wanted to use Solovay-Strassen to be completely sure that 75913 is prime, we'd need 37957 trials. The naive prime testing would only require 276 divisions.*

3.3 Proposing a Deterministic Alternative

This limitation means that, in the current form, the Solovay-Strassen test can only be a **probabilistic** primality test. Luckily for us, an important result in this field was since proven [7] (p. 6):

Theorem 3.8 (Deterministic version of the test)**.** *[ERH]*
Assuming the truth of the Extended Riemann Hypothesis, the Solovay-Strassen test becomes a ***deterministic*** *primality test, under the condition $t > C \log^2 n$ for some constant C, and a slight modification in the integer selection process.*

More specifically, the new version of the test doesn't require random selection, but will instead use with integers from 2 to t in order. This makes the test not only deterministic but also efficient since it would mean that it runs in polynomial time. An excellent upper bound of $C < 2$ follows from the work of Eric Bach in his 1985

Ph.D. thesis, part of which later was incorporated in an article that can be found here [4]. How does this upper bound affect our computations?

Example 3.9.
This theorem tells us that, assuming the truth of ERH, in the $n = 75913$ *example we would only need to check integers up to* $2\log^2(75913) \approx 253$ *to be sure of its primality.*

The significance of this bound might not be immediately apparent to the reader: after all, with only 15 trials, we had already obtained a 99% accurate result! In these cases, it would do us well to remember that probabilistic tests, while incredibly useful in some fields, can't be used in rigorous math, which requires results that are certain. Moreover, while computing up to $t = 253$ is a cumbersome and time-consuming task for a human, it poses little challenge to a modern computer. And, while in the example given the naive method seems to be at least somewhat competitive, it has a cost of $O(\sqrt{n})$, scaling up significantly faster than $O(2\log^2 n)$ as n becomes larger and larger. But why do we even need ERH in the first place? The relation between the Riemann Hypothesis, its generalizations, and this result, is absolutely not obvious at a first glance. With this next section, we aim to clarify that connection and make some of the rather hostile passages more approachable.

4 In Search of a Bound

As mentioned in previous sections, we are aiming to find the smallest possible x such that any $t > x$, where t is the number of trials to be done, makes the test deterministic. We'll start off this section with some seemingly unrelated estimates, in the forms of lemmas. This will mostly be calculations, but it's important to remember that the even marginal improvements to the bounds, such as the ones we are about to establish, make a world of difference. This section is heavily based on Eric Bach's work [4] and, as such, each result will be labeled with the respective number in that paper, making cross referencing easier for the reader.

4.1 Some Necessary Approximations

We'll being this subsection by taking one of the fundamental results in the paper and examining the more specific case of $K = \mathbb{Q}$. For this section, we'll use the notation:

$$I_0 = (\beta - 1)\frac{1}{a^2} + \frac{\log x}{x^a}\left(\frac{\zeta^{'}}{\zeta} - \frac{L^{'}}{L}\right)(-a) + \frac{1}{x^a}\left(\frac{\zeta^{'}}{\zeta} - \frac{L^{'}}{L}\right)^{'}(-a) - \beta\frac{1}{x(a-1)^2},$$

and

$$I_- = \beta\sum_{k=2}^{\infty}\frac{(-1)^k}{(a-k)^2x^k}.$$

With that in mind:

Lemma 4.1 (4.4)**.**
Let χ be a nonprincipal primitive character. and let n be a positive integer. Then, if $0 < a < 1$:

$$\frac{x}{(a+1)^2} = \sum_{\rho}\frac{x^\rho}{(\rho+a)^2} + I_0 + I_-,$$

where the $\pm$ sign is to be interpreted as + for the roots of $\zeta(s)$ and - for the roots of $L(s,\chi)$.
Proof
This can be proved in a similar manner to Theorem 28 in [11], using estimates for $\frac{L^{'}}{L}$ that can be found in (5.6),(6.2) and (6.3) of [13]. □

To get an actual upper bound on x, we need to get some further estimates on the maximum value of the right side. These estimates are generally true even for number fields that are not $\mathbb{Q}$. We'll start with I_-:

Lemma 4.2 (5.1)**.**
Let I_- be defined like in the previous lemma. Then:

$$I_- \leq \frac{\beta}{(a-2)^2 x^2} = O(n).$$

Proof
As k, $x \geq 1$ and $0 < a < 1$, it follows that $(a-(k+1))^2 > (a-k)^2$, which implies

$$x^{k+1}(a-(k+1))^2 > x^k(a-(k+1))^2 > x^k(a-k)^2.$$

Thus if we take the reciprocals of both sides of the previous equation we get:

$$\frac{1}{x^{k+1}(a-(k+1))^2} < \frac{1}{x^k(a-k)^2}.$$

In other words for $i \geq 1$, each pair of consecutive numbers in the sum is such that

$$\frac{1}{x^{2i+2}(a-(2i+2))^2} - \frac{1}{x^{2i+1}(a-(2i+1))^2} \leq 0.$$

We can then split the sum as:

$$\begin{aligned}\beta \sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2 x^k} &= \frac{\beta}{(a-2)^2 x^2} + \sum_{i=1}^{\infty} \frac{1}{x^{2i+2}(a-(2i+2))^2} - \frac{1}{x^{2i+1}(a-(2i+1))^2} \\ &\leq \frac{\beta}{(a-2)^2 x^2}.\end{aligned}$$

□

The task of estimating I_0 proves to be slightly more difficult. We'll express I_0 as a sum and then estimate each part of it. The next result follows from the properties we discussed for the logarithmic derivatives of ζ and L, and won't be proven:

Lemma 4.3 (5.2)**.**
Let χ be a primitive character. Then, with the usual convention that $\pm$ is to be interpreted as + for roots of ζ and as - for roots of $L(s,\chi)$, the following representations are valid for all s:

$$\left(\frac{\zeta^{'}}{\zeta}-\frac{L^{'}}{L}\right)(s)=\sum_{\rho}\pm\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)-\frac{1}{s}-\frac{1}{s-1}-$$

$$-\frac{\beta}{2}\left[\psi\left(\frac{s}{2}\right)-\psi\left(\frac{s+1}{2}\right)-\psi(1)+\psi\left(\frac{3}{2}\right)\right]+\left(\frac{\zeta^{'}}{\zeta}-\frac{L^{'}}{L}\right)(2)+\frac{3}{2}.$$

and

$$\left(\frac{\zeta^{'}}{\zeta}-\frac{L^{'}}{L}\right)^{'}(s)=\sum_{\rho}\mp\frac{1}{(s-\rho)^2}+\frac{1}{s^2}+\frac{1}{(s-1)^2}-\frac{\beta}{4}\left[\psi^{'}\left(\frac{s}{2}\right)-\psi^{'}\left(\frac{s+1}{2}\right)\right].$$

4.2 Using ERH to find bounds

It's now finally time to reintroduce ERH into the mix. First and foremost, knowing the real part of the zeroes of ζ and L allows us to properly compare their norm, which we will denote with $\|\cdot\|$. In the next lemma, we'll make use of this fact to conclude the following:

Lemma 4.4 (5.4)**.** *[ERH]*
Let I_0 be defined like in lemma 4.4. Then, for $0<a<1$ and $x\geq 1$:

$$I_0\leq\max\left(0,\frac{\beta-1}{a^2}\right)+\frac{\log x}{x^a}\left[\sum_{\rho}\frac{a+2}{\|\rho+a\|^2}+\frac{5}{2}\right]+\frac{1}{x^a}\left[\sum_{\rho}\frac{1}{\|\rho+a\|^2}+1\right].$$

Proof
We'll only treat the case $\beta=0$, as we are working in $\mathbf{Q}$ and that's the one where the ERH is necessary.
Taking s=-a in lemma 5.2 we obtain:

$$I_0=-\left[\frac{1}{a^2}-\frac{\log x}{ax^a}-\frac{1}{a^2x^a}\right]+\frac{\log x}{x^a}\left[\sum+\frac{1}{a+1}+\left(\frac{\zeta^{'}}{\zeta}-\frac{L^{'}}{L}\right)(2)+\frac{3}{2}\right]$$

$$+\frac{1}{x^a}\left[\sum{}' + \frac{1}{(a+1)^2}\right],$$

where

$$\sum = \sum_\rho \pm\left(\frac{1}{-a-\rho} - \frac{1}{2-\rho}\right), \text{ and } \sum{}' = \sum_\rho \mp\frac{1}{(\rho+a)^2}.$$

