Spring 5-1-2021

The Generalized Riemann Hypothesis and Applications to Primality Testing

Peter Hall
peter.fenteany@gmail.com

The Generalized Riemann Hypothesis and Applications to Primality Testing

Peter Hall

B.A., Mathematics

An Undergraduate Honors Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor of Arts

at the

University of Connecticut

May 2021

APPROVAL PAGE

Bachelor of Arts Honors Thesis

The Generalized Riemann Hypothesis and Applications to Primality Testing

Presented by

Peter Hall, B.A. Math

Honors Major Advisor ______________________________
Álvaro Lozano-Robledo

Honors Thesis Advisor ______________________________
Keith Conrad

University of Connecticut

May 2021

ACKNOWLEDGMENTS

This thesis is the result of a year and a half of continual support of the University Scholar Program, my advisory committee, and in particular my primary thesis advisor, Dr. Keith Conrad. Dr. Conrad helped me develop my ideas when proposing this project, was with me when collecting research, and pushed me when it came to writing and finalizing this work.

Dr. Conrad not only provided support, but he pushed me to realize my potential as a mathematician and writer and realize this piece into what it has become. When graduate applications were underway and pandemic-fueled malaise threatened to creep in, Dr. Conrad kept me oriented and honest, and for that I thank him. A project of the scope I set out on was not easy. When planning, I had to be extra comprehensive. When writing, I had to be extra adaptive. And when editing, I had to be extra critical. Dr. Conrad helped push me to accomplish all of this, through the triumphs and tribulations, through the best of times and the most difficult. I thank him for his specific time and care in poring over this thesis time and time again with me.

I thank Dr. Conrad along with my associate advisors, Dr. Benjamin Fuller and Dr. Álvaro Lozano-Robledo, for all their collective excitement and interest in both my project here and my future development as I applied to and was accepted to graduate schools. My peers, professors, and administrators in the Mathematics and Computer Science and Engineering departments at the University of Connecticut also helped

me greatly along my academic journey thus far, and for that I acknowledge them as well. The University Scholar Program gave me the opportunity and resources to give this topic the focus and diligence it deserves.

Finally, I would like to thank my family and friends, both within and outside of the UConn community. My mother was a great sounding board for me to rant about the project to and my greatest cheerleader when giving my seminar talk on this material. My friends and roommates kept me sane through this past year and a half while also being understanding as I had to work and write through the critical moments. My family at The Daily Campus gave me fulfillment and community in a time where solitude through the pandemic and this independent project was a real risk. To all mentioned here, this thesis is just as much a testament to your presence in my life as it is to my effort.

The Generalized Riemann Hypothesis and Applications to Primality Testing

Peter Hall, B.A.

University of Connecticut, May 2021

ABSTRACT

The Riemann Hypothesis, posed in 1859 by Bernhard Riemann, is about zeros of the Riemann zeta-function in the complex plane. The zeta-function can be represented as a sum over positive integers n of terms $1/n^s$ when s is a complex number with real part greater than 1. It may also be represented in this region as a product over the primes called an Euler product. These definitions of the zeta-function allow us to find other representations that are valid in more of the complex plane, including a product representation over its zeros. The Riemann Hypothesis says that all zeros of the zeta-function with real part between 0 and 1 fall exactly on the line $\mathrm{Re}(s) = 1/2$.

The Generalized Riemann Hypothesis deals with a similar class of functions to the zeta-function called Dirichlet L-functions. This time, instead of a series with terms $1/n^s$, we consider the series with terms $\chi(n)/n^s$ for a (primitive) Dirichlet character χ. Similar to the zeta-function, this definition of a Dirchlet L-function leads to other representations, including an Euler product over the primes and a Hadamard product over its zeros. The Generalized Riemann Hypothesis says that all zeros of a Dirichlet L-function with real part between 0 and 1 have real part 1/2. Comparing product representations of the zeta-function and L-functions over prime numbers and over zeros gives intuition as to why the Riemann Hypothesis and Generalized Riemann Hypothesis about zeros of certain functions have implications for the prime numbers.

In this thesis we look at concepts necessary to build up an understanding of the Generalized Riemann Hypothesis (including the zeta-function, Dirichlet characters, and some background from complex analysis) and then discuss one application: primality testing. Specifically, we will show how the Generalized Riemann Hypothesis implies a widely used probabilistic primality test could be turned into an efficient, usable, deterministic primality test.

Contents

Introduction

The Riemann Hypothesis says all nontrivial zeros of the Riemann zeta-function have real part 1/2. This is one of the million dollar problems on the Clay Mathematics Institute's Millennium Problems list in 2000. Before the Millennium Problem list was created, the Riemann Hypothesis was already regarded as the most important problem in mathematics and was on Hilbert's famous list of 23 problems in 1900.

The mere statement of the Riemann Hypothesis itself leaves a lot of questions unanswered. What is the Riemann zeta-function? Why should it have zeros with real part 1/2? What makes a zero of this function "nontrivial" (or "trivial")? Why is knowing where this function vanishes so intensely interesting? A partial answer to the last question is that the Riemann Hypothesis is a special case of a much broader conjecture called the Generalized Riemann Hypothesis, which is about the nontrivial zeros of infinitely many functions, and there are hundreds of consequences that are already known to follow from a positive solution to that problem.

In Chapter 1, we will introduce the Riemann zeta-function and some of its properties, finishing with a more nuanced statement of the Riemann Hypothesis for the completed zeta-function. In Chapter 2, we will discuss background in complex analysis that will be used elsewhere, including the Gamma function. In Chapter 3, we will introduce Dirichlet characters and their L-functions, which lead to the Generalized Riemann Hypothesis. Chapter 4 is about primality tests and their practical importance. Finally, in Chapter 5 we will see how the Generalized Riemann Hypothesis turns some probabilistic primality tests into efficient deterministic primality tests.

Readers are expected to be familiar with basic complex analysis and number theory, as well as asymptotic notation and big-O notation.

Chapter 1

The Riemann Zeta-function

We introduce the Riemann zeta-function. While it has a simple definition in an initial domain, we will see that complex analysis allows this function to be extended to the whole complex plane. After explaining what the zeta-function is and its connection to the primes through an Euler product, we will look at other topics related to the zeta-function such as the Prime Number Theorem and the Riemann Hypothesis.

1.1 Primes and the Riemann zeta-function

To understand properties of prime numbers, either rigorously or heuristically, mathematicians have used techniques from numerous areas of mathematics, such as abstract algebra, probability, and analysis. This thesis is about applications of complex analysis to study the prime numbers. We will begin with Euler's use of an infinite series from calculus to prove the following old theorem of Euclid.

Theorem 1.1.1. *There are infinitely many primes.*

Proof. We argue by contradiction. Suppose there are finitely many primes, say $p_1, \ldots, p_m$. Since $0 < 1/p_i < 1$, we can expand the factors in the finite product

$$\prod_{i=1}^{m} \frac{1}{1 - 1/p_i} = \prod_{i=1}^{m} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots\right)$$

as geometric series. In particular, $1/(1-1/p) > 1 + 1/p + 1/p^2 + \cdots + 1/p^k$ for $k \geq 1$.

We can multiply these finitely many geometric series together by picking one term from each series and multiplying them. This leads to a term $1/n$ for each integer $n \geq 1$: writing the prime factorization of n as $p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, where each $e_i \geq 0$, multiplying the e_i-th term from the ith factor (the first term in each geometric series has $e_i = 0$) gives us

$$\frac{1}{p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}} = \frac{1}{n}.$$

By unique factorization, $1/n$ arises in this way exactly once. Therefore

$$\prod_{i=1}^{m} \frac{1}{1 - 1/p_i} \geq \sum_{n \geq 1} \frac{1}{n}.$$

The harmonic series on the right is infinite, but the product of $1/(1 - 1/p_i)$ on the left is finite since it has finitely many terms. This is a contradiction. Thus there are infinitely many primes. □

The above proof gives us a glimpse at one of the central topics of this thesis: the Riemann zeta-function. It is denoted $\zeta(s)$ and is defined as follows.

Definition 1.1.2. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, the *Riemann zeta-function* at s is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots .$$

Let's show this series makes sense. When working with complex numbers s, we will use the traditional notation σ for $\mathrm{Re}(s)$ and t for $\mathrm{Im}(s)$, so $s = \sigma + it$.

Theorem 1.1.3. *For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, the series $\zeta(s)$ converges.*

Proof. We present two arguments.

First proof: We will show the series $\zeta(s)$ converges when $\mathrm{Re}(s) > 1$ since it is in fact absolutely convergent at such s. Writing $s = \sigma + it$,

$$n^s = n^{\sigma+it} = n^\sigma n^{it} = n^\sigma e^{it\log n},$$

so $|n^s| = n^\sigma$ since $|e^{i\theta}| = 1$ by Euler's formula for $e^{i\theta}$ when θ is real. It was not important that $n \in \mathbb{Z}^+$ here: $|a^s| = a^\sigma$ for all real $a > 0$ and all $s \in \mathbb{C}$.

The series $\sum_{n\ge1} 1/n^\sigma$ converges for $\sigma > 1$ by the integral test on $\int_1^\infty dx/x^\sigma$, so $\sum_{n\ge1} 1/n^s$ is absolutely convergent when $\mathrm{Re}(s) > 1$.

Second proof: We will more directly apply the Cauchy criterion for convergence. Let $1 < A < B$ for natural numbers A and B. Then

$$\left|\sum_{n=A}^{B} \frac{1}{n^s}\right| \le \sum_{n=A}^{B} \left|\frac{1}{n^s}\right| \le \sum_{n=A}^{B} \frac{1}{n^\sigma}.$$

We have $1/n^\sigma \le \int_{n-1}^{n} (1/x^\sigma)\,dx$ for $n \ge 2$, so by adding these together for $n = A, \ldots, B$,

$$\sum_{n=A}^{B} \frac{1}{n^\sigma} \le \int_{A-1}^{B} \frac{1}{x^\sigma}\,dx = \left.\frac{-1}{(\sigma-1)x^{\sigma-1}}\right|_{A-1}^{B} = \frac{1}{\sigma-1}\left(\frac{1}{(A-1)^{\sigma-1}} - \frac{1}{B^{\sigma-1}}\right).$$

For $\sigma > 1$, that integral approaches 0 as $A, B \to \infty$. Therefore, by Cauchy's convergence test we have shown $\zeta(s)$ is absolutely convergent. This second proof is basically a more careful account of why the integral test works in the first proof. □

In Euler's proof of Theorem 1.1.1 we were essentially working with $\zeta(s)$ at $s = 1$, where the series doesn't make sense. The following infinite product decomposition for $\zeta(s)$, when $\mathrm{Re}(s) > 1$, is inspired by the product over primes at $s = 1$ that led to a contradiction in Euler's argument.

Theorem 1.1.4. *For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$,*

$$\zeta(s) = \prod_{\text{prime } p} \frac{1}{1 - 1/p^s}.$$

Proof. To show the product on the right converges, we will apply a criterion for convergence from [8, Prop. 7.4]: for a sequence $\{a_k\}$ in $\mathbb{C}$ such that $|a_k| < 1$ for all k and $\sum_{k\geq 1} |a_k|$ converges, the infinite product $\prod_{k\geq 1} 1/(1 - a_k)$ converges (to a nonzero value). Apply this criterion to $a_k = 1/p_k^s$, where p_k is the k-th prime number and $\mathrm{Re}(s) > 1$. The series $\sum_{k\geq 1} |1/p_k^s| = \sum_{k\geq 1} 1/p_k^\sigma$ converges since its terms are part of the convergent series of positive numbers $\zeta(\sigma)$. Therefore the infinite product

$$\prod_{k\geq 1} \frac{1}{1 - 1/p_k^s} = \prod_{p} \frac{1}{1 - 1/p^s} \tag{1.1.1}$$

converges for $\sigma > 1$.

The expansion of this product over p into the series $\sum_{n\geq 1} 1/n^s$ defining $\zeta(s)$ when $\mathrm{Re}(s) > 1$ is a special case of [8, Prop. 7.5]: when we expand each of the factors into a geometric series

$$\prod_{k\geq 1} \frac{1}{1 - 1/p_k^s} = \prod_{k\geq 1} \left(1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} + \cdots\right)$$

this product equals the infinite series of numbers obtained by multiplying together one term from each of finitely many of the geometric series at a time (while intuitively all the other geometric series contribute their first term 1).

By unique factorization of natural numbers, each integer $n \geq 2$ can be written as $n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$, where the product is over finitely many primes and $e_i \geq 1$. Then

$$\frac{1}{n^s} = \frac{1}{p_1^{e_1 s} p_2^{e_2 s} \cdots p_m^{e_m s}} = \frac{1}{p_1^{e_1 s}} \frac{1}{p_2^{e_2 s}} \cdots \frac{1}{p_m^{e_m s}}.$$

The numbers on the right are exactly what we get when we multiply together one term each from the finitely many geometric series in (1.1.1) associated to primes p_k dividing n (and intuitively the geometric series for $1/(1 - 1/p_k^s)$ at primes p_k not dividing n contribute their first term 1). Including also the constant term $1 = 1/n^s$ for $n = 1$, we obtain in this way all the terms of the series $\sum_{n \geq 1} 1/n^s$ exactly once, and nothing more, and that series defines $\zeta(s)$. □

For $\mathrm{Re}(s) > 1$, the product representation of the zeta-function in Theorem 1.1.4 is called its *Euler product*. This product is naturally indexed by the prime numbers, which is an indication that $\zeta(s)$ is linked to the primes.

1.2 Analytic continuation and the completed zeta-function

The series and product representation of the Riemann zeta-function in the previous section are defined on the right half-plane $\{s : \mathrm{Re}(s) > 1\}$. We will use complex analysis to extend the zeta-function outside this half-plane, when neither the series nor the product can be used anymore.

The series $\zeta(s)$ is an analytic function when $\mathrm{Re}(s) > 1$, as a special case of Theorem 2.2.4 coming up. Recall that an analytic function f defined on a nonempty connected open subset U of $\mathbb{C}$ (like an open disc or right half-plane $\mathrm{Re}(s) > c$) has at most one extension to an analytic function on a larger connected open subset V in $\mathbb{C}$ [17, Chap.2, Cor. 4.9]: if f_1 and f_2 are analytic on V and

$$f_1(s) = f_2(s)$$

for all $s \in U$, then $f_1(s) = f_2(s)$ for all $s \in V$. There is no guarantee that such a function on V exists, but if it does then it is unique: two constructions of an analytic function on V that both restrict to f on U must be the same function on all of V. We can therefore speak about an *analytic continuation* of f from U to V to mean an analytic function on V that equals f on U. Building an analytic continuation can be hard work!

With analytic functions in mind, we will extend the Riemann zeta-function to the half-plane $\mathrm{Re}(s) > 0$ except at the point $s = 1$.

Theorem 1.2.1. *There is an extension of the Riemann zeta-function to an analytic function on the half-plane* $\mathrm{Re}(s) > 0$ *except for a simple pole at* $s = 1$ *with residue* 1.

Proof. We define the *alternating zeta-function* as

$$\zeta^{\pm}(s) := \sum_{n \geq 1} \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots,$$

which converges for real $s > 0$ since it is an alternating series. Convergence at these real numbers turns out to imply the series $\zeta^{\pm}(s)$ converges and is analytic for all complex s with $\mathrm{Re}(s) > 0$: see Remark 2.2.3 and Theorem 2.2.4. Its value at $s = 1$

is the alternating harmonic series:

$$\zeta^{\pm}(1) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} = \log 2.$$

For $\mathrm{Re}(s) > 1$, we have a relation between $\zeta(s)$ and $\zeta^{\pm}(s)$:

$$\zeta^{\pm}(s) = \left(1 - \frac{2}{2^s}\right)\zeta(s). \tag{1.2.1}$$

This comes from multiplying out the right side carefully (when $\mathrm{Re}(s) > 1$):

$$\begin{aligned}\left(1 - \frac{2}{2^s}\right)\zeta(s) &= \zeta(s) - \frac{2}{2^s}\zeta(s) \\ &= \sum_{m\geq 1}\frac{1}{m^s} - \sum_{m\geq 1}\frac{2}{(2m)^s} \\ &= \sum_{m\geq 1}\left(\frac{1}{(2m-1)^s} + \frac{1}{(2m)^s}\right) - \sum_{m\geq 1}\frac{2}{(2m)^s} \\ &= \sum_{m\geq 1}\left(\frac{1}{(2m+1)^s} - \frac{1}{(2m)^s}\right) \\ &= \sum_{n\geq 1}\frac{(-1)^{n-1}}{n^s} \\ &= \zeta^{\pm}(s).\end{aligned}$$

Since the alternating zeta-function makes sense for $\mathrm{Re}(s) > 0$, we can try to extend $\zeta(s)$ to $\mathrm{Re}(s) > 0$ by solving for $\zeta(s)$ in (1.2.1):

$$\zeta(s) = \frac{\zeta^{\pm}(s)}{1 - 2/2^s}. \tag{1.2.2}$$

This formula is consistent with the previous meaning of $\zeta(s)$ when $\mathrm{Re}(s) > 1$, and now gives a meaning to $\zeta(s)$ as an analytic function when $\mathrm{Re}(s) > 0$ except at s where $2/2^s = 1$, which corresponds to $s = 1 + 2\pi i k/\log 2$ for $k \in \mathbb{Z}$.