Now:

$$\left\|\sum\right\| = \left\|\sum_\rho \pm\left(\frac{1}{-a-\rho} - \frac{1}{2-\rho}\right)\right\| \leq \sum_\rho \left\|\frac{1}{-a-\rho} - \frac{1}{2-\rho}\right\|$$
$$= \sum_\rho \left\|\frac{1}{+a+\rho} + \frac{1}{2-\rho}\right\|.$$

In turn we have that:

$$\sum_\rho \left\|\frac{1}{+a+\rho} + \frac{1}{2-\rho}\right\| \leq \sum_\rho \frac{2+a}{\|(\rho+a)(\rho-2)\|} = \sum_\rho \frac{2+a}{\|\rho+a\|\,\|\rho-2\|}.$$

If ERH holds, then $\mathrm{Re}(\rho) \geq \frac{1}{2}$ *and, because* $a < 1$*, we have that* $\|\rho-2\| > \|\rho+a\|$*. Thus:*

$$\left\|\sum\right\| \leq \sum_\rho \frac{2+a}{\|\rho+a\|\,\|\rho-2\|} \leq \sum_\rho \frac{2+a}{\|\rho+a\|^2}.$$

Keeping in mind the fact that $\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(2) < 0$*, we then conclude:*

$$\sum +\frac{1}{a+1} + \left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(2) + \frac{3}{2} \leq \sum +\frac{1}{1+1} + \frac{3}{2} \leq \sum_\rho \frac{a+2}{\|\rho+a\|^2} + \frac{5}{2}$$

Estimating $\sum'$ *in a similar manner and using the fact that* $\frac{1}{(1+a)^2} < 1$ *we obtain:*

$$\left[\sum{}' + \frac{1}{\|a+1\|^2}\right] \leq \left[\sum_\rho \frac{1}{\|\rho+a\|^2} + 1\right].$$

Lastly, some analytic manipulation yields:

$$\left[\frac{1}{a^2} - \frac{\log x}{ax^a} - \frac{1}{a^2x^a}\right] > 0.$$

Adding together these estimates leads us to the desired result. □

It is important to note that the use of ERH is fundamental for the proof. If, hypothetically, there was a zero with real part above 1, the inequality required to estimate $\sum$ would be flipped! This lemma and the following one are the reason why the assumption of ERH has profound implications on the Solovay-Strassen test and on primality tests in general. Referring back to lemma 4.4, we are now left with one last function to estimate. Once again we require the help of ERH:

Lemma 4.5 (5.6)**.** *[ERH]*
If χ is primitive, then:

$$\sum_{\rho} \frac{1}{|\rho + a|^2} = \frac{1}{2a+1}\left[log\frac{\Delta A_\chi}{\pi^{2n}} + 2\left(\frac{1}{a+1} + \frac{1}{a}\right) + (n+\alpha)\psi\left(\frac{a+1}{2}\right)\right.$$
$$\left. +(n-\alpha)\psi\left(\frac{a+2}{2}\right) + 2\frac{\zeta'}{\zeta}(1+a) + 2Re\frac{L'}{L}(1+a)\right] \leq$$
$$\leq \frac{1}{2a+1}\left[log(\Delta A_\chi) + 2n(\psi(a+1) - log(2\pi)) + 2\left(\frac{1}{a} + \frac{1}{a+1}\right)\right],$$

where the sum is over ρ roots of ζ and L (with multiplicities).
Proof
Let $\sigma > 0$, consider the representation discussed in the first section, and subsitute $s = \sigma$ to get

$$\frac{\zeta'}{\zeta}(\sigma) = B + \sum_{\rho}\left(\frac{1}{\sigma - \rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log\Delta - \frac{1}{\sigma} - \frac{1}{\sigma - 1} - \psi_\zeta(\sigma)$$

and

$$\frac{L'}{L}(\sigma) = B_\chi + \sum_{\rho}\left(\frac{1}{\sigma - \rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log A_\chi - \psi_L(\sigma).$$