Since $1 - 2/2^s$ has a simple zero at $s = 1$, while $\zeta^{\pm}(1) = \log 2 \neq 0$, $\zeta(s)$ has a simple pole at $s = 1$ and its residue there is

$$\zeta^{\pm}(1) \lim_{s\to 1} \frac{s-1}{1-2/2^s} = \log 2 \lim_{s\to 1} \frac{s-1}{1-2e^{-s\log 2}} = \log 2\, \frac{1}{\log 2} = 1.$$

To handle the points $1 + 2\pi i k/\log 2$ where $k \neq 0$, consider a series with every third term negated:

$$\zeta^{+\pm}(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \dots.$$

This series converges for real $s > 0$. We can see this by viewing $\zeta^{+\pm}(s)$ as an alternating series: $1/n^s + 1/(n+1)^s > 2/(n+2)^s$ for $n \geq 1$ and $s > 0$, so $\zeta^{+\pm}(s)$ converges for $s > 0$ by the alternating series test. The series therefore converges and is analytic for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$ (Remark 2.2.3 and Theorem 2.2.4). For $\mathrm{Re}(s) > 1$ we have

$$\zeta^{+\pm}(s) = \left(1 - \frac{3}{3^s}\right)\zeta(s)$$

by an argument analogous to that for (1.2.1). Therefore we can try to define $\zeta(s)$ for $\mathrm{Re}(s) > 0$ in a second way as

$$\zeta(s) = \frac{\zeta^{+\pm}((s)}{1 - 3/3^s}. \tag{1.2.3}$$

This defines $\zeta(s)$ as an analytic function for $\mathrm{Re}(s) > 0$ except perhaps at s where $3/3^s = 1$, which means except perhaps when $s = 1 + 2\pi i m/\log 3$ for $m \in \mathbb{Z}$. We have $1 + 2\pi i k/\log 2 = 1 + 2\pi i m/\log 3$ if and only if $3^k = 2^m$, which occurs only when

$k = m = 0$ by unique factorization. So the uniqueness of analytic continuation, using either $\zeta^{\pm}(s)$ or $\zeta^{+\pm}(s)$ depending on the value of s, shows $\zeta(s)$ extends analytically from $\mathrm{Re}(s) > 1$ to $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$ with residue 1. □

This proof is a nice example of how the uniqueness of analytic continuation can help us extend a function by different methods to a larger domain.

The function $\zeta(s)$ can be extended analytically to the entire complex plane except for the simple pole at $s = 1$. We describe here one way to achieve that with the help of the Gamma function $\Gamma(s)$, which we will review in Section 2.4. The function $\Gamma(s)$ is initially defined on $\mathrm{Re}(s) > 0$ as an integral:

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1}\, dx = \int_0^\infty e^{-x} x^s \, \frac{dx}{x}.$$

Among the properties we'll see about $\Gamma(s)$ in Section 2.4 is that

- it is analytic for $\mathrm{Re}(s) > 0$,
- it can be extended to an analytic function on all of $\mathbb{C}$ except for simple poles at 0 and the negative integers and it has no zeros. In particular, $1/\Gamma(s)$ is entire since simple poles of $\Gamma(s)$ become simple zeros of $1/\Gamma(s)$, and $1/\Gamma(s)$ has no poles since $\Gamma(s)$ has no zeros.

Riemann extended $\zeta(s)$ from $\mathrm{Re}(s) > 1$ to $\mathbb{C}$ by combining $\zeta(s)$ with $\Gamma(s/2)$ and an exponential factor to form the completed zeta-function.

Definition 1.2.2. For $\mathrm{Re}(s) > 1$, the *completed zeta-function* $Z(s)$ is defined by the formula

$$Z(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

.

Using the integral defining $\Gamma(s)$ for $\mathrm{Re}(s) > 0$, the function $Z(s)$ for $\mathrm{Re}(s) > 1$ can be written as an integral over $(0, \infty)$ [17, Chap. 7, Theorem 2.2]:

$$Z(s) = \int_0^\infty \left(\sum_{n \geq 1} e^{-\pi n^2 x} \right) x^{s/2} \, \frac{dx}{x}.$$

By splitting the integral over $(0, \infty)$ into two integrals over $(0, 1]$ and $[1, \infty)$, making a change of variables to turn $(0, 1]$ into $[1, \infty)$, and using the Poisson summation formula, an alternative formula for $Z(s)$ is obtained that involves an integral over $[1, \infty)$ plus two simple extra terms that have simple poles at 0 or 1:

$$Z(s) = \int_1^\infty \left(\sum_{n \geq 1} e^{-\pi n^2 x} \right) \left(x^{s/2} + x^{(1-s)/2} \right) \frac{dx}{x} - \frac{1}{s} - \frac{1}{1-s}. \tag{1.2.4}$$

The integral here, over $[1, \infty)$, is absolutely convergent for all s in $\mathbb{C}$, and is an entire function. The right side of (1.2.4) provides an analytic continuation of $Z(s)$ to $\mathbb{C}$ except for simple poles at 0 and 1, so we get an analytic continuation for $\zeta(s)$ to $\mathbb{C}$ by writing $\zeta(s)$ in terms of $Z(s)$:

$$\zeta(s) = \frac{\pi^{s/2} Z(s)}{\Gamma(s/2)} = \pi^{s/2} \frac{1}{\Gamma(s/2)} Z(s). \tag{1.2.5}$$

Since $1/\Gamma(s)$ is entire, (1.2.5) defines $\zeta(s)$ on $\mathbb{C}$ as an analytic function except perhaps at $s = 0$ and $s = 1$, where $Z(s)$ has simple poles. The simple pole of $Z(s)$ at $s = 0$ is canceled by the simple pole of $\Gamma(s/2)$ at $s = 0$, so $\zeta(s)$ is actually analytic and nonzero at $s = 0$ (in fact, $\zeta(0) = -1/2$). The simple pole of $Z(s)$ at $s = 1$ is not canceled by the other factors $\pi^{s/2}$ or $1/\Gamma(s/2)$, which are analytic and nonvanishing at $s = 1$. Since $Z(s)$ at $s = 1$ has residue 1 (its polar term at $s = 1$ in (1.2.4) is $-1/(1-s) = 1/(s-1)$), from (1.2.5) the residue of $\zeta(s)$ at $s = 1$ is $\pi^{1/2}/\Gamma(1/2)$, which is 1 since $\Gamma(1/2) = \sqrt{\pi}$ (Theorem 2.4.4). Thus $\zeta(s)$ is analytic on $\mathbb{C}$ except for a simple pole at $s = 1$ with residue 1. This is a second explanation of the pole at $s = 1$ and its residue there, which we saw by another method in Theorem 1.2.1.

From the symmetric roles of s and $1-s$ in (1.2.4), the completed zeta-function satisfies the *functional equation*

$$Z(s) = Z(1-s).$$

We can turn this into an uglier (but sometimes useful) functional equation for the Riemann zeta-function itself.

Theorem 1.2.3. *For $s \in \mathbb{C}$, $\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\pi s/2)\zeta(s)$.*

Proof. Substituting the formula in Definition 1.2.2 at s and $1-s$ on both sides of the equation $Z(s) = Z(1-s)$ and solving for $\zeta(1-s)$,

$$\zeta(1-s) = \frac{\pi^{-s/2}\Gamma(s/2)}{\pi^{-(1-s)/2}\Gamma((1-s)/2)}\,\zeta(s) = \pi^{1/2-s}\frac{\Gamma(s/2)}{\Gamma((1-s)/2)}\,\zeta(s). \tag{1.2.6}$$

The Gamma function satisfies $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$ for all s in $\mathbb{C}$. This is called the reflection formula and we'll meet it in Theorem 2.4.4. Replacing s with $(1-s)/2$ in the reflection formula, $\Gamma((1-s)/2)\Gamma((1+s)/2) = \pi/\sin(\pi/2 - \pi s/2) = \pi/\cos(\pi s/2)$. Solving for $\Gamma((1-s)/2)$ and subtituting into (1.2.6) gives us

$$\zeta(1-s) = \pi^{-1/2-s}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{1+s}{2}\right)\cos\left(\frac{\pi s}{2}\right)\zeta(s). \tag{1.2.7}$$

Another identity for the Gamma function is the duplication formula $\Gamma(s)\Gamma(s+1/2) = 2^{1-2s}\sqrt{\pi}\Gamma(2s)$ for $s \in \mathbb{C}$ [10, Prop. 8.9]. Replacing s with $s/2$ in the duplication formula makes it $\Gamma(s/2)\Gamma((s+1)/2) = 2^{1-s}\sqrt{\pi}\Gamma(s)$. The left side is part of (1.2.7), so

$$\zeta(1-s) = \pi^{-1/2-s}2^{1-s}\sqrt{\pi}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s). \qquad \square$$

The next theorem puts the functional equation for $Z(s)$ in Theorem 1.2.2 to work.

Theorem 1.2.4. *The function $Z(s)$ is nonvanishing for $\mathrm{Re}(s) > 1$ and $\mathrm{Re}(s) < 0$.*

Proof. The Euler product for $\zeta(s)$ implies that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$. The Gamma function is analytic with no zeros on $\mathrm{Re}(s) > 1$, and the function $\pi^{-s/2} = e^{-(s/2)\log\pi}$ is analytic and nowhere vanishing on $\mathbb{C}$. Therefore $Z(s)$ has no zeros on the half-plane $\mathrm{Re}(s) > 1$.

If $\mathrm{Re}(s) < 0$ then $\mathrm{Re}(1-s) > 1$, so $Z(1-s) \neq 0$, and by the functional equation $Z(s)$ is also nonzero. □

Thus all zeros of $Z(s)$ lie in the vertical strip $0 \leq \mathrm{Re}(s) \leq 1$, which is called the *critical strip*. What does this tell us about zeros of $\zeta(s)$?

Theorem 1.2.5. *The function $\zeta(s)$ has simple zeros at the negative even integers and its other zeros are in the critical strip and are the same as the zeros of $Z(s)$ with the same multiplicities. It has no real zeros in the critical strip.*

Proof. Since $\Gamma(s)$ has no zeros and has poles at 0 and the negative integers, which are all simple, $\Gamma(s/2)$ has no zeros and has simple poles at 0 and the negative even integers. Therefore the nonvanishing of $Z(s)$ for $\mathrm{Re}(s) < 0$ implies $\zeta(s) = \pi^{s/2}Z(s)/\Gamma(s/2)$ has simple zeros at the negative even integers and nowhere else when $\mathrm{Re}(s) < 0$. Other zeros for $\zeta(s)$ must lie in the critical strip.

Since $\pi^{s/2}$ and $\Gamma(s/2)$ are analytic and nonvanishing on the critical strip for $s \neq 0$, and we already saw from (1.2.5) that $\zeta(0) \in \mathbb{C}^\times$, the zeros of $\zeta(s)$ in the critical strip are the same as the zeros of $Z(s)$ with the same multiplicities.

To show $\zeta(s)$ has no real zeros in the critical strip, we already mentioned that $\zeta(0) \neq 0$ and there is a pole at $s = 1$. For real s in $(0, 1)$ we can use the alternating zeta-function:

$$\zeta(s) = \left(1 - \frac{2}{2^s}\right) \zeta^{\pm}(s).$$

The factor $1 - 2/2^s$ is negative while $\zeta^{\pm}(s) > 0$ due to its formula as an alternating series, so $\zeta(s) < 0$ when $s \in (0, 1)$. □

The negative even integers are called the *trivial zeros* of $\zeta(s)$ since they are easy to explain (coming from poles of $\Gamma(s/2)$ except at 0). All other zeros of $\zeta(s)$ are called *nontrivial*, so the nontrivial zeros of $\zeta(s)$ are the same thing as the zeros of $Z(s)$ (with the same multiplicities). From the functional equation of $Z(s)$, a zero ρ of $Z(s)$ in the critical strip (that is, a nontrivial zero of $\zeta(s)$) leads to a zero $1 - \rho$, and these two numbers are symmetric with respect to the point $s = 1/2$: one is in the upper half-plane and the other is in the lower half-plane since we have shown there are no real zeros of $Z(s)$.

Theorem 1.2.6. *The function $Z(s)$ is nonvanishing for* $\mathrm{Re}(s) = 1$ *and* $\mathrm{Re}(s) = 0$.

Proof. First we treat $\mathrm{Re}(s) = 1$. The factors $\pi^{-s/2}$ and $\Gamma(s/2)$ are analytic and nonvanishing on that line, so it remains to prove $\zeta(s) \neq 0$ when $\mathrm{Re}(s) = 1$.

The nonvanishing of $\zeta(s)$ on the line $\mathrm{Re}(s) = 1$ can't be seen from the series or

Euler product for $\zeta(s)$, which converge only when $\mathrm{Re}(s) > 1$. It is a more subtle analytic argument, which proceeds by contradiction: if $\zeta(1 + it_0) = 0$ for a nonzero real number t_0 (there is no zero at 1 since there is a pole at 1), then by using a product of functions such as

$$\zeta(s)^2\zeta(s + it_0)\zeta(s - it_0),$$

or

$$\zeta(s)^3\zeta(s + it_0)^4\zeta(s + 2it_0)$$

and a trigonometric inequality, a contradiction is reached. Details are in [16, Theorem 4.2.3] using the first product and [1, Theorem 13.6], [5, Chap. 5, Lemma 3], and [17, Chap. 7, Theorem 1.2] using the second product.

Since $Z(s) = Z(1 - s)$, from $Z(s)$ not vanishing on $\mathrm{Re}(s) = 1$ we see that $Z(s)$ also does not vanish on $\mathrm{Re}(s) = 0$. □

The first few zeros of $Z(s)$ (equivalently, of $\zeta(s)$) in the upper part of the critical strip have real part $1/2$, and they are approximately

$$\frac{1}{2} + 14.13472i, \quad \frac{1}{2} + 21.02203i, \quad \text{and} \quad \frac{1}{2} + 25.01085i.$$

The LMFDB page `https://www.lmfdb.org/L/1/1/1.1/r0/0/0` has approximations to further zeros. Whether all the nontrivial zeros have real part $1/2$ is what the Riemann Hypothesis is about.

Riemann Hypothesis: All nontrivial zeros of $\zeta(s)$ satisfy $\mathrm{Re}(s) = 1/2$.

By Theorem 1.2.5, an equivalent formulation of the Riemann Hypothesis is that all zeros of $Z(s)$ have real part $1/2$.

Riemann worked in analysis (Riemann integral, Cauchy-Riemann equations) and geometry (Riemann surfaces, Riemannian manifolds). He introduced $\zeta(s)$ and posed the Riemann Hypothesis in an 1859 paper on number theory where he proposed a way to settle what became known later as the Prime Number Theorem. That theorem and its link to $\zeta(s)$ is explained in the next section.

1.3 The Prime Number Theorem

The Prime Number Theorem is about the growth of the prime counting function.

Definition 1.3.1. For $x > 0$, $\pi(x)$ is the number of primes up to x.

For example, $\pi(8.3) = 4$ since there are 4 primes up to 8.3: 2, 3, 5, and 7.

Theorem 1.3.2 (Prime Number Theorem)**.** *As* $x \to \infty$*,* $\pi(x) \sim \dfrac{x}{\log x}$.

The proof of the Prime Number Theorem in 1896, independently by Hadamard and de la Vallée Poussin, was a landmark achievement of 19th century mathematics. We will not give the proof here, but will highlight some of the key ideas.

1. The Prime Number Theorem is equivalent to $\sum_{p^k \leq x} \log p \sim x$, where the sum runs over prime powers p^k up to x. It is technically simpler to prove a sum of terms up to x is asymptotic to x instead of to $x/\log x$ (note $\pi(x) = \sum_{p \leq x} 1$).