Remember that for these equation we have that:

$$B + \sum_{\rho}\frac{1}{\rho} = 0 \text{ and } B_\chi + \sum_{\rho}\frac{1}{\rho} = 0.$$

Thus, with some rearrangement, we can rewrite them like this:

$$\sum_{\rho}\frac{1}{\sigma - \rho} = \frac{\zeta'}{\zeta}(\sigma) + \frac{1}{2}\log\Delta + \frac{1}{\sigma} + \frac{1}{\sigma - 1} + \psi_\zeta(\sigma)$$

$$\sum_{\rho} \frac{1}{\sigma - \rho} = \frac{L^{'}}{L}(\sigma) + \frac{1}{2}\log A_{\chi} + \psi_{L}(\sigma).$$

Now we conjugate both sides to get :

$$\sum_{\rho} \frac{1}{\sigma - \bar{\rho}} = \frac{\zeta^{'}}{\zeta}(\sigma) + \frac{1}{2}\log \Delta + \frac{1}{\sigma} + \frac{1}{\sigma - 1} + \psi_{\zeta}(\sigma)$$

$$\sum_{\rho} \frac{1}{\sigma - \bar{\rho}} = \overline{\frac{L^{'}}{L}(\sigma)} + \frac{1}{2}\log A_{\chi} + \psi_{L}(\sigma).$$

We then sum both pairs together and we obtain this formula:

$$\sum_{\rho} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \bar{\rho}} \right) = log\Delta A_{\chi} + 2\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1} \right) + 2(\psi_{\zeta}(\sigma) + \psi_{L}(\sigma)) + 2\frac{\zeta^{'}}{\zeta}(\sigma) + 2\,\mathrm{Re}\,\frac{L^{'}}{L}(\sigma).$$

Now, assuming ERH (and thus that $\rho = \frac{1}{2} + i\omega$) gives us the following algebraic identity:

$$\frac{1}{\|\rho + \sigma - 1\|^{2}} = \frac{1}{2\sigma - 1}\left(\frac{1}{\rho - \sigma} + \frac{1}{\sigma - \bar{\rho}} \right).$$

Using it with the substitution $\sigma = a + 1$ yields:

$$(2a+1)\sum_{\rho} \frac{1}{\|\rho + a\|^{2}} = log\Delta A_{\chi} + 2\left(\frac{1}{a+1} + \frac{1}{a} \right) + 2(\psi_{\zeta}(a+1) + \psi_{L}(a+1)) + 2\frac{\zeta^{'}}{\zeta}(a+1) + 2\,\mathrm{Re}\,\frac{L^{'}}{L}(a+1).$$

Lastly, we refer back to the properties previously discussed to express $2(\psi_{\zeta}(a+1) + \psi_{L}(a+1))$ and we divide both sides by (2a+1):

$$\sum_{\rho} \frac{1}{\|\rho + \sigma - 1\|^{2}} = \frac{1}{2a+1}\left[log\frac{\Delta A_{\chi}}{\pi^{2n}} + 2\left(\frac{1}{a+1} + \frac{1}{a} \right) + (n+\alpha)\psi\left(\frac{a+1}{2} \right) + +(n-\alpha)\psi\left(\frac{a+2}{2} + 2\frac{\zeta^{'}}{\zeta}(a+1) + 2\,\mathrm{Re}\,\frac{L^{'}}{L}(a+1) \right) \right].$$

This proves the first part of the theorem. From this, the upper bound is obtained by estimating $\frac{\zeta^{'}}{\zeta}(a+1) + \mathrm{Re}(\frac{L^{'}}{L}(a+1)) < 0$, and using the monotonicity of ψ together with the duplication formula. □

4.3 Bounds for the Rational Field

Now that we have obtained a generally true estimate, we can go back to focus on the specific $K = \mathbb{Q}$ case. As a reminder, we are trying to estimate where Euler Nonwitnesses lie on the real number line. To do that, we'll use the next two lemmas to pinpoint a specific property of subgroups of $\mathbb{Z}/(m)^*$. You can find a proof of these in pages 16-17 of [4].