2. The proof of the Prime Number Theorem does not directly use $\zeta(s)$, but instead $-\zeta'(s)/\zeta(s)$, which for $\mathrm{Re}(s) > 1$ is as a series over prime powers:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p^k} \frac{\log p}{p^{ks}},$$

where p is prime and $k \geq 1$. This series comes from the Euler product for $\zeta(s)$ and will be explained in Section 2.2. The numerators in this series are precisely the terms being added up in $\sum_{p^k \leq x} \log p$, and the growth of this sum is analyzed using $-\zeta'(s)/\zeta(s)$.

3. The key technical property of $\zeta(s)$ needed in the proof of the Prime Number Theorem is that $\zeta(s) \neq 0$ on the line $\mathrm{Re}(s) = 1$ (see the proof of Theorem 1.2.6). That implies $-\zeta'(s)/\zeta(s)$ is analytic on $\mathrm{Re}(s) = 1$ except for a simple pole at $s = 1$ and the behavior of $-\zeta'(s)/\zeta(s)$ around the line $\mathrm{Re}(s) = 1$ is where most of the analytic subtleties of the proof of the Prime Number Theorem occur.

The Prime Number Theorem can be proved using nothing hard about $\zeta(s)$ near the line $\mathrm{Re}(s) = 1$ other than its nonvanishing for $\mathrm{Re}(s) \geq 1$. That is the approach of Newman (see [5, Chap. 5]). In order to prove the Prime Number Theorem with an error term, estimates are needed for $\zeta(s)$ in a region on both sides of the line $\mathrm{Re}(s) = 1$, and this is carried out in [10, Chap. 6]. Getting a sharp error term for the Prime Number Theorem is closely related to the Riemann Hypothesis, and to explain that we need to express the Prime Number Theorem in terms of an approximation to $\pi(x)$ that is more complicated than $x/\log x$.

For $x \geq 2$, the *logarithmic integral* at x is

$$\mathrm{Li}(x) = \int_2^x \frac{dy}{\log y}.$$

Using integration by parts once ($u = 1/\log y$, $dv = dy$),

$$\mathrm{Li}(x) = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dy}{(\log y)^2} = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right). \tag{1.3.1}$$

The O-estimates comes from the fact that $\int_2^x dy/(\log y)^2 \sim x/(\log x)^2$. To see this, we have $\int_2^x dy/(\log y)^2 \geq \int_2^x dy/(\log x)^2 = (x-2)/(\log x)^2$. This tends to ∞ with x, so both it and $x/(\log x)^2$ diverge as $x \to \infty$. We can therefore use L'Hopital's rule:

$$\lim_{x\to\infty} \frac{\int_2^x dy/(\log y)^2}{x/(\log x)^2} = \lim_{x\to\infty} \frac{1/(\log x)^2}{(\log x - 2)/(\log x)^3} = \lim_{x\to\infty} \frac{\log x}{\log x - 2} = 1.$$

This shows $\mathrm{Li}(x) \sim x/\log x$, so the Prime Number Theorem could be stated as $\pi(x) \sim \mathrm{Li}(x)$. It seems strange to introduce a more complicated function than the simple $x/\log x$ for the Prime Number Theorem, but a bound on the approximation of $\pi(x)$ by $\mathrm{Li}(x)$, not by $x/\log x$, turns out to be equivalent to the Riemann Hypothesis.

Theorem 1.3.3. *The Riemann Hypothesis is equivalent to the estimate*

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$

Proof. See [10, Section 10.2]. □

We can't replace $\mathrm{Li}(x)$ with $x/\log x$ since the difference $\mathrm{Li}(x) - x/\log x$ is nowhere close to $O(\sqrt{x}\log x)$. That can be seen by carrying out integration by parts on $\mathrm{Li}(x)$ in (1.3.1) a second time ($u = 1/(\log y)^2, dv = dy$),

$$\begin{aligned}\mathrm{Li}(x) &= \frac{x}{\log x} - \frac{2}{\log 2} + \frac{x}{(\log x)^2} - \frac{2}{(\log 2)^2} + \int_2^x \frac{2\,dy}{(\log y)^3} \\ &= \frac{x}{\log x} + \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right),\end{aligned}$$

so the difference $\mathrm{Li}(x) - x/\log x$ is asymptotic to $x/(\log x)^2$, which is not $O(\sqrt{x}\log x)$.

In the error term $O(\sqrt{x}\log x)$ of Theorem 1.3.3, the exponent in $\sqrt{x} = x^{1/2}$ comes from the 1/2 in the Riemann Hypothesis: the error term can't be $O(x^c)$ for some

$c < 1/2$ because that can be shown to imply $\zeta(s) \neq 0$ for $\text{Re}(s) > c$ while we know there are zeros with real part $1/2$. It is far from obvious why real parts of zeros of $\zeta(s)$ should be related to error terms in estimates on $\pi(x)$. At the end of this thesis we will see how real parts of zeros of $\zeta(s)$ (and related functions) all being $1/2$ lead to bounds on error terms for the running time of a primality test.

Chapter 2

Analysis Background

This chapter lays out most of the tools from complex analysis that we will need in order to build up an understanding of the Riemann Hypothesis and its implications. First we will introduce general terminology and results in complex analysis. Then we will discuss Dirichlet series, which are the class of functions that are modeled on the zeta-function. We will next look at infinite products, such as Euler products and Hadamard factorizations. Finally, we will see a particular meromorphic function known as the Gamma function (already introduced in Section 1.2). These topics may seem to jump around a bit, but later on we will see how they all come together.

2.1 Analytic functions

We present some definitions and concepts from complex analysis that will be generally useful for understanding the rest of this chapter.

Definition 2.1.1. For a sequence $\{z_n\}$ in $\mathbb{C}$, the series $\sum_{n\geq 1} z_n$ is called *absolutely* *convergent* if $\sum_{n\geq 1}|z_n|$ is finite.

As in real analysis, absolute convergence lets us to do much more with a series than we would be able to otherwise. In particular, general commutativity and associativity is valid: terms can be reordered or regrouped without changing the value of the series.

For a connected open set $\Omega \subseteq \mathbb{C}$, a function $f : \Omega \to \mathbb{C}$ is called *holomorphic* or *analytic* if it is complex differentiable at each point in Ω. This is much stronger than differentiability in real analysis: functions on an open interval in $\mathbb{R}$ can be differentiable once but not twice, or be infinitely differentiable with no power series representation (see `https://en.wikipedia.org/wiki/Non-analytic_smooth_function`), but holomorphic (complex differentiable) functions on Ω are infinitely differentiable at each point of Ω and have local power series expansions on a neighborhood of each point in Ω. Functions that are holomorphic on the entire complex plane are called *entire*.

Remark 2.1.2. If a holomorphic function on Ω extends continuously to the boundary of Ω, then it might not be holomorphic on the boundary. For example, if a power series $\sum c_n z^n$ converges at a point on the unit circle then it converges and is holomorphic on the open unit disc $|z| < 1$, but on the unit circle this series is a complex Fourier series in disguise: $\sum c_n z^n = \sum c_n e^{in\theta}$ when $z = e^{i\theta}$, and even basic convergence questions about Fourier series have many subtleties.

When f is holomorphic in a neighborhood of a point a and $\lim_{z\to a}|f(z)| = \infty$, then a is called a *pole* of the function. For example, the function $1/z$ is analytic on $\mathbb{C}^\times$ and has a pole at $z = 0$. A function defined on a connected open set Ω except for poles on a discrete subset of Ω is called a *meromorphic* function on Ω.

Logarithms on $\mathbb{C}^\times$ are much more complicated than on the positive real axis:

there is no continuous or holomorphic function $L(z)$ on all of $\mathbb{C}^\times$ where $L(zw) = L(z) + L(w)$ everywhere other than the zero function. To speak about the logarithm of a holomorphic function, we need to be more careful than composing the function with "the logarithm".

Definition 2.1.3. A *logarithm* of a holomorphic function $f\colon \Omega \to \mathbb{C}$ is a holomorphic function $g\colon \Omega \to \mathbb{C}$ such that $e^{g(z)} = f(z)$ for all $z \in \Omega$.

Intuitively, if $e^{g(z)} = f(z)$ then $g(z) = \log f(z)$, but we already pointed out that logarithms of nonzero complex numbers are tricky things. That is why we did not define logarithms of holomorphic functions by using logarithms anywhere. We instead defined them using inverted exponential relations: g is called a logarithm of f when f is the exponential of g. Exponentials of complex numbers have none of the subtleties of logarithms of complex numbers.

Necessarily f has to be nonvanishing on Ω in order to have a logarithm, since a function of the form $e^{g(z)}$ is always nonvanishing. The next theorem, part of which will be applied to the zeta-function in Theorem 2.2.6, shows that necessary condition for f to have a logarithm is also sufficient as long as the domain of f is nice enough (the domain does not have disjoint open pieces and has no holes).

Theorem 2.1.4. *If $f\colon \Omega \to \mathbb{C}$ is holomorphic and nowhere vanishing on a connected and simply connected open set Ω, then f has a logarithm on Ω: there is a holomorphic function g on Ω such that*

$$f(z) = e^{g(z)}$$

for all $z \in \Omega$. This function $g(z)$ is unique up to addition by $2\pi ik$ for an integer k and $g'(z) = f'(z)/f(z)$.

Proof. (From [16, Theorem 2.2.7] and [17, Section 3.4]) Fix a point z_0 in Ω, and pick $c_0 \in \mathbb{C}$ such that $e^{c_0} = f(z_0)$. We can find c_0 since $f(z_0) \neq 0$ and the exponential function takes on all nonzero values.

If we could find a holomorphic function $g(z)$ such that $e^{g(z)} = f(z)$ then differentiating both sides tells us $e^{g(z)}g'(z) = f'(z)$, so $g'(z) = f'(z)/f(z)$. That suggests $g(z)$, if it exists at all, should be an integral of $f'(z)/f(z)$, which is why we now define

$$g(z) = \int_{\gamma_z} \frac{f'(w)}{f(w)} dw + c_0,$$

where γ_z is a path in Ω connecting z_0 to z.

This definition of $g(z)$ makes sense on account of several properties.

1. A path γ_z from z_0 to z in Ω exists because Ω is path-connected (connected open sets in $\mathbb{C}$ are path-connected).

2. Since f is nonvanishing on Ω, $f'(w)/f(w)$ is holomorphic on Ω, so we can integrate it on a path in Ω.

3. For two different paths in Ω from z_0 to z, the integrals of $f'(w)/f(w)$ on those paths are equal by the Cauchy integral formula: two different paths from z_0 to z in Ω form a loop if we traverse one path from z_0 to z and then the reverse of the other path from z back to z_0. Since $f'(w)/f(w)$ is holomorphic on both paths and in the region between them (since Ω is simply connected), the integral of $f'(w)/f(w)$ along one path plus the reverse of the other is 0 by the Cauchy integral formiula, so the integrals of $f'(w)/f(w)$ along both paths from z_0 to z are equal.

We put c_0 in the definition of $g(z)$ to make $g(z_0) = c_0$ (the path γ_{z_0} is a loop at

z_0 and an integral of $f'(w)/f(w)$ on that loop is 0 by the Cauchy integral formula), so $e^{g(z_0)} = e^{c_0} = f(z_0)$. Without c_0, $g(z_0)$ would be 0, so $e^{g(z_0} = 1$ and $f(z_0)$ need not be 1.

Next we will show $g'(z) = f'(z)/f(z)$, which is intuitively reasonable since $g(z)$ is an integral of $f'(z)/f(z)$. The derivative of g at z is defined to be

$$\lim_{h\to 0} \frac{g(z+h) - g(z)}{h} = \lim_{h\to 0} \frac{1}{h} \int_z^{z+h} \frac{f'(w)}{f(w)}\, dw,$$

where the integral is along a small path from z to $z+h$. Integrals of holomorphic functions on paths in Ω depend only on the endpoints and not on the specific path between the endpoints (as long as the path is in Ω), so for small nonzero h we use the straight line path from z to $z+h$. That path is $z + th$ for $0 \le t \le 1$, so

$$\frac{g(z+h) - g(z)}{h} = \frac{1}{h} \int_z^{z+h} \frac{f'(w)}{f(w)}\, dw, = \frac{1}{h} \int_0^1 h \frac{f'(z+th)}{f(z+th)}\, dt = \int_0^1 \frac{f'(z+th)}{f(z+th)}\, dt.$$

Since f is holomorphic, f'/f is continuous and bounded on a neighborhood of z,so we can take the limit inside the integral as $h \to 0$. Therefore

$$g'(z) = \int_0^1 \frac{f'(z)}{f(z)}\, dt = \frac{f'(z)}{f(z)}.$$

Now we show $e^{g(z)} = f(z)$ for all $z \in \Omega$. The product $f(z)e^{-g(z)}$ has derivative 0:

$$\begin{aligned}\left(f(z)e^{-g(z)}\right)' &= f'(z)e^{-g(z)} - f(z)g'(z)e^{-g(z)} \\ &= f'(z)e^{-g(z)} - f(z)\frac{f'(z)}{f(z)}e^{-g(z)} \\ &= f'(z)e^{-g(z)} - f'(z)e^{-g(z)},\end{aligned}$$

which is 0, so $f(z)e^{-g(z)}$ is constant. Evaluating this at z_0, we find $f(z_0)e^{-c_0} = e^{c_0}e^{-c_0} = 1$, so the constant value of $f(z)e^{-g(z)}$ is 1. Thus $f(z) = e^{g(z)}$ for $z \in \Omega$.

Two analytic functions $g_1(z)$ and $g_2(z)$ such that $f(z) = e^{g_1(z)} = e^{g_2(z)}$ on Ω differ at each z by an integral multiple of $2\pi i$: $g_2(z) = g_1(z) + 2\pi i k(z)$ for all $z \in \Omega$, where $k(z) \in \mathbb{Z}$. Because Ω is connected and $\mathbb{Z}$ is a discrete set, $k(z)$ must be constant. Then g_1 and g_2 differ on Ω by $2\pi i k$ for some $k \in \mathbb{Z}$. □

For a function $f(z)$ fitting the hypotheses of the previous theorem, a logarithm of it is denoted $\log f(z)$.

Because the derivative of $\log f(z)$ is $f'(z)/f(z)$, we refer to $f'(z)/f(z)$ as the *logarithmic derivative* of f even when f has poles: we don't need $\log f(z)$ to make sense in order for $f'(z)/f(z)$ to make sense. The formation of logarithmic derivatives converts products to sums. For a product of two terms this is the product rule:

$$\frac{(f_1f_2)'(z)}{(f_1f_2)(z)} = \frac{f_1'(z)f_2(z) + f_1(z)f_2'(z)}{f_1(z)f_2(z)} = \frac{f_1'(z)}{f_1(z)} + \frac{f_2'(z)}{f_2(z)}.$$

A helpful property of logarithmic derivatives is the information at their poles, which are the zeros and poles of the original function.

Theorem 2.1.5. *When a nonzero function $f(z)$ is meromorphic at a number a and its Laurent series at a has lowest-order term in degree m, $f'(z)/f(z)$ has a simple pole at a with residue m (so no pole if $m = 0$): for z near a,*

$$f(z) = c_m(z-a)^m + O((z-a)^{m+1}) \text{ with } c_m \neq 0 \Longrightarrow \frac{f'(z)}{f(z)} = \frac{m}{z-a} + O(1).$$

Proof. If $f(z)$ has a Laurent series representation centered at a with lowest-order term $c_m(z-a)^m$ (so $c_m \neq 0$), then $f'(z)$ has a Laurent series representation centered at a with lowest-order term $mc_m(z-a)^{m-1}$, so near a

$$\begin{aligned}\frac{f'(z)}{f(z)} &= \frac{mc_m(z-a)^{m-1}+O((z-a)^m)}{c_m(z-a)^m+O((z-a)^{m+1})}\\ &= \frac{mc_m(z-a)^{m-1}(1+O(z-a))}{c_m(z-a)^m(1+O(z-a))}\\ &= \frac{m}{z-a}\cdot\frac{1+O(z-a))}{1+O(z-a))}\\ &= \frac{m}{z-a}\,(1+O(z-a)))\\ &= \frac{m}{z-a}+O(1).\end{aligned}$$

This shows logarithmic derivatives have simple poles when $m \neq 0$: that is at poles of the original function ($m < 0$) and at zeros of the original function ($m > 0$). When $f(z)$ has neither a zero nor pole at a, $f'(z)/f(z)$ is analytic at a. □

2.2 Dirichlet series

The function $\zeta(s) = \sum_{n\geq 1} 1/n^s$ for $\mathrm{Re}(s) > 1$ has a rather different appearance than the more familiar representation of functions by power series in complex analysis. Infinite series of this kind are quite prominent in number theory, and this general type of function is called a Dirichlet series.