Lemma 4.6 (6.1)**.**
Let χ be a nonprincipal character on $\mathbb{Z}/(m)^*$ with $\chi(n) = 1$ for all positive $n < x$. Then, for $0 < a < 1$, we define:

$$r(x) = \frac{(a+2)\log x + 1}{x^{a+1/2}},$$

$$s(x) = \frac{\frac{5}{2}\log x + 1}{x^{a+1/2}} + \frac{\beta}{(a-2)^2 x^{5/2}} \ ,$$

and

$$t(x) = -\log \pi + \psi\left(\frac{\alpha+\beta+1}{2}\right) + (2a+1)(\gamma + 2\log(4\pi)) + 2\frac{\zeta'}{\zeta}(1+a) + 4\sum_{n\geq x}\frac{\Lambda(n)}{n^{1+a}}.$$

That being said, the following is then true:

$$\frac{\sqrt{x}}{(a+1)^2} \leq \frac{1}{2a+1}(1 + r(x))\left[\log m + t(x)\right] + s(x).$$

And for a more accurate estimate:

Lemma 4.7 (6.3)**.**
Let $\mu(x) = \sum_{n\leq x}\Lambda(n)$, and choose A, $B > 0$ so that $\mu(t) \leq At$ for all positive t, and $\mu(x) > x - B\sqrt{x}$. Then:

$$\sum_{n\geq x}\frac{\Lambda(n)}{n^{1+a}} \leq \left(A\frac{(a+1)}{a} - 1 + \frac{B}{\sqrt{x}}\right)\frac{1}{x^a}.$$

In particular, for $x < 10^8$, we'll use the explicit values A=1.038 and B=2.052, found in [16]. Applying those values to the previous estimates, gives us the central theorem of this thesis, a very powerful result in group theory:

Theorem 4.8 (Bound on nontrivial subgroups)**.**
Let G be a nontrivial subgroup of $\mathbb{Z}/(m)^*$, such that $n \in G$ for all positive $n < x$. Then $x < 2\log^2 m$.
Proof
This proof will assume, without loss of generality, that G is maximal. Therefore there is a nonprincipal character χ whose Kernel contains G. We can assume that $\chi(n)$ =1 for every positive $n < x$. We now split the proof in two cases, based on the value of m: 1) Firstly we consider $m < 1000$. If $m < 3$, the theorem is vacuously true, as there are no nontrivial subgroups of $\mathbb{Z}/(m)^*$. If $m \geq 3$ and m is a prime, then m must have a primitive root $< 1.7\log^2 m$ [1].
Lastly, if $m \geq 3$ and m is a composite number, then it must have a divisor that is $\leq \sqrt{m}$, but a convexity argument shows that, for $6 \leq m \leq 1000$, we have $\sqrt{m} \leq 2\log^2 m$.

2) If instead we take $m \geq 1000$, and pick $a = 1/2$ we can use lemma 6.3 to approximate

$$4\sum_{n\geq x}\frac{\Lambda(n)}{n^{3/2}} \leq 4\left(-0.23+\frac{2.05}{\sqrt{x}}\right)\frac{1}{\sqrt{x}}.$$

Note that for $x > 2$ (the nontrivial cases), we have the upper bound

$$4\sum_{n\geq x}\frac{\Lambda(n)}{n^{3/2}} \leq 5.$$

We now use the approximations $2\frac{\zeta'}{\zeta}(3/2) \approx -3$ [18], and $\psi(3/4) = -\gamma + \frac{\pi}{2} - \log 8 \approx -1.085$, which give us:

$$\log m + t(x) \approx \log - \log \pi - \gamma + \frac{\pi}{2} - \log 8 + 2\gamma + 4 - 2\log 4\pi - 3 + 4\sum_{n\geq x}\frac{\Lambda(n)}{n^{1+a}} \approx$$

$$\approx \log m - 5.28 + 4\sum_{n\geq x}\frac{\Lambda(n)}{n^{1+a}} \leq \log m - 5.28 + 5 \leq \log m.$$