Definition 2.2.1. A *Dirichlet series* is a function of the form

$$f(s) = \sum_{n\geq 1}\frac{a_n}{n^s}.$$

for a sequence of complex numbers $\{a_n\}$, The zeta-function is the Dirichlet series where $a_n = 1$ for all n. Another Dirichlet series is the alternating zeta-function from the proof of Theorem 1.2.1:

$$\zeta^{\pm}(s) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots .$$

The series $\zeta(s)$ and $\zeta^{\pm}(s)$ both converge absolutely at the same values of s, since the terms in both series have the same absolute values. This is the half-plane $\mathrm{Re}(s) > 1$. A general result for all Dirichlet series is that if they converge absolutely somewhere then their domains of absolute convergence are half-planes.

Theorem 2.2.2. *Let $f(s) = \sum_{n\geq 1} a_n/n^s$ be a Dirichlet series. If $f(s_0)$ converges absolutely for some $s_0 \in \mathbb{C}$, then $f(s)$ converges absolutely for all s with $\mathrm{Re}(s) \geq \mathrm{Re}(s_0)$.*

Proof. For $s = \sigma + it$, $|1/n^s| = 1/n^\sigma$ (as we saw in the proof of Theorem 1.1.3). Write $s_0 = \sigma_0 + it_0$. Because $f(s_0) = \sum_{n\geq 1} a_n/n^{s_0}$ converges absolutely, the series

$$\sum_{n\geq 1} \frac{|a_n|}{n^{\sigma_0}}$$

converges. For $\sigma \geq \sigma_0$, the series $\sum_{n\geq 1} |a_n|/n^\sigma$ is term-by-term less than or equal to the series $\sum_{n\geq 1} |a_n|/n^{\sigma_0}$, which is convergent. Therefore the series $f(s)$ is absolutely convergent when $\mathrm{Re}(s) \geq \mathrm{Re}(s_0)$. □

A consequence of this is that if we can show a Dirichlet series converges absolutely at one complex number s_0, we automatically get absolute convergence of the series at every complex number s in the half-plane $\mathrm{Re}(s) \geq \sigma_0$.

Remark 2.2.3. Being more careful with the treatment of convergence, Theorem 2.2.2 can be extended to the case of a Dirichlet series converging perhaps only conditionally at a point: if $\sum a_n/n^s$ converges at s_0, but not necessarily absolutely there, then the series $\sum a_n/n^s$ converges at all s with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ (an open half-plane, not a closed half-plane). See [1, Theorem 11.8].

Just as a power series is infinitely differentiable and can be differentiated termwise on any open disc where it converges, the same is true for a Dirichlet series.

Theorem 2.2.4. *If a Dirichlet series $f(s) = \sum a_n/n^s$ converges on an open half-plane $\sigma > c$ then it is analytic on this half plane and its derivative there can be computed by termwise differentiation of the Dirichlet series:*

$$f'(s) = \sum_{n\geq 1} \frac{-a_n \log n}{n^s} = \sum_{n\geq 2} \frac{-a_n \log n}{n^s}.$$

Proof. See [1, Theorem 11.12]. This result does not require the series to converge absolutely on all of $\mathrm{Re}(s) > c$. □

Example 2.2.5. For $\mathrm{Re}(s) > 1$, $\zeta'(s) = -\sum_{n\geq 2} \frac{\log n}{n^s}$.

Using this, we will find a Dirichlet series for the negative logarithmic derivative of $\zeta(s)$.

Theorem 2.2.6. *For* $\mathrm{Re}(s) > 1$, $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p^k} \frac{\log p}{p^{ks}}$.

Proof. This is based on taking logarithmic derivatives of the Euler product representation $\zeta(s) = \prod_p 1/(1 - 1/p^s)$.

Since logarithmic differentiation turns products into sums, $(f^m)'/f^m = mf'/f$ for all integers m. We will use this when $m = -1$: $(1/f)'/(1/f) = -f'/f$, so

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

Therefore from $\zeta(s) = \prod_p 1/(1-1/p^s)$,

$$\begin{aligned}\frac{\zeta'(s)}{\zeta(s)} &= \sum_p \frac{-(\log p)/p^s}{1-1/p^s} \\ &= \sum_p \frac{-\log p}{p^s} \sum_{k\geq 0} \frac{1}{p^{ks}} \\ &= \sum_p \sum_{k\geq 0} \frac{-\log p}{p^{(k+1)s}} \\ &= \sum_{p^k} \frac{-\log p}{p^{ks}},\end{aligned}$$

where the last (absolutely convergent) sum runs over prime powers p^k where $k \geq 1$.

We did not justify why the logarithmic derivative of an infinite product is the sum of the logarithmic derivatives of the factors, so here is a completely separate way to derive that Dirichlet series for $\zeta'(s)/\zeta(s)$. From calculus,

$$\frac{1}{1-x} = e^{-\log(1-x)} = \exp\left(\sum_{k\geq 1} \frac{x^k}{k}\right)$$

when $|x| < 1$. The series $\sum_{k\geq 1} z^k/k$ converges for z in the open unit disc, so

$$\frac{1}{1-z} = \exp\left(\sum_{k\geq 1} \frac{z^k}{k}\right). \qquad (2.2.1)$$

when $|z| < 1$ because both sides are analytic there and agree on the interval $(-1, 1)$.

We'll use (2.2.1) for $z = 1/p^s$ when $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \prod_p \frac{1}{1 - 1/p^s} = \prod_p \exp\left(\sum_{k\geq 1} \frac{(1/p^s)^k}{k}\right) = \prod_p \exp\left(\sum_{k\geq 1} \frac{1}{kp^{ks}}\right).$$

The product over p is a limit of finite products and the exponential function is continuous, so for $\mathrm{Re}(s) > 1$

$$\zeta(s) = \exp\left(\sum_p \sum_{k\geq 1} \frac{1}{kp^{ks}}\right).$$

The single series $\sum_{p^k} 1/(kp^{ks})$ over prime powers converges absolutely for $\mathrm{Re}(s) > 1$, so it can be rewritten as the double series in the exponent above, and we get

$$\zeta(s) = \exp\left(\sum_{p^k} \frac{1}{kp^{ks}}\right)$$

for $\mathrm{Re}(s) > 1$. Thus $\sum_{p^k} 1/(kp^{ks})$ is a logarithm of $\zeta(s)$, so by Theorems 2.1.4 and 2.2.4.

$$\frac{\zeta'(s)}{\zeta(s)} = \left(\sum_{p^k} \frac{1}{kp^{ks}}\right)' = \sum_{p^k} \frac{-\log(p^k)}{kp^{ks}} = \sum_{p^k} \frac{-\log p}{p^{ks}}. \qquad \square$$

To make the Dirichlet series for $-\zeta'(s)/\zeta(s)$ a sum over $\mathbb{Z}^+$ rather than a sum only over prime powers, we introduce a standard number-theoretic function.

Definition 2.2.7. The *von Mangoldt function*, denoted $\Lambda(n)$, is defined on natural numbers n by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for prime } p \text{ and } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Example 2.2.8. Here is a table of the values of $\Lambda(n)$ for $1 \leq n \leq 10$.

n	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

For $\mathrm{Re}(s) > 1$ the Dirichlet series for $-\zeta'(s)/\zeta(s)$ over prime powers now becomes

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n \geq 1} \frac{\Lambda(n)}{n^s}. \tag{2.2.2}$$

One of the most important results about a Dirichlet series $f(s) = \sum a_n/n^s$ is a formula for the partial sums of its coefficients $\sum_{n \leq x} a_n$ in terms of an integral along a vertical line.

Theorem 2.2.9 (Perron's Formula)**.** *Let a_n be a sequence such that the Dirichlet series $f(s) = \sum a_n/n^s$ converges absolutely for $\mathrm{Re}(s) > 1$. For $c > 1$ and $x > 0$,*

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f(s) \frac{x^s}{s}\, ds = \sum_{n \leq x}{}^{*} a_n,$$

where $\int_{c-i\infty}^{c+i\infty}$ is defined to mean $\lim_{T\to\infty} \int_{c-iT}^{c+iT}$ and the last term in the partial sum is halved if $x \in \mathbb{Z}^+$.

Proof. See [1, Theorem 11.18]. The result in fact is true if the line $\mathrm{Re}(s) = c$ is in an open half-plane of convergence for the series $f(s)$ and the series converges on the line $\mathrm{Re}(s) = c$ only conditionally. □

The intuition behind Perron's formula comes from interchanging a sum and integral:

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f(s)\frac{x^s}{s}\,ds &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\sum_{n\geq 1}\frac{a_n}{n^s}\frac{x^s}{s}\,ds \\ &= \sum_{n\geq 1} a_n\left(\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{(x/n)^s}{s}\,ds\right) \qquad (2.2.3)\end{aligned}$$

and the vertical contour integrals can be computed from the following formula with $y = x/n$:

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{y^s}{s}\,ds = \begin{cases} 1, & \text{if } y > 1, \\ 1/2, & \text{if } y = 1, \\ 0, & \text{if } 0 < y < 1. \end{cases} \qquad (2.2.4)$$

The intuition behind these values when $y \neq 1$ is based on the residue theorem. Since $|y^s/s| = y^{\mathrm{Re}(s)}/|s|$, when $y > 1$ we want to push the contour we form to the left in order to make y^s/s tend to 0. This causes us to pass over the pole at the origin and the residue of y^s/s at $s = 0$ is 1. When $y < 1$, we want to push the contour to the right to make y^s/s tends to 0, which picks up no poles, so the integral will be 0. When $y = 1$, neither of these intuitions work, so we must calculate the integral more directly. The intuition behind (2.2.4) at $y = 1$ is that the halfway value between the values 0 and 1 is like the halfway value at a jump discontinuity in a Fourier series.

Plugging (2.2.4) into (2.2.3) with $y = x/n$, the nth term in (2.2.3) is 0 when $x/n < 1$, meaning $n > x$. For $n < x$, the nth term in (2.2.3) is a_n, and for $n = x$ (if $x \in \mathbb{Z}^+$) the nth term in (2.2.3) is $(1/2)a_n$. This gives us all the terms in the sum $\sum_{n\leq x}^{*} a_n$ in Perron's formula.

Example 2.2.10. Taking $f(s) = \zeta(s)$ in Perron's formula, so $a_n = 1$ for all n, we have for $c > 1$ and $x > 0$

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \zeta(s)\,\frac{x^s}{s}\,ds = \sum_{n\le x}{}^{*} 1 = \begin{cases} \lfloor x \rfloor, & \text{if } x \notin \mathbb{Z}^+, \\ x - 1/2, & \text{if } x \in \mathbb{Z}^+. \end{cases}$$

Example 2.2.11. Using $f(s) = -\zeta'(s)/\zeta(s) = \sum \Lambda(n)/n^s$ (by (2.2.2)) in Perron's formula, we have for $c > 1$ and $x > 0$

$$\sum_{n\le x}{}^{*}\Lambda(n) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)}\,\frac{x^s}{s}\,ds. \tag{2.2.5}$$

The partial sums of the von Mangoldt function are traditionally denoted by

$$\psi(x) := \sum_{n\le x}\Lambda(n) = \sum_{p^k\le x}\log p,$$

which was introduced by Chebyshev. We had mentioned this function of x in the summary of key ideas in the proof of the Prime Number Theorem in Section 1.3, where we said the relation $\pi(x) \sim x/\log x$ is equivalent to $\sum_{p^k\le x}\log p \sim x$, and that means $\psi(x) \sim x$ by the definition of $\psi(x)$. The Prime Number Theorem is essentially always proved by showing $\psi(x) \sim x$.

In (2.2.5) we have a formula for $\psi(x)$ when x is not a positive integer, or more precisely, not a prime power. If $x = p^k$ is a prime power, then the sum on the left side in (2.2.5) has last term $(1/2)\log p$ instead of $\log p$. Thus the left side of (2.2.5), while not always equal to $\psi(x)$ is always $\psi(x) + O(\log x)$.

2.3 Infinite products

Complex analysis focuses a lot on power series representations of functions, but product representations for functions will be just as important for us as series representations. We already saw this in the setting of the Euler product for $\zeta(s)$, which is how we got a Dirichlet series for $-\zeta'(s)/\zeta(s)$. The following theorem describes a more general class of Euler products than just the one for $\zeta(s)$, and this will be useful in the next chapter.

Theorem 2.3.1. *An Euler product of the form* $\prod_p \frac{1}{1 - a_p/p^s}$ *with* $|a_p| \leq 1$ *for all primes* p*, converges for* $\mathrm{Re}(s) > 1$ *and there it can be written as the absolutely convergent Dirichlet series* $\sum_{n \geq 1} \frac{a_n}{n^s}$*, where* $a_n = a_{p_1}^{e_1} \cdots a_{p_r}^{e_r}$ *when* n *has prime factorization* $p_1^{e_1} \cdots p_r^{e_r}$ *and* $a_1 = 1$.

Proof. See [8, Prop. 7.5]. □

We saw an example of an Euler product in Chapter 1, where we started with $\zeta(s)$ as a series converging absolutely on $\mathrm{Re}(s) > 1$ and then recognized it as having an Euler product there with $a_p = 1$ for all p. Theorem 2.3.1 allows us to reverse-engineer the half-plane of absolute convergence for the series defining the Riemann zeta-function if we had started with a definition of $\zeta(s)$ by its Euler product instead of by its series. Some analogues of the Riemann zeta-function, such as Artin L-functions, are defined as Euler products since the coefficients of their Dirichlet series representation don't have a simple interpretation.

A second type of product representation, which we have not met before, is applicable to entire functions with a restricted type of growth on large circles. The following theorem about these products is due to Hadamard and was inspired by Riemann's paper on the zeta-function.

Theorem 2.3.2 (Hadamard)**.** *For an entire function $f(s)$ that is not identically zero, let $|f|_r := \max_{|s|=r} |f(s)|$ for $r > 0$. Suppose for all $\varepsilon > 0$ that $\log |f|_r = O_\varepsilon(r^{1+\varepsilon})$ as $r \to \infty$. Then we have a product representation*

$$f(s) = e^{as+b} s^m \prod_{n \geq 1} \left(1 - \frac{s}{\rho_n}\right) e^{s/\rho_n},$$

for all $s \in \mathbb{C}$, where a and b are constant, $m = \operatorname{ord}_{s=0} f(s)$, and ρ_n runs over the zeros of f besides 0. The n-th factor in the product appears as often as the multiplicity of ρ_n as a zero of f.

The product above is absolutely convergent and for each $\varepsilon > 0$, the series

$$\sum_{n \geq 1} \frac{1}{|\rho_n|^{1+\varepsilon}}$$

converges, where each ρ_n is repeated with its multiplicity as a zero of f.

Proof. See [17, Section 5.1]. □

The product representation of $f(s)$ in Theorem 2.3.2 is called its *Hadamard factorization*. It is a generalization of the factorization of polynomials (a finite product with $a = 0$), with one difference being that here we associate to a zero ρ_n the factor $(1 - s/\rho_n)e^{s/\rho_n}$ with constant term 1 instead of the factors $s - \rho_n$ with leading coefficient 1. An infinite product of terms like $\prod_{n \geq 1}(s - \rho_n)$ doesn't make much sense: what would the constant term be if $\rho_n \to \infty$?

The purpose of the exponential factors e^{s/ρ_n} is to improve the convergence (compared to $\prod_{n \geq 1}(1 - s/\rho_n)$) without introducing additional zeros, as exponentials are always nonzero. Since $1 - s/\rho$ makes no sense when $\rho = 0$, we need to treat zeros at $s = 0$ separately and that is why there is a term s^m outside the product.

The factor e^{as+b} out front accounts for the only variations allowed when $|f|_r = O_\varepsilon(r^{1+\varepsilon})$ if we know the zeros and their multiplicities: multiplication by e^{as+b} maintains the growth condition on $|f|_r$ as $r \to \infty$. These extra factors e^{as+b} are analogous to the role of nonzero constants being multiplied by a factored polynomial, which change a polynomial while keeping it a polynomial and not affecting its zeros.

Example 2.3.3. Consider the entire function $f(s) = \sin(\pi s)$. It has simple zeros at the integers and no other zeros in $\mathbb{C}$, which can be seen from the identity $\sin(\pi s) = (e^{i\pi s} - e^{-i\pi s})/2i$, which vanishes only at the integers. When $|s| = r$ for some real $r > 0$, $|\sin s| = |(e^{i\pi s} - e^{-i\pi s})/2i| \leq (e^{\pi r} + e^{\pi r})/2 = e^{\pi r}$, so $|\sin(\pi s)| = O(e^{\pi r})$, which gives us $\log |f|_r = O(\pi r) = O(r) = O_\varepsilon(r^{1+\varepsilon})$ for all $\varepsilon > 0$. So we can use Theorem 2.3.2. In the same notation from there, we need $m = 1$ and a zero $\rho_n = n$ for each nonzero integer n. The Hadamard factorization of $\sin(\pi s)$ is

$$\sin(\pi s) = e^{as+b} s \prod_{n \in \mathbb{Z} - \{0\}} \left(1 - \frac{s}{n}\right) e^{s/n}$$

for some a and b. For $n \in \mathbb{Z}^+$, combining the terms in the product at n and $-n$ cancels out the exponential factors on those terms, so the Hadamard factorization for $\sin(\pi s)$ simplifies to

$$\sin(\pi s) = e^{as+b} s \prod_{n \geq 1} \left(1 - \frac{s^2}{n^2}\right).$$

At this point we can solve for a and b.

Determine b. Since $\sin(\pi s)/s \to \pi$ as $s \to 0$, we need $e^b = \pi$. Thus

$$\sin(\pi s) = e^{as}\pi s \prod_{n\geq 1}\left(1 - \frac{s^2}{n^2}\right).$$

Determine a. The infinite product over $n \geq 1$ is an even function of s and $\sin(\pi s)/(\pi s)$ is an even function of s, so e^{as} must be an even function of s: $e^{as} = e^{-as}$ for all $s \in \mathbb{C}$. Therefore $e^{2as} = 1$ for all $s \in \mathbb{C}$, which forces $a = 0$ (if $a \neq 0$ then $\{2as : s \in \mathbb{C}\} = \mathbb{C}$, so $\{e^{2as} : s \in \mathbb{C}\}$ is $\mathbb{C}^\times$ instead of 1).

As Theorem 2.3.2 predicts, for each $\varepsilon > 0$ the series

$$\sum_{n\geq 1}\left(\frac{1}{|n|^{1+\varepsilon}} + \frac{1}{|-n|^{1+\varepsilon}}\right) = \sum_{n\geq 1}\frac{2}{n^{1+\varepsilon}}$$

converges, which we saw in Chapter 1.

We now apply the Hadamard factorization to the completed zeta-function $Z(s)$. In Chapter 1, we saw

$$Z(s) = \int_1^\infty \left(\sum_{n\geq 1} e^{-\pi n^2 x}\right)(x^{s/2} + x^{(1-s)/2})\frac{dx}{x} - \frac{1}{s} - \frac{1}{1-s}$$

for all $s \in \mathbb{C}$ and this has zeros only in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$. The integral converges for all $s \in \mathbb{C}$ and is entire. Due to the simple poles at 0 and 1, multiply $Z(s)$ by $s(s-1)$ to make $Z(s)$ entire without changing its zeros in the critical strip or changing the functional equation.

Theorem 2.3.4. *The function $s(s-1)Z(s)$ has a Hadamard factorization*

$$s(s-1)Z(s) = e^{Bs}\prod_{\rho}\left(1 - \frac{s}{\rho}\right)e^{s/\rho}$$

for some $B \in \mathbb{C}$. Additionally, $\sum_\rho 1/|\rho|^{1+\varepsilon}$ converges for all $\varepsilon > 0$, where this sum is over the zeros of $s(s-1)Z(s)$ and each zero appears with its multiplicity in $Z(s)$.

Proof. The function $s(s-1)Z(s)$ can be shown to satisfy the growth hypotheses of Theorem 2.3.2 (see [4, p. 79]), so there are $A, B \in \mathbb{C}$ and $m \geq 0$ such that

$$s(s-1)Z(s) = e^{A+Bs}s^m \prod \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

On the left side, since $Z(s) = -1/s + O(1)$ near $s = 0$, $s(s-1)Z(s)$ at $s = 0$ has value 1: $s(s-1)Z(s)$ is nonvanishing at the origin. Thus $m = 0$ in the Hadamard factorization and $e^A = 1$. We are left with the product representation as in the statement of the theorem. □

The function $s(s-1)Z(s)$ has a Hadamard product on $\mathbb{C}$ and the function $\zeta(s)$ has an Euler product on the half-plane $\mathrm{Re}(s) > 1$, so when $\mathrm{Re}(s) > 1$ we have an equation involving two infinite product representations together with the Gamma function:

$$e^{Bs}\prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho} = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\prod_p \frac{1}{1-1/p^s}.$$

This shows $\pi^{-s/2}\Gamma(s/2)$ can be considered comparable to the Euler factors in the Euler product of $\zeta(s)$, even though it does not appear similar to $1/(1-1/p^s)$.

By carrying out the same analytic operations on both sides of this equation (forming logarithmic derivatives, integrating, etc.), we can relate the zeros ρ on the left side and the primes p on the right side. This is how nontrivial zeros of $\zeta(s)$ (the same thing as zeros of $Z(s)$) can be related to prime numbers.

In Chapter 3 we'll see generalizations of the zeta-function that lead to other pairs of related infinite product representations.

2.4 The Gamma function

We already met the Gamma function in Chapter 1 in the process of analytic continuation of the Riemann zeta-function. It will appear again in the next chapter when we analytically continue Dirichlet L-functions. Here we will discuss this function and its properties that are useful for us.

Definition 2.4.1. For real $s > 0$, the Gamma function at s is defined as

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1}\, dx = \int_0^\infty e^{-x} x^s \, \frac{dx}{x}.$$

This integral converges for positive s since x^{s-1} as a function of x is integrable just to the right of $x = 0$ (where e^{-x} is nearly 1) and e^{-x} decays much faster than x^{s-1} as $x \to \infty$. For $s \in \mathbb{C}$, since $|x^{s-1}e^{-x}| = x^{\sigma-1}e^{-x}$, the integral defining the Gamma function is absolutely integrable when $\sigma > 0$. Therefore we can define $\Gamma(s)$ by the above (absolutely convergent) integral when $\mathrm{Re}(s) > 0$, and it is analytic in s [17, Chap. 6, Prop. 1.1].

We can extend the Gamma function to all of $\mathbb{C}$, based on the following relation.

Theorem 2.4.2. *For all s with* $\mathrm{Re}(s) > 0$*,*

$$\Gamma(s+1) = s\Gamma(s).$$

Proof. This is integration by parts. By definition,

$$\Gamma(s+1) = \int_0^\infty e^{-x} x^s \, dx.$$

Cut this integral down to a finite interval $[\varepsilon, 1/\varepsilon]$ for small $\varepsilon > 0$ and apply integration by parts with $u = x^s$ and $dv = e^{-x}\,dx$:

$$\int_{\varepsilon}^{1/\varepsilon} e^{-x}x^s\,dx = -x^s e^{-x}\Big|_{\varepsilon}^{1/\varepsilon} + \int_{\varepsilon}^{1/\varepsilon} e^{-x}sx^{s-1}\,dx.$$

As $\varepsilon \to 0^+$, the integral on the right tends to $s\Gamma(s)$. As for the boundary terms, we show they go to 0 as $\varepsilon \to 0^+$:

$$|-x^s e^{-x}| = \frac{x^\sigma}{e^x},$$

which at $x = \varepsilon$ is $\varepsilon^\sigma/e^\varepsilon$ and that tends to 0 as $\varepsilon \to 0^+$ since $\sigma > 0$. The other boundary term is $(1/\varepsilon)^\sigma/e^{1/\varepsilon}$, which in term of the large number $y = 1/\varepsilon$ has the form y^σ/e^y, and this tends to 0 as $y \to \infty$ due to the exponential denominator. □

Since

$$\Gamma(1) = \int_0^\infty e^{-x}\,dx = -\,e^{-x}\Big|_0^\infty = 1,$$

the relation $\Gamma(s+1) = s\Gamma(s)$ for positive integers n becomes $\Gamma(n) = (n-1)!$ for positive integers n.

Using $\Gamma(s+1) = s\Gamma(s)$ repeatedly, we can extend the function $\Gamma(s)$ to a meromorphic function on $\mathbb{C}$ with only simple poles.

Theorem 2.4.3. *The function $\Gamma(s)$ has an analytic continuation to a meromorphic function on $\mathbb{C}$ with simple poles only at the nonpositive integers $s = 0, -1, -2, \ldots$.*

Proof. Rewrite the relation $\Gamma(s+1) = s\Gamma(s)$ when $\mathrm{Re}(s) > 0$ as $\Gamma(s) = \Gamma(s+1)/s$ and use the right of that to define $\Gamma(s)$ when $\mathrm{Re}(s) > -1$ as an analytic function except for a simple pole at $s = 0$ (since $\Gamma(s+1)$ at $s = 0$ has value $\Gamma(1) = 1$). Then using

$$\Gamma(s) = \frac{\Gamma(s+1)}{s} = \frac{\Gamma(s+2)}{s(s+1)}$$

we can use the last expression on the right to define $\Gamma(s)$ when $\mathrm{Re}(s) > -2$ as an analytic function except for simple poles at $s = 0$ and -1 (the numerator at $s = -1$ has value $\Gamma(1) = 1$). Iterating this, we eventually get $\Gamma(s)$ defined on all of $\mathbb{C}$ as an analytic function except for simple poles at the integers $0, -1, -2, -3, \ldots$. □

To show the Gamma function has no zeros, we can use the following result, called the reflection formula.

Theorem 2.4.4. *For all $s \in \mathbb{C}$,*

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

In particular, $\Gamma(1/2) = \sqrt{\pi}$.

Proof. Since both sides of the identity are meromorphic, it suffices to prove it on a nonempty open subset of $\mathbb{C}$. A proof for s in the strip $0 < \sigma < 1$, where $\Gamma(s)$ and $\Gamma(1-s)$ are both expressible as integrals, is in [10, Prop. 8.8] and [17, Theorem 1.4, Chapter 6]. At $s = 1/2$ the reflection formula becomes $\Gamma(1/2)^2 = \pi$, so $\Gamma(1/2) = \sqrt{\pi}$ since $\Gamma(1/2)$ is positive by its definition as an integral at $s = 1/2$. □

Corollary 2.4.5. *The function $\Gamma(s)$ has no zeros.*

Proof. At positive integers n there is no zero since $\Gamma(n) > 0$ from its definition as an integral (or because we know the exact value is $(n-1)!$). At 0 and negative integers the Gamma function has poles.

If $s_0 \in \mathbb{C}$ is not an integer, then in the relation $\Gamma(s_0)\Gamma_(1 - s_0) = \pi/\sin(\pi s_0)$, the right side is finite and nonzero. So if $\Gamma(s)$ vanishes at s_0, the function $\Gamma(1-s)$ must have a pole at s_0. That means $1-s_0$ equals 0 or a negative integer, so $s_0 = 1-(1-s_0)$ must be a positive integer, which is a contradiction since s_0 is not an integer.

Thus $\Gamma(s)$ has no zeros. □

In later work we will need to compute logarithmic derivatives like $(\Gamma'/\Gamma)(s)$ and $(\zeta'/\zeta)(s)$ at negative numbers such as $-1/4$ and $-3/2$. While computer algebra packages ca n give us these values to as much accuracy as needed, we will express $(\Gamma'/\Gamma)(s)$ and $(\zeta'/\zeta)(s)$ at such negative numbers in terms of $(\Gamma'/\Gamma)(s)$ and $(\zeta'/\zeta)(s)$ at positive numbers, where the logarithmic derivatives are absolutely convergent integrals or series (their original definitions, not needing analytic continuation on $\Gamma(s)$ or $\zeta(s)$).

Lemma 2.4.6. *The following identities hold for all $s \in \mathbb{C}$.*

$$\frac{\Gamma'}{\Gamma}(s+1) = \frac{\Gamma'}{\Gamma}(s) + \frac{1}{s}, \tag{2.4.1}$$

$$\frac{\Gamma'}{\Gamma}(s) = \frac{\Gamma'}{\Gamma}(1-s) - \pi\cot(\pi s), \tag{2.4.2}$$

$$\frac{\zeta'}{\zeta}(s) = \log(\pi) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1-s}{2}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) - \frac{\zeta'}{\zeta}(1-s), \tag{2.4.3}$$

$$\left(\frac{\zeta'}{\zeta}\right)'(s) = \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1-s}{2}\right) - \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{s}{2}\right) + \left(\frac{\zeta'}{\zeta}\right)'(1-s). \tag{2.4.4}$$

Proof. Equation (2.4.1) is the logarithmic derivative of the identity $\Gamma(s+1) = s\Gamma(s)$.

The logarithmic derivative of the identity $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$ is (2.4.2):

$$\frac{\Gamma'}{\Gamma}(s) - \frac{\Gamma'}{\Gamma}(1-s) = -\frac{\pi\cos(\pi s)}{\sin(\pi s)} = -\pi\cot(\pi s)$$

and bring $(\Gamma'/\Gamma)(1-s)$ to the right side.

To derive (2.4.3), we take the logarithmic derivative of the functional equation for the completed zeta-function $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$:

$$Z(s) = Z(1-s) \Longrightarrow \frac{Z'}{Z}(s) = -\frac{Z'}{Z}(1-s)$$

and in expanded form this says (since logarithmic differentiation turns products into sums and $(a^s)'/(a^s) = \log a$ for $a > 0$)

$$-\frac{1}{2}\log(\pi) + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) + \frac{\zeta'}{\zeta}(s) = -\left(-\frac{1}{2}\log(\pi) + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1-s}{2}\right) + \frac{\zeta'}{\zeta}(1-s)\right).$$

Bringing all terms except $(\zeta'/\zeta)(s)$ over to the right side, we get (2.4.3).

Equation (2.4.4) follows from (2.4.3) by differentiating both sides. □

Chapter 3

Dirichlet L-functions

In this chapter we will generalize the Riemann zeta-function by defining new Dirichlet series that are called L-functions of Dirichlet characters, or Dirichlet L-functions. They have many properties analogous to those of the zeta-function: a defining Dirichlet series, an Euler product when $\mathrm{Re}(s) > 1$, and a completed L-function formed by multiplication of the Dirichlet L-function by an exponential and Gamma factor. The completed L-function has an analytic continuation and functional equation and is expected to satisfy an analogue of the Riemann Hypothesis that is called the Generalized Riemann Hypothesis. In contrast to $\zeta(s)$, Dirichlet L-functions (other those those that are nearly equal to $\zeta(s)$) don't have poles: they are entire functions.

3.1 Dirichlet characters

An *arithmetic function* is a complex-valued function $a : \mathbb{Z}^+ \to \mathbb{C}$ on the positive integers. *Totally multiplicative* and *multiplicative* arithmetic functions are those that satisfy $a(mn) = a(m)a(n)$ for all $m, n \in \mathbb{Z}^+$ or just for co-prime m, n respectively.

One of the most well-known multiplicative functions to students of number theory is Euler's totient function $\varphi(n)$, which counts the number of positive integers up to n that are relatively prime to n (or the number of units in $(\mathbb{Z}/n\mathbb{Z})^\times$). The von Mangoldt function $\Lambda(n)$ is an example of an arithmetic function that is not multiplicative.

For any arithmetic function, we can form its Dirichlet series $\sum_{n\geq 1} a(n)/n^s$. As long as the sequence $a(n)$ does not grow too quickly, the Dirichlet series will converge absolutely on a right half-plane: if $|a(n)| = O(n^c)$ then the Dirichlet series is absolutely convergent when $\mathrm{Re}(s) > c + 1$. For totally multiplicative functions $a(n)$ where $|a(n)| \leq 1$ for all n (in practice here, $|a(n)|$ will be 0 or 1 for all n), there is an analogue of the Euler product for $\zeta(s)$:

$$\sum_{n\geq 1} \frac{a(n)}{n^s} = \prod_p \frac{1}{1 - a(p)/p^s} \tag{3.1.1}$$

for $\mathrm{Re}(s) > 1$. and reordering terms in the sum and product does not affect the value by Theorem 2.3.1.

Here are the particular arithmetic functions we will use in this thesis.