Furthermore, for $m > 1000$, $\log m > 6.9$, so $0 \leq \log m + t(x) \leq \log m$. Therefore by lemma 6.1 we have that:

$$\frac{\sqrt{x}}{9/8} \leq \frac{1}{2}(1+r(x))\left(\log m + t(x)\right) + s(x) \leq \frac{\log m}{2}(1+r(x)) + s(x) =$$

$$= \frac{\log m}{2}\left(1 + r(x) + \frac{2s(x)}{\log m}\right) \leq \log m \left(1 + r(x) + \frac{2s(x)}{\log m}\right)$$

Finally we multiply both sides by $\frac{9}{8}$*:*

$$\sqrt{x} \leq \frac{9}{8}\log m \left(1 + r(x) + \frac{2s(x)}{\log m}\right) \leq \frac{9}{8}\log m \left(1 + r(x) + \frac{2s(x)}{\log 1000}\right)$$

With $a = 1/2$ *and* $\beta = 0$*, given a sufficiently large* x*, such as* $x \geq 56$*, we have that:*

$$\frac{9}{8}\left(1 + r(x) + \frac{2s(x)}{\log 1000}\right) < \sqrt{2}$$

Applying this to the right portion of the previous equation results in:

$$\frac{9}{8}\log m \left(1 + r(x) + \frac{2s(x)}{\log 1000}\right) \leq \sqrt{2}\log m \text{ and thus } x \leq 2\log^2 m,$$

which is the desired bound.
Since $m > 1000$*, the case* $x < 56$ *is trivial, as* $x < 56 < 95 < 2\log^2 1000$. □

The above result is of an algebraic nature, but following the same process and with the help of modern computers, we can actually refine the case $m > 1000$ for better bounds, such as taking $x \geq 83.3$, which gives us a bound of $x < 1.783\log^2 m < 85$. With the same idea, even for the case $m \leq 1000$, a computational approach yields $x < 1.78\log^2 m$.

4.4 Applying the bounds to Solovay-Strassen

But what does this important result have to do with the original question? Well, it turns out that the set of Euler Nonwitnesses for a certain number has the structure of a nontrivial subgroup!

Proposition 4.9 (Nature of Euler Nonwitnesses)**.**
Let G *be the set of Euler Nonwitnesses for an integer* n*, then* G *is a nontrivial subgroup of* $\mathbb{Z}/(n)^*$*.*
Proof

Let a be a Euler Nonwitnesses, by definition $gcd(a, n) = 1$ and thus $a \in \mathbb{Z}/(n)^*$. Let a, $b \in G$, then

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \equiv a^{(n-1)/2}b^{(n-1)/2} \mod n \equiv (ab)^{(n-1)/2} \mod n.$$

Thus we have that $ab \in G$. Moreover, the Euler criterion is always true for 1, which implies that $1 \in G$. Lastly, since G is a subset of $\mathbb{Z}/(n)^*$, it inherits its associative property.
Therefore G is a nontrivial subgroup with standard multiplication as its binary operation. □

This theorem establishes that G has the structure we need to use the bounds we calculated for generic subgroups of $\mathbb{Z}/(n)^*$. In other words, it gives us an upper bound for the maximum value of x, below which we are certain to find at least one Euler witness, if n is composite. We thus arrive at the following conclusion:

Theorem 4.10 (Location of the first Euler witness)**.**
The Extended Riemann Hypothesis implies that any composite positive integer n has an Euler witness that is at most $2\log^2 n$.
Proof
Let n be a composite integer and let G be the set of Euler nonwitnesses of n. Due to n not being prime, the previous theorem tells us that G is a nontrivial subgroup of $\mathbb{Z}/(n)^*$. Let e_0 be the smallest Euler witness, by definition G is such that for every $n < e_0$, $n \in G$. Therefore theorem 4.8 can be applied to G, and we conclude that $e_0 < 2\log^2 n$ □

This proves that the proposed new version of the Solovay-Strassen test is indeed deterministic if we accept ERH, and gives a specific bound for the number of trials that are required.