Definition 3.1.1. A *Dirichlet character* (mod m) is a function $\chi_m : (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$ that is a group homomorphism from the units modulo m to the unit circle.

We can turn χ_m into a function on $\mathbb{Z}$ by setting $\chi_m(n) = \chi_m(n \bmod m)$ when $(n, m) = 1$ and $\chi_m(n) = 0$ when $(n, m) > 1$. Then $\chi_m(nn') = \chi_m(n)\chi_m(n')$ for all integers n and n', so χ_m is totally multiplicative as a function on $\mathbb{Z}$.

Example 3.1.2. Define $\chi_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to S^1$ by $\chi_4(1) = 1$ and $\chi_4(3) = -1$. These are all the units modulo 4. We lift this to a function on $\mathbb{Z}$ by setting

$$\chi_4(n) = \begin{cases} 1, & \text{if } n \equiv 1 \bmod 4, \\ -1, & \text{if } n \equiv 3 \bmod 4, \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

Example 3.1.3. Define $\chi_5 : (\mathbb{Z}/5\mathbb{Z})^\times \to S^1$ as in the table below.

a	1	2	3	4
$\chi_5(a)$	1	i	$-i$	-1

This is a homomorphism since 2 generates the group $(\mathbb{Z}/5\mathbb{Z})^\times$, of order 4, and we set $\chi_5(2^k \bmod 5) = i^k$. We can lift χ_5 to a function on $\mathbb{Z}$ by setting $\chi_5(n) = \chi_5(n \bmod 5)$ when $5 \nmid n$ and $\chi_5(n) = 0$ when $5 \mid n$.

Example 3.1.4. For an odd prime p, the Legendre symbol is a Dirichlet character $\chi_p \colon (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, where for $n \not\equiv 0 \bmod p$,

$$\chi_p(n \bmod p) = \left(\frac{n}{p}\right) = \begin{cases} 1, & \text{if } n \text{ is a nonzero square modulo } p, \\ -1, & \text{if } n \text{ is a nonsquare modulo } p. \end{cases}$$

That this is a homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ is the well-known multiplicativity of the Legendre symbol: $(\frac{nn'}{p}) = (\frac{n}{p})(\frac{n'}{p})$. Lift the Legendre symbol to all of $\mathbb{Z}$ in a similar way as the previous examples, so $\chi_p(n) = 0$ if $p \mid n$.

Example 3.1.5. For each modulus $m \geq 2$ we have a *trivial character* mod m, denoted $\mathbf{1}_m$, where $\mathbf{1}_m(n \bmod m) = 1$ when $(n, m) = 1$. As a function on $\mathbb{Z}$, $\mathbf{1}_m(n) = 1$ if $(n, m) = 1$ and $\mathbf{1}_m(n) = 0$ if $(n, m) > 1$. We will allow a trivial character mod 1 too: $\mathbf{1}_1(n) = 1$ for all integers n.

To each Dirichlet character χ we can associate a Dirichlet series by viewing χ as a function on $\mathbb{Z}^+$ and using $\chi(n)$ as the coefficient in the nth term of the series. These are called Dirichlet L-functions.

Definition 3.1.6. For a Dirichlet character χ, the *Dirichlet L-function* $L(s,\chi)$ is defined for $\mathrm{Re}(s) > 1$ as

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

Example 3.1.7. The L-function of χ_4 is

$$L(s,\chi_4) = \sum_{n\geq 1} \frac{\chi_4(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \cdots .$$

For real s this is an alternating series, so the series converges for real $s > 0$ and thus for complex s with $\mathrm{Re}(s) > 0$ (Remark 2.2.3). More generally, it can be shown that the series $L(s,\chi)$ for every nontrivial χ converges for $\mathrm{Re}(s) > 0$. The half-plane of absolute convergence is $\mathrm{Re}(s) > 1$, as with the Riemann zeta-function.

Example 3.1.8. For $m \geq 1$, the L-function of the trivial character $\mathbf{1}_m$ is

$$L(s,\mathbf{1}_m) = \sum_{\substack{n\geq 1\\ (n,m)=1}} \frac{1}{n^s}.$$

In particular, $L(s,\mathbf{1}_1) = \zeta(s)$. The series $L(s,\mathbf{1}_m)$ looks like $\zeta(s)$ but it is missing terms at n where $(n,m) > 1$. For example,

$$L(s,\mathbf{1}_4) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots .$$

By Theorem 2.3.1, $L(s,\chi)$ has an Euler product for $\mathrm{Re}(s) > 1$:

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)/p^s}.$$

In the case of the trivial character mod m, this becomes the Euler product for $\zeta(s)$ with factors at primes dividing m missing (or we can say those factors equal 1):

$$L(s,\mathbf{1}_m) = \prod_p \frac{1}{1-\mathbf{1}_m(p)/p^s} = \prod_{p\nmid m} \frac{1}{1-1/p^s}. \tag{3.1.2}$$

Dirichlet L-functions were first defined and studied by Dirichlet in order to prove the following theorem.

Theorem 3.1.9 (Dirichlet, 1837)**.** *For integers a and m with $(a,m) = 1$, infinitely many primes p satisfy $p \equiv a \bmod m$.*

Proof. See [16]. In the proof, the key analytic input about Dirichlet L-functions is that $L(1,\chi) \neq 0$ for nontrivial χ. □

3.2 Primitive characters

For each m, there can be many Dirichlet characters mod m. In fact, there are exactly $\varphi(m)$ Dirichlet characters mod m, so when $m > 2$ there is always a nontrivial character, and when $m \neq 1,2,3,4,6$ there is more than one nontrivial character since $\varphi(m) > 2$.

Example 3.2.1. The four Dirichlet characters mod 5 are $\mathbf{1}_5$, χ_5 (see Example 3.1.3), the complex conjugate $\overline{\chi_5}$, and the Legendre symbol $(\frac{\cdot}{5})$. The table below shows all of their values on $(\mathbb{Z}/5\mathbb{Z})^\times$.

a	1	2	3	4
$\mathbf{1}_5(a)$	1	1	1	1
$\chi_5(a)$	1	i	$-i$	-1
$\overline{\chi_5}(a)$	1	$-i$	i	-1
$\left(\frac{a}{5}\right)$	1	-1	-1	1

In order to formulate an analytic continuation and especially functional equation for a Dirichlet L-function $L(s, \chi)$, we need to focus on a particular type of Dirichlet character called a primitive character. These will have a rather technical-sounding definition, but the basic point is that the these Dirichlet characters χ will turn out to have two good properties:

- χ is defined for the "right" modulus (not one that is too big),
- there are no "missing" factors in the Euler product of $L(s, \chi)$.

For example, in (3.1.2) we see that $L(s, \mathbf{1}_m)$ for $m > 1$ is missing Euler factors at primes p that divide m. The "best" trivial character is the one with modulus 1, which is identically 1 on all positive integers: the L-function of $\mathbf{1}_1$ is $\zeta(s)$.

Definition 3.2.2. Let $d \mid m$. A Dirichlet character χ modulo m is said to be *lifted* from modulus d if χ is a composition of group homomorphisms

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\text{redn.}} (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\chi'} S^1,$$

where the first mapping is reduction of units from modulus m to modulus d and the second mapping is a Dirichlet character modulo d.

In this definition, when we lift χ and χ' to functions on $\mathbb{Z}$, they have the same nonzero values on integers relatively prime to m. So the only difference between χ and χ' as functions on $\mathbb{Z}$ is that χ' might be nonzero sometimes where χ is 0 (at integers relatively prime to d that are not relatively prime to m). We'll see examples of this below.

Definition 3.2.3. A Dirichlet character χ modulo m is called *primitive* if, for each proper divisor d of m, χ can't be lifted from modulus d.

Example 3.2.4. The character χ_4 is primitive since the only characters mod 2 and mod 1 are trivial, while χ_4 is nontrivial (it has values other than 1 on $(\mathbb{Z}/4\mathbb{Z})^\times$), so χ_4 can't be lifted from modulus 1 or 2.

If we compose $\chi_4\colon (\mathbb{Z}/4\mathbb{Z})^\times \to S^1$ with reduction from modulus 8 and modulus 12 to modulus 4 then we get nonprimitive characters χ_8 mod 8 and χ_{12} mod 12, as shown in the table below.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\chi_4(a)$	1	0	-1	0	1	0	-1	0	1	0	-1	0
$\chi_8(a)$	1	0	-1	0	1	0	-1	0	1	0	-1	0
$\chi_{12}(a)$	1	0	0	0	1	0	-1	0	0	0	-1	0

Notice χ_8 is the same function on $\mathbb{Z}^+$ as χ_4. That is because an integer is relatively prime to 8 if and only if it is relatively prime to 4. The character χ_{12} agrees with χ_4 at positive integers that are relatively prime to 12, but χ_{12} is zero at the multiples of 3 and χ_4 is sometimes 0 and sometimes not 0 at multiples of 3. This is a general result — the lift of character to a larger modulus is the same function on $\mathbb{Z}$ except perhaps at some integers where the original character is not 0 and the lifted character is 0.

Example 3.2.5. For a prime p, each nontrivial character mod p is primitive. The trivial character mod p is not primitive. More generally, $\mathbf{1}_m$ is not primitive when $m > 1$.

When Dirichlet characters are collected together from being lifts of a common Dirichlet character, there is always one character in a collection that, as a function on $\mathbb{Z}$, is zero as little as possible. The character that on $\mathbb{Z}$ is zero as little as possible is a primitive character and the rest are not.

We look at how primitivity of a character affects the L-function of the character. For each of the characters χ_4, χ_8, and χ_{12} above, here are the first few terms of the Dirichlet series for their L-functions:

$$\begin{aligned}
L(s,\chi_4) &= \sum_{n\geq 1} \frac{\chi_4(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \frac{1}{13^s} - \frac{1}{15^s} + \cdots \\
L(s,\chi_8) &= \sum_{n\geq 1} \frac{\chi_8(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \frac{1}{13^s} - \frac{1}{15^s} + \cdots \\
L(s,\chi_{12}) &= \sum_{n\geq 1} \frac{\chi_{12}(n)}{n^s} = 1 + \frac{1}{5^s} - \frac{1}{7^s} - \frac{1}{11^s} + \frac{1}{13^s} + \cdots .
\end{aligned}$$

As we see from the fact that $\chi_4 = \chi_8$ as functions on $\mathbb{Z}^+$, their L-functions match completely. More generally, if χ is a nontrivial primitive character modulo a prime power $p^k > 1$, each lift of it to a character modulo a higher power of p has exactly the same L-function.

On the other hand, $L(s,\chi_{12})$ is missing terms where $\chi_{12}(n) = 0$ but $\chi_4(n) \neq 0$ (i.e., the odd multiples of 3). This has an effect on the Euler product. We see from

Theorem 2.3.1 that the L-function of the primitive character χ_4 is

$$L(s,\chi_4) = \prod_p \frac{1}{1-\chi_4(p)/p^s} = \left(\frac{1}{1+1/3^s}\right)\left(\frac{1}{1-1/5^s}\right)\left(\frac{1}{1+1/7^s}\right)\left(\frac{1}{1+1/11^s}\right)\cdots .$$

while the Euler product of $L(s,\chi_{12})$ is the same except it is missing the factor at 3:

$$L(s,\chi_{12}) = \prod_p \frac{1}{1-\chi_{12}(p)/p^s} = \left(\frac{1}{1-1/5^s}\right)\left(\frac{1}{1+1/7^s}\right)\left(\frac{1}{1+1/11^s}\right)\cdots .$$

What this is showing is that L-functions of nonprimitive characters may sometimes be missing Euler factors. This has an effect on the analytic continuation that we discuss later.

The Euler product of $L(s,\chi)$ allows us to write $-L'(s,\chi)/L(s,\chi)$ as a Dirichlet series in a similar way to that of $-\zeta'(s)/\zeta(s)$ in (2.2.2): for $\mathrm{Re}(s) > 1$,

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n\geq 1}\frac{\chi(n)\Lambda(n)}{n^s} = \sum_{p^k}\frac{\chi(p^k)\log p}{p^{ks}}.$$

Here, $\Lambda(n)$ is the von Mangoldt function from Definition 2.2.7. We can think of the terms in this series as a "twisting" by χ of the terms of the series for $-\zeta'(s)/\zeta(s)$, which means each term in the series for $-\zeta'(s)/\zeta(s)$ is multiplied by a value of χ.

The function $\zeta(s)$ has a completed function $Z(s)$ with a nice functional equation. It turns out that Dirichlet L-functions of all primitive characters have a completed L-function with a nice functional equation (note $\zeta(s) = L(s,\mathbf{1}_1)$ and $\mathbf{1}_1$ is primitive), and having a nice functional equation is the reason primitivity of a character matters. In order to describe the functional equation we will use a particular "character sum".

Definition 3.2.6. For a Dirichlet character χ modulo m, its *Gauss sum* is

$$G(\chi) := \sum_{j\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(j)e^{2\pi ij/m}. = \sum_{j=0}^{m-1} \chi(j)e^{2\pi ij/m}.$$

The sum can extend over all integers from 0 to $m-1$ since $\chi(j) = 0$ if $(j, m) > 1$.

When $\chi \bmod m$ is primitive, it turns out that $|G(\chi)| = \sqrt{m}$ [1, Theorems 8.11, 8.19], and this is always false if $\chi \bmod m$ is not primitive: $|G(\chi)| < \sqrt{m}$. We may even have $G(\chi) = 0$.

Example 3.2.7. Let's look at the Gauss sums of χ_4, χ_8, and χ_{12}:

$$\begin{aligned}
G(\chi_4) &= \chi_4(1)e^{2\pi i/4} + \chi_4(3)e^{3\cdot 2\pi i/4)} \\
&= (1)i + (-1)(-i) \\
&= 2i, \\
G(\chi_8) &= \chi_8(1)e^{2\pi i/8} + \chi_8(3)e^{3\cdot 2\pi i/8)} + \chi_8(5)e^{5\cdot 2\pi i/8} + \chi_8(7)e^{7\cdot 2\pi i/8} \\
&= \frac{1+i}{\sqrt{2}} + (-1)\cdot\frac{-1+i}{\sqrt{2}} + 1\cdot\frac{-1-i}{\sqrt{2}} + (-1)\cdot\frac{1-i}{\sqrt{2}} \\
&= 0, \\
G(\chi_{12}) &= \chi_{12}(1)e^{2\pi i/12} + \chi_{12}(5)e^{5\cdot 2\pi i/12} + \chi_{12}(7)e^{7\cdot 2\pi i/12} + \chi_{12}(11)e^{11\cdot 2\pi i/12} \\
&= e^{\pi i/6} + e^{5\pi i/6} - e^{7\pi i/6} - e^{11\pi i/6} \\
&= 2(e^{\pi i/6} + e^{5\pi i/6}) \\
&= 2i.
\end{aligned}$$

So $|G(\chi_4)| = 2 = \sqrt{4}$, $|G(\chi_8)| = 0$, and $|G(\chi_{12})| = 2 < \sqrt{12}$.

Example 3.2.8. The Gauss sums of χ_5 and $(\frac{\cdot}{5})$ in Example 3.2.1 are:

$$\begin{aligned}
G(\chi_5) &= \chi_5(1)e^{2\pi i/5} + \chi_5(2)e^{2\cdot 2\pi i/5} + \chi_5(3)e^{3\cdot 2\pi i/5} + \chi_5(4)e^{4\cdot 2\pi i/5} \\
&= e^{2\pi i/5} + ie^{4\pi i/5} - ie^{6\pi i/5} - e^{8\pi i/5} \\
&\approx -1.17557 + 1.90211i, \\
G\left(\left(\frac{\cdot}{5}\right)\right) &= \left(\frac{1}{5}\right) e^{2\pi i/5} + \left(\frac{2}{5}\right) e^{2\cdot 2\pi i/5} + \left(\frac{3}{5}\right) e^{3\cdot 2\pi i/5} + \left(\frac{4}{5}\right))e^{4\cdot 2\pi i/5} \\
&= e^{2\pi i/5} - e^{4\pi i/5} - e^{6\pi i/5} + e^{8\pi i/5} \\
&= \sqrt{5}.
\end{aligned}$$

The absolute value of $G(\chi_5)$ is precisely $\sqrt{5}$.

3.3 Analytic continuation and the completed L-function

For each Dirichlet character χ, we know $\chi(-1) = \pm 1$ since $\chi(-1)^2 = \chi(1) = 1$. We call χ *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$. This corresponds to χ being an even or odd function since $\chi(-n) = \chi(-1)\chi(n)$. It turns out that the parity of χ (whether it is even or odd) affects the additional factors we multiply $L(s, \chi)$ by to get a function with an analytic continuation and nice functional equation. Notationally, for a character χ, define δ to be the integer in $\{0, 1\}$ such that $\chi(-1) = (-1)^\delta$.

Definition 3.3.1. For a primitive Dirichlet character $\chi \bmod m$, the *completed L-function* for χ is

$$\Lambda(s, \chi) = \left(\frac{\pi}{m}\right)^{-(s+\delta)/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi). \tag{3.3.1}$$

for $\mathrm{Re}(s) > 1$.

This use of Λ has nothing to do with the von Mangoldt function $\Lambda(n)$. It will be obvious from context what “Λ” means.

Notice that in the definition of $\Lambda(s, \chi)$ we need δ to be the integer 0 or 1, not just 0 or 1 as an integer mod 2 (which would be good enough for saying $\chi(-1) = (-1)^{\delta}$), since δ is being used in the functions $(\pi/m)^{-(s+\delta)/2}$ and $\Gamma((s + \delta)/2)$.

Example 3.3.2. For the primitive character $\mathbf{1}_1$, $m = 1$ and $\delta = 0$. Then $L(s, \mathbf{1}_1) = \zeta(s)$ and $\Lambda(s, \mathbf{1}_1) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, which is the completed zeta-function $Z(s)$.

Example 3.3.3. For the primitive character χ_4, $m = 4$. Since $\chi_4(-1) = \chi_4(3) = -1$, $\delta = 1$. Therefore

$$\Lambda(s, \chi_4) = \left(\frac{\pi}{4}\right)^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) L(s, \chi_4).$$

Example 3.3.4. Nontrivial characters mod 5 are primitive. For the characters χ_5 and $(\frac{\cdot}{5})$ in Example 3.2.1, $\chi_5(-1) = \chi_5(4) = -1$ and $(\frac{-1}{5}) = (\frac{4}{5}) = 1$, so χ_5 has $\delta = 1$ and $(\frac{\cdot}{5})$ has $\delta = 0$. Therefore

$$\begin{aligned} \Lambda(s, \chi_5) &= \left(\frac{\pi}{5}\right)^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) L(s, \chi_5), \\ \Lambda\left(s, \left(\frac{\cdot}{5}\right)\right) &= \left(\frac{\pi}{5}\right)^{-s/2} \Gamma\left(\frac{s}{2}\right) L\left(s, \left(\frac{\cdot}{5}\right)\right). \end{aligned}$$

The completed L-function of a primitive Dirichlet character χ has an analytic continuation and functional equation, where the functional equation involves the completed L-function of the conjugate character $\overline{\chi}$. It is straightforward to see that $\overline{\chi}$ is primitive when χ is, as otherwise χ could be lifted from the conjugate of the character

$\overline{\chi}$ is lifted from.

Theorem 3.3.5. *If* $\chi \bmod m$ *is primitive and* $m > 1$ *then* $\Lambda(s, \chi)$ *is an entire function and satisfies the functional equation*

$$\Lambda(1 - s, \chi) = W(\chi)\Lambda(s, \overline{\chi}), \tag{3.3.2}$$

where $W(\chi) = G(\chi)/(i^{\delta}\sqrt{m})$ *is a complex number of absolute value* 1*.*

Saying $|W(\chi)| = 1$ is equivalent to saying $|G(\chi)| = \sqrt{m}$ for primitive $\chi \bmod m$, a property of primitive Dirichlet characters that we mentioned before.

Proof. See [10, Prop. 8.11]. This is done by a method similar to that for $Z(s)$: write $\Lambda(s, \chi)$ as an integral over $(0, \infty)$, split up the integral into $(0, 1]$ and $[1, \infty)$, and use a change of variables and a "twisted" version of the Poisson summation formula to write $\Lambda(s, \chi)$ as an integral over $[1, \infty)$ that is analogous to (1.2.4) and satisfies the functional equation (3.3.2). The terms that would be analogous to $-1/s$ and $-1/(1 - s)$ from (1.2.4) don't appear since $\chi(0) = 0$ when χ is a nontrivial primitive character, in contrast to $\mathbf{1}_1(0) = 1$. □

Corollary 3.3.6. *If* $\chi \bmod m$ *is primitive and* $m > 1$ *then* $L(s, \chi)$ *is an entire function.*

Proof. For $\mathrm{Re}(s) > 1$, solving for $L(s, \chi)$ in (3.3.1) tells us

$$L(s, \chi) = \left(\frac{\pi}{m}\right)^{(s+\delta)/2} \frac{1}{\Gamma((s + \delta)/2)} \Lambda(s, \chi), \tag{3.3.3}$$

and the right side is an entire function since each of the three factors is an entire function. Therefore (3.3.3) shows us $L(s, \chi)$ extends analytically to all of $\mathbb{C}$. □

We could show $L(s,\chi)$ is analytic for $\mathrm{Re}(s) > 0$ without using $\Lambda(s,\chi)$: the initial Dirichlet series definition of $L(s,\chi)$ when $\mathrm{Re}(s) > 1$ converges conditionally for $0 < \mathrm{Re}(s) \leq 1$ and therefore is analytic there.

Unlike $\zeta(s)$, $L(s,\chi)$ for nontrivial primitive χ has no pole.

Example 3.3.7. The function $\Lambda(s,\chi_4)$ satisfies $\Lambda(1-s,\chi_4) = W(\chi_4)\Lambda(s,\overline{\chi_4})$ where $W(\chi_4) = G(\chi_4)/(i\sqrt{4}) = 2i/(2i) = 1$ and $\Lambda(s,\overline{\chi_4}) = \Lambda(s,\chi_4)$ since $\overline{\chi_4} = \chi_4$. Thus the functional equation for $\Lambda(s,\chi_4)$ becomes

$$\Lambda(1-s,\chi_4) = \Lambda(s,\chi_4), \tag{3.3.4}$$

which looks like the one for the completed zeta-function $Z(s)$. The first few nontrivial zeros of $\Lambda(s,\chi_4)$ in the upper half-plane are on the critical line $\mathrm{Re}(s) = 1/2$ and they are approximately

$$\frac{1}{2} + 6.02095i, \quad \frac{1}{2} + 10.24377, \quad \text{and} \quad \frac{1}{2} + 12.98810i.$$

The LMFDB page https://www.lmfdb.org/L/1/2e2/4.3/r1/0/0 has approximations to further zeros.

Example 3.3.8. We consider the L-function for χ_5:

$$L(s,\chi_5) = \sum_{n\geq 0} \frac{\chi_5(n)}{n^s} = \frac{1}{1^s} + \frac{i}{2^s} - \frac{i}{3^s} - \frac{1}{4^s} + \cdots.$$

This character is primitive, so it satisfies

$$\Lambda(1-s,\chi_5) = W(\chi_5)\Lambda(s,\overline{\chi_5}),$$

where $W(\chi_5) = G(\chi_5)/(i\sqrt{5})$ and $|W(\chi_5)| = 1$. Approximations to the initial zeros of $\Lambda(s, \chi_5)$ are on the LMFDB page https://www.lmfdb.org/L/1/5/5.2/r1/0/0.

The L-function of a primitive Dirichlet character has an ugly functional equation that is analogous to the one for $\zeta(s)$ in Theorem 1.2.3.

Theorem 3.3.9. *For a primitive Dirichlet character* $\chi \bmod m$*,*

$$L(1-s, \chi) = \frac{2W(\chi)}{\sqrt{m}} \left(\frac{2\pi}{m}\right)^{-s} \Gamma(s) \cos\left(\frac{\pi}{2}(s-\delta)\right) L(s, \overline{\chi}).$$

Proof. When $\chi = \mathbf{1}_1$, so $L(s, \chi) = \zeta(s)$, we have $m = 1$ and $\delta = 0$, and the formula in the theorem is precisely the ugly functional equation for $\zeta(s)$. When $m > 1$, solve for $L(1-s, \chi)$ in (3.3.2) and use the Gamma function identities from the proof of Theorem 1.2.3. □

There are analogues of Theorems 1.2.4, 1.2.5, and 1.2.6 about the location of zeros of $\Lambda(s, \chi)$ and $L(s, \chi)$.

Theorem 3.3.10. *For nontrivial primitive* χ*, the function* $\Lambda(s, \chi)$ *is nonvanishing for* $\text{Re}(s) > 1$ *and* $\text{Re}(s) < 0$*.*

Proof. For $\text{Re}(s) > 1$, $L(s, \chi) \neq 0$ by the Euler product. Additionally, the π and Gamma factors in $\Lambda(s, \chi)$ do not vanish in this half-plane, so $\Lambda(s, \chi) \neq 0$ when $\text{Re}(s) > 1$. For $\text{Re}(s) < 0$, $\Lambda(s, \chi) = W(\chi)\Lambda(1-s, \overline{\chi})$ and $\text{Re}(1-s) > 1$. We have $\Lambda(1-s, \overline{\chi}) \neq 0$ when $\text{Re}(1-s) > 1$, and $|W(\chi)| = 1$, so $\Lambda(s, \chi) \neq 0$ when $\text{Re}(s) < 0$. □

So as with the completed zeta-function $Z(s)$, all zeros of $\Lambda(s, \chi)$ are in the critical strip $0 \leq \text{Re}(s) \leq 1$.

Theorem 3.3.11. *For nontrivial primitive χ, $L(s, \chi)$ has simple zeros at the negative even integers when χ is even and simple zeros at the negative odd integers when χ is odd. All of its other zeros satisfy $0 \leq \mathrm{Re}(s) \leq 1$.*

Proof. The function $L(s, \chi)$ is nonzero for $\mathrm{Re}(s) > 1$ by its Euler product. For $\mathrm{Re}(s) < 0$, $L(s, \chi)$ is described by (3.3.3), where the exponential term $(\pi/m)^{(s+\delta)/2}$ is nonvanishing on $\mathbb{C}$ and $\Lambda(s, \chi) \neq 0$ for $\mathrm{Re}(s) < 0$ by Theorem 3.3.10. Therefore zeros of $L(s, \chi)$ for $\mathrm{Re}(s) < 0$ come from $1/\Gamma((s + \delta)/2)$, which has simple zeros where $(s + \delta)/2)$ is 0 or a negative integer. That means $s = 0, -2, -4, -6, -8, \ldots$ when $\delta = 0$ and $s = -1, -3, -5, -7, -9, \ldots$ when $\delta = 1$. Ignoring $s = 0$, which is outside the half-plane $\mathrm{Re}(s) < 0$, we conclude that $L(s, \chi)$ for even nontrivial primitive χ has simple zeros at the negative even integers and $L(s, \chi)$ for odd primitive χ (always nontrivial) has simple zeros at the negative odd integers when $\mathrm{Re}(s) < 0$ □

Theorem 3.3.12. *For nontrivial primitive χ, the functions $\Lambda(s, \chi)$ and $L(s, \chi)$ are nonvanishing for $\mathrm{Re}(s) = 1$ and $\mathrm{Re}(s) = 0$ except $L(s, \chi)$ has a simple zero at $s = 0$ when χ is even. The zeros of $\Lambda(s, \chi)$ and $L(s, \chi)$ when $0 < \mathrm{Re}(s) < 1$ are at the same numbers and have the same multiplicity.*

Proof. First we treat $\mathrm{Re}(s) = 1$. The functions $(\pi/m)^{-(s+\delta)2/}$ and $\Gamma((s + \delta)/2)$ for $\delta = 0$ and 1 are analytic and nonvanishing when $\mathrm{Re}(s) = 1$, so the nonvanishing of $\Lambda(s, \chi)$ on this line follows from showing $L(s, \chi) \neq 0$ when $\mathrm{Re}(s) = 1$. As with the proof that $\zeta(s) \neq 0$ on $\mathrm{Re}(s) = 1$, the proof that $L(s, \chi) \neq 0$ on $\mathrm{Re}(s) = 1$ is by contradiction and uses a product of three functions built out of $L(s, \chi)$. Details are in [16, Theorem 4.2.3].

When $\mathrm{Re}(s) = 0$ we can show $\Lambda(s, \chi) \neq 0$ by using the functional equation in Theorem 3.3.5. For a primitive character χ, the number $W(\chi)$ in Theorem 3.3.5

is nonzero (in fact $|W(\chi)| = 1$). Therefore $\Lambda(s,\chi) \neq 0$ when $\mathrm{Re}(s) = 0$ because $\Lambda(s,\overline{\chi}) \neq 0$ when $\mathrm{Re}(s) = 1$ by the argument above with $\overline{\chi}$ in place of χ.

To determine where $L(s,\chi)$ is 0 on the line $\mathrm{Re}(s) = 0$, note $(\pi/m)^{-(s+\delta)2/}$ and $\Gamma((s+\delta)/2)$ are analytic and nonvanishing when $\mathrm{Re}(s) = 0$ except for $\Gamma(s/2)$ having a simple pole at $s = 0$. Therefore $\Lambda(s,\chi)$ being nonzero on $\mathrm{Re}(s) = 0$ implies $L(s,\chi) \neq 0$ for $\mathrm{Re}(s) = 0$ except perhaps at $s = 0$ by (3.3.3) if χ is even (and so $\delta = 0$). In this case, the term $1/\Gamma(s/2)$ in (3.3.3) gives $L(s,\chi)$ a simple zero at $s = 0$.

When $0 < \mathrm{Re}(s) < 1$, the zeros of $\Lambda(s,\chi)$ and $L(s,\chi)$ are at the same numbers with the same multiplicities because the terms $(\pi/m)^{(s+\delta)/2}$ and $1/\Gamma((s+\delta)/2)$ in (3.3.3) introduce no zeros or poles in this region. So the only zeros for $L(s,\chi)$ in this region come from $\Lambda(s,\chi)$, with the same multiplicity. □

For nontrivial primitive χ, zeros of $L(s,\chi)$ coming from poles of $1/\Gamma((s+\delta)/2)$ are called the *trivial zeros* of $L(s,\chi)$. By Theorems 3.3.11 and 3.3.12, the trivial zeros of $L(s,\chi)$ are

- 0 and negative even integers for even χ,
- negative odd integers for odd χ.

Notice $\zeta(s) = L(s,\mathbf{1}_1)$ does not have a zero at $s = 0$, which is a distinction between the trivial even primitive character $\mathbf{1}_1$ and all other primitive even characters. As with the zeta-function, the nontrivial zeros of $L(s,\chi)$ are the same thing (locations and their multiplicities) as the zeros of $\Lambda(s,\chi)$.

We are now ready to state a first form of the Generalized Riemann Hypothesis.

The *Generalized Riemann Hypothesis* states that, for all primitive Dirichlet characters χ, the nontrivial zeros of $L(s,\chi)$ have real part 1/2. Equivalently, all zeros of

$\Lambda(s, \chi)$ have real part 1/2.

This includes the Riemann Hypothesis for the zeta-function using the trivial primitive character $\mathbf{1}_1$.

Just as $\zeta(s)$ is known to have no real zeros in the critical strip (see Theorem 1.2.5), it is expected that all $L(s, \chi)$ have no real zeros in the critical strip, but this is still an unsolved problem in general. Specific examples can be checked, for instance, $L(s, \chi_4) \neq 0$ for $0 < s < 1$ since the the Dirichlet series representation of $L(s, \chi_4)$ for real $s > 0$ is an alternating series:

$$L(s, \chi_4) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \cdots .$$

This shows $L(s, \chi_4) \neq 0$ for real $s > 0$ since the value is positive.

By relating the L-function of each nonprimitive nontrivial character to the L-function of a primitive character, we can extend the analytic continuation of $L(s, \chi)$ in Corollary 3.3.6 to the nonprimitive case.

Theorem 3.3.13. *For all nontrivial Dirichlet characters χ, $L(s, \chi)$ extends analytically to $\mathbb{C}$ as an entire function.*

Proof. When χ is primitive this follows from Corollary 3.3.6.

When χ is nonprimitive, we will prove $L(s, \chi)$ is entire by relating it to the L-function of the primitive character that lifts to χ, which is already known to be entire. The basic point is that these two L-functions are related by removing a finite number of Euler factors, and that involves multiplication by very simple entire functions. This is best understood with an example.