Final remarks

Some more informed readers might be aware of the fact that the Solovay-Strassen test, even in its hypothetical deterministic form, has computational costs higher than similar primality tests, such as the Miller-Rabin test [6]. Nevertheless, we made the

conscious choice of focusing on the Solovay-Strassen test for the following reasons: first and foremost, a not insignificant amount of the newer, more optimal, primality tests that are available, such as the aforementioned one by Miller and Rabin, are somewhat derivative of the work of Solovay and Strassen, and share most of the ideas. As such, while this thesis didn't delve into it too deeply, it's possible to compute similar bounds for these tests, also dependant on the Extended Riemann Hypothesis. In addition to that, some other procedures, like the one used in the Baillie–PSW primality test, are partly based on Fermat's little theorem and, as such, can struggle when confronted with some numbers that are known to be problematic for it (Carmicheal numbers are the most well known). Due to the risk of running into false positives, these tests usually rely on an additional small test to check for accuracy. The historic importance of the Solovay-Strassen test thus can't be understated, and its study still proves useful to mathematicians to this day.

Acknowledgements

The help of several people was instrumental in writing this thesis: without their help my work would not have been as complete and my journey would have certaintly been harder. First and foremost, I would like to express my deepest gratitude to my thesis advisor, professor Lars Halvard Halle, who introduced me to the subject of this thesis, and patiently guided me in the writing process. Moreover, I could not have undertaken this journey without the help of fellow mathematician and friend Francesca Nanni, who taught me so much about LaTeX, and supported me all throughout the experience. I am also deeply indebted to Luke Jones, who spent many precious hours teaching me how to best convey my thoughts, while proofreading the thesis. Lastly, I would be remiss in not mentioning my family, whose support is the only reason I could realize my childhood dream of becoming a mathematician. From the bottom of my heart, grazie.

References

[1] J. C. P. Miller A. E. Western. *Tables of indices and primitive roots*. Royal Society, Cambridge, 1968.

[2] Milton Abramowitz and Irene A Stegun. *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Vol. 55. Courier Corporation, 1965, pp. 258–259.

[3] MM Artjuhov. "Certain criteria for primality of numbers connected with the little Fermat theorem". In: *Acta Arith* 12.355-364 (1966), p. 67.

[4] Eric Bach. "Explicit bounds for primality testing and related problems". In: *Mathematics of Computation* 55.191 (1990), pp. 355–380.

[5] Pete L Clark. "Number theory: A contemporary introduction". In: *Dep. of Mathematics, University of Georgia. http://math. uga. edu/pete/4400FULL. pdf* (2012), pp. 198–220.

[6] Keith Conrad. "The miller–rabin test". In: *Encyclopedia of Cryptography and Security* (2011).

[7] Keith Conrad. "The Solovay–Strassen Test". In: *URL https://kconrad. math. uconn. edu/blurbs/ugradnumthy/solovaystrassen. pdf* (2016).

[8] R Daileda and N Jones. "On primitivity of Dirichlet characters". In: *International Journal of Number Theory* 11.06 (2015), pp. 1913–1939.

[9] C.F. Gauss. *Disqvisitiones arithmeticae*. in commission apvd G. Fleischer, jun., 1801. URL: `https://books.google.it/books?id=raxeAAAAcAAJ`.

[10] Carl Friedrich Gauss. *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik:(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova... etc.)* Springer, 1889.

[11] Albert Edward Ingham. *The distribution of prime numbers*. 30. Cambridge University Press, 1990.

[12] Carl Gustav Jacob Jacobi. *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie.* Walter de Gruyter, Berlin/New York Berlin, New York, 1846.

[13] Jeffrey C Lagarias and Andrew M Odlyzko. "Effective versions of the Chebotarev density theorem". In: *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*. Vol. 7. 1977, pp. 409–464.

[14] H.L. Montgomery and H. Davenport. *Multiplicative Number Theory*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475759273. URL: https://books.google.it/books?id=SFztBwAAQBAJ.

[15] Bernhard Riemann. "Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse". In: *Ges. Math. Werke und Wissenschaftlicher Nachlaß* 2.145-155 (1859), p. 2.

[16] J Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois Journal of Mathematics* 6.1 (1962), pp. 64–94.

[17] Robert Solovay and Volker Strassen. "A fast Monte-Carlo test for primality". In: *SIAM journal on Computing* 6.1 (1977), pp. 84–85.

[18] Alwin Walther. *Anschauliches zur Riemannschen zetafunktion*. 1926.