In Section 3.2 we saw that the Euler product of the L-function of the nonprimitive character χ_{12} is the same as the L-function of the primitive character χ_4 except for a missing Euler factor at 3: for $\mathrm{Re}(s) > 1$,

$$\begin{aligned} L(s, \chi_{12}) &= \prod_p \frac{1}{1 - \chi_{12}(p)/p^s} \\ &= \left(\frac{1}{1 - 1/5^s}\right)\left(\frac{1}{1 + 1/7^s}\right)\left(\frac{1}{1 + 1/11^s}\right)\cdots \\ &= \left(1 + \frac{1}{3^s}\right) L(s, \chi_4) \\ &= \left(1 - \frac{\chi_4(3)}{3^s}\right) L(s, \chi_4). \end{aligned} \tag{3.3.5}$$

Since χ_4 is primitive, $L(s, \chi_4)$ is an entire function. The factor $1 + 1/3^s$ is also entire. Therefore (3.3.5) provides us with an analytic continuation of $L(s, \chi_{12})$ to $\mathbb{C}$.

For a general nonprimitive χ mod m, it is a lifting to modulus m of some primitive character χ' mod d, where $d \mid m$. We can express $L(s, \chi)$ in terms of $L(s, \chi')$ when $\mathrm{Re}(s) > 1$ by comparing their Euler products. Similar to (3.3.5),

$$L(s, \chi) = \prod_{p \in S} \left(1 - \frac{\chi'(p)}{p^s}\right) L(s, \chi'), \tag{3.3.6}$$

where S is the set of primes dividing m and not dividing d. That subset might be empty, for instance when $\chi = \chi_8$ ($m = 8$ and $d = 4$), but it is always finite and each factor $1 - \chi'(p)/p^s$ for $p \in S$ is entire. Also $L(s, \chi')$ is entire since χ' is primitive, so the right side of (3.3.6) is an analytic continuation of $L(s, \chi)$ to $\mathbb{C}$. □

Remark 3.3.14. In (3.3.6), the function $L(s, \chi')$ has no zeros on the imaginary axis except at $s = 0$ if χ' is even, but if $S \neq \emptyset$ then the factors $1 - \chi'(p)/p^s$ for $p \in S$ each have an infinite periodic set of zeros on the imaginary axis with period $2\pi i/\log p$ (these zeros are the s where $p^s = \chi'(p)$). So the L-function of a nonprimitive character χ sometimes reveals the nonprimitivity of χ through the presence of zeros on the imaginary axis other than at $s = 0$. But sometimes this does not happen, such as $L(s, \chi_8)$, which equals $L(s, \chi_4)$.

Theorem 3.3.15. *For the trivial Dirichlet character $\mathbf{1}_m$, $L(s, \mathbf{1}_m)$ extends analytically to $\mathbb{C}$ except for a simple pole at $s = 1$ with residue $\prod_{p|m}(1 - 1/p)$.*

Proof. For $\mathrm{Re}(s) > 1$, the Euler product for $L(s, \mathbf{1}_m)$ in (3.1.2) can be written as

$$L(s, \mathbf{1}_m) = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right) \zeta(s).$$

On the right side, $\zeta(s)$ is analytic on $\mathbb{C}$ except for a simple pole at $s = 1$ and each factor $1 - 1/p^s$ is analytic and is nonzero at $s = 1$, so the right side of the above formula gives an analytic continuation of $L(s, \mathbf{1}_m)$ to $\mathbb{C}$ except for a simple pole at $s = 1$ with residue $\prod_{p|m}(1 - 1/p)$. □

While $\zeta(s)$ has no zeros on the imaginary axis, $L(s, \mathbf{1}_m)$ for $m > 1$ has infinitely many zeros there: they are the zeros of $1 - 1/p^s$ for primes p dividing m.

We are now ready to state a second form of the Generalized Riemann Hypothesis, where the restriction to primitive characters is dropped by focusing on the interior of the critical strip.

The *Generalized Riemann Hypothesis* states that, for all Dirichlet characters χ, the zeros of $L(s, \chi)$ with $0 < \mathrm{Re}(s) < 1$ have real part $1/2$.

This second form is equivalent to the first form because the only way zeros of $L(s, \chi)$ might occur on the boundary has a simple explanation:

- a zero of $L(s, \chi)$ at $s = 0$ for nontrivial even χ,

- zeros from a reciprocal Euler factors $1 - \chi'(p)/p^s$ where χ' is the primitive character that lifts to χ and p is a prime where $\chi'(p) \neq 0$ and $\chi(p) = 0$.

We defined $\Lambda(s,\chi)$ only when χ is primitive, but for a nontrivial Dirichlet character χ that is not primitive, the definition of $\Lambda(s,\chi)$ makes sense and both sides of the functional equation from the primitive case make sense since $L(s,\chi)$ is an entire function for all nontrivial χ. However, the functional equation from the primitive case is simply wrong when χ is not primitive. Here are two examples.

Example 3.3.16. Set $\Lambda(s,\chi_8) := (\pi/8)^{-(s+1)/2}\Gamma((s+1)/2)L(s,\chi_8)$, since χ_8 is defined on $(\mathbb{Z}/8\mathbb{Z})^\times$ and $\chi_8(-1) = \chi_4(-1) = -1$. We don't have a functional equation $\Lambda(1-s,\chi_8) = W(\chi_8)\Lambda(s,\overline{\chi_8})$ since $W(\chi_8) = 0$ and the left side is not identically 0. Instead,

$$\begin{aligned}
\Lambda(s,\chi_8) &:= \left(\frac{\pi}{8}\right)^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi_8)\\
&= \left(\frac{1}{2}\right)^{-(s+1)/2}\left(\frac{\pi}{4}\right)^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi_4)\\
&= 2^{(s+1)/2}\Lambda(s,\chi_4),
\end{aligned}$$

so by the functional equation for $\Lambda(s,\chi_4)$ in (3.3.4),

$$\Lambda(s,\chi_8) = 2^{(s+1)/2}\Lambda(1-s,\chi_4) = 2^{(s+1)/2}\frac{\Lambda(1-s,\chi_8)}{2^{(1-s+1)/2}} = 2^{s-1/2}\Lambda(1-s,\chi_8). \quad (3.3.7)$$

This has an extra factor $2^{s-1/2}$ due to using the wrong modulus for the character: the 8 instead of 4 led to $\pi/8$ instead of $\pi/4$ when defining $\Lambda(s,\chi_8)$ to complete the Dirichlet L-function $L(s,\chi_8) = L(s,\chi_4)$.

Example 3.3.17. Set $\Lambda(s,\chi_{12}) := (\pi/12)^{-(s+1)/2}\Gamma((s+1)/2)L(s,\chi_{12})$ since χ_{12} is defined on $(\mathbb{Z}/12\mathbb{Z})^\times$ and $\chi_{12}(-1) = \chi_4(-1) = -1$. Then

$$\begin{aligned}
\Lambda(s,\chi_{12}) &= \left(\frac{\pi}{12}\right)^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) L(s,\chi_{12}) \\
&= \left(\frac{1}{3}\right)^{-(s+1)/2} \left(\frac{\pi}{4}\right)^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) \left(1+\frac{1}{3^s}\right) L(s,\chi_4) \text{ by (3.3.5)} \\
&= 3^{(s+1)/2}\left(1+\frac{1}{3^s}\right)\Lambda(s,\chi_4). \qquad (3.3.8) \\
&= 3^{(s+1)/2}\left(1+\frac{1}{3^s}\right)\Lambda(1-s,\chi_4) \text{ by (3.3.4)} \\
&= 3^{(s+1)/2}\left(1+\frac{1}{3^s}\right)\cdot\left[\frac{3^{-((1-s+1)/2)}}{1+1/3^{1-s}}\Lambda(1-s,\chi_{12})\right] \text{ by (3.3.8)} \\
&= 3^{s-1/2}\frac{1+1/3^s}{1+1/3^{1-s}}\Lambda(1-s,\chi_{12}). \qquad (3.3.9)
\end{aligned}$$

The $3^{s-1/2}$ in (3.3.9) is analogous to the $2^{s-1/2}$ in (3.3.7) (using the wrong modulus 12 instead of 4 for the character) and the ratio in (3.3.9) is due to the missing Euler factor $1/(1+1/3^s)$ in $L(s,\chi_{12})$ compared to $L(s,\chi_4)$.

Similarly to how there is a Hadamard factorization for $s(s-1)Z(s)$ in Theorem 2.3.4, there is a similar factorization for $\Lambda(s,\chi)$ for nontrivial primitive χ. Unlike $Z(s)$, which used multiplication by s and $s-1$ to become entire due to the simple poles at 0 and 1, $\Lambda(s,\chi)$ for nontrivial primitive χ is entire as is.

Theorem 3.3.18. *Let χ be a nontrivial primitive Dirichlet character. There is a Hadamard factorization of $\Lambda(s,\chi)$ of the form*

$$\Lambda(s,\chi) = e^{A+Bs}\prod_{\rho_\chi}\left(1-\frac{s}{\rho_\chi}\right)e^{s/\rho_\chi}$$

where $e^A = \Lambda(0,\chi)$ and $B \in \mathbb{C}$. Additionally, $\sum_{\rho_\chi} 1/|\rho_\chi|^{1+\varepsilon}$ converges for all $\varepsilon > 0$, where this sum is over the zeros of $\Lambda(s,\chi)$ counted with multiplicity.

Proof. The function $\Lambda(s,\chi)$ fits the growth hypotheses of Theorem 2.3.2 by [4, p. 82]. Therefore there are $A, B \in \mathbb{C}$ and $m \geq 0$ such that

$$\Lambda(s,\chi) = e^{A+Bs} s^m \prod_{\rho_\chi} \left(1 - \frac{s}{\rho_\chi}\right) e^{s/\rho_\chi}$$

Since $\Lambda(0,\chi) \neq 0$ (Theorem 3.3.12), $m = 0$ and $e^A = \Lambda(0,\chi)$. □

We can express e^A in the Hadamard product directly in terms of a Dirichlet L-function at $s = 1$ by using the functional equation of $\Lambda(s,\chi)$:

$$e^A = \Lambda(0,\chi) = W(\chi)\Lambda(1,\overline{\chi}) = W(\chi)\left(\frac{\pi}{m}\right)^{-(1+\delta)/2} \Gamma\left(\frac{1+\delta}{2}\right) L(1,\overline{\chi}).$$

Let's separately consider $\delta = 0$ and $\delta = 1$ to make e^A more explicit. When $\delta = 0$,

$$\begin{aligned} e^A &= W(\chi)\sqrt{\frac{m}{\pi}}\Gamma\left(\frac{1}{2}\right) L(1,\overline{\chi}) \\ &= \frac{G(\chi)}{\sqrt{m}}\frac{\sqrt{m}}{\sqrt{\pi}}\sqrt{\pi}L(1,\overline{\chi}) \text{ by Theorem 2.4.4} \\ &= G(\chi)L(1,\overline{\chi}). \end{aligned}$$

When $\delta = 1$,

$$\begin{aligned} e^A &= W(\chi)\left(\frac{m}{\pi}\right)\Gamma(1)L(1,\overline{\chi}) \\ &= \frac{G(\chi)}{i\sqrt{m}}\left(\frac{m}{\pi}\right) L(1,\overline{\chi}) \text{ since } \Gamma(1) = 1 \\ &= \frac{G(\chi)\sqrt{m}}{i\pi}\ L(1,\overline{\chi}). \end{aligned}$$

Chapter 4

Primality Tests

The distribution of the primes is interesting for its own sake, and the Riemann Hypothesis has applications to questions about primes besides an error term in the Prime Number Theorem. We will see in the next chapter how the Riemann Hypothesis and the Generalized Riemann Hypothesis can be applied to primality testing. In this chapter, we discuss some primality tests and how they are useful in computer science.

4.1 Cryptography and cryptosystems

We give a brief overview of some concepts in cryptography. A good general reference on the subject is [7].

Cryptography is the study of exchanging messages secretly. Until the availability of computers in the second half of the 20th century, implementing a cryptosystem may have involved parties sharing code words in advance in order to encrypt communications. The security of a cryptosystem was regarded as depending on keeping the code words for encryption hidden from adversaries, as knowledge of how to encrypt made it very easy to decrypt. This is similar to how a permutation or matrix easily determines and is determined by its inverse. An encryption process where knowledge of how to encrypt makes it easy to decrypt is called symmetric.

Today, the security of a cryptosystem is no longer measured in part by keeping the overall process of encryption unknown to others. To the contrary, we are in the era of public-key cryptography, where all parties can send an encrypted message to someone (like a computer or phone sending a customer's PIN code to a credit card company or bank) using a public key and procedure made available to all, while decryption depends on a private key known only to the receiver of the encrypted messages. Public-key cryptography is necessary for most of the secure internet to function, from sending end-to-end encrypted messages on various applications to safely inputting passwords on websites. Old-fashioned symmetric encryption still runs far faster than public-key (asymmetric) encryption, so in practice both systems are used together: an initial public-key encrypted message is often sent that generates a secret key for a symmetric encryption process.

What is used to make modern cryptosystems secure (we hope) is apparently "hard" mathematical problems as the tool for encryption. Vastly oversimplifying, public-key cryptography relies on "trapdoor" or one-way functions. Such functions are easy or efficient to compute in one direction, but appear to be hard to compute in the other direction without some extra information. A basic example of a one-way function is multiplying compared to factoring. Or rather multiplication appears to be a one-way function. There is no actual proof that factoring is hard, and in fact there is no actual proved example of a one-way function. But there are many candidates.

The (apparent) one-way functions used in modern cryptography often depend on large prime numbers. An example of this is the RSA cryptosystem, named after its discoverers Rivest, Shamir, and Adleman. RSA is one of the most successful and commonly used public-key cryptography protocols. The difficult problem its security is based on is not factoring of general numbers, but factoring of numbers that are a product of two large primes of approximately the same size (bit length). Some specific assumptions related to this problem are in [7, Section 7.2].

Here is a broad overview of how RSA works, before formally defining it. The goal is to transmit a plaintext message m from one party to another securely as an encoded message c, called the ciphertext. At the receiving end, the ciphertext has to be decrypted to reveal m. The whole process depends on an initial choice of two different primes p and q. Set $N = pq$, so $\varphi(N) = (p-1)(q-1)$. The primes p and q will no longer play roles individually, but only through the derived numbers N and $\varphi(N)$. We need an integer e, called the encryption exponent, that is invertible modulo $\varphi(N)$. All plaintext messages need to be expressed as numbers from 0 to $N-1$ (so they can be recovered from knowing them modulo N). The encryption and decryption procedures are as follows:

(1) A message m is encrypted as $m^e \bmod N$.

(2) An encoded message c is decrypted as $c^d \bmod N$, where $de \equiv 1 \bmod \varphi(N)$ and d is called the decryption exponent (it only matters modulo $\varphi(N)$).

What makes this work is that (by Fermat's little theorem, not by Euler's theorem)

$$(m^e)^d \equiv m \bmod N \text{ for all } m \in \mathbb{Z}/N\mathbb{Z}.$$

(This is true even in the rare case that $(m, N) > 1$.)

A key point here is that for other people to encrypt messages, all they need to know is N and e; they do not need to know (and should not know) p or q or d. To decrypt messages requires knowledge of d, and that has to kept secret. While the math allows p and q to be arbitrary primes (with $p \neq q$), in practice they are primes having the same (or nearly the same) bit length.

In RSA, the *public key* is N and e while the *private key* is N and d. Since $de \equiv 1 \bmod \varphi(N)$, anyone who can figure out $\varphi(N)$ from the publicly announced N and e can quickly determine d with Euclid's algorithm on e and $\varphi(N)$.

With this background, we can define the RSA cryptosystem in terms of 3 ingredients: the process Gen that generates the public and private keys $\langle N, e\rangle$ and $\langle N, d\rangle$, the process $\mathsf{Enc}_{\langle N,e\rangle}$ that converts plaintext messages to ciphertext messages (using N and e), and the process $\mathsf{Dec}_{\langle N,d\rangle}$ that converts ciphertext messages to plaintext messages (using N and d).

Definition 4.1.1. The RSA public-key cryptosystem is a triple $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where

1. $\mathsf{Gen}(1^n)$ uses the even positive integer n (a unary security parameter) to generate two different $n/2$-bit primes p and q, and computes $N = pq$ as well as a member e of the group $(\mathbb{Z}/\varphi(N)\mathbb{Z})^\times$. It outputs (N, e, d), where $de \equiv 1 \bmod \varphi(N)$. Note $\varphi(N) = (p-1)(q-1)$.

2. $\mathsf{Enc}_{\langle N,e\rangle}(m)$ takes in a plaintext message m from $\mathbb{Z}/N\mathbb{Z}$ to be encrypted, as well as the public key $\langle N, e\rangle$ and computes a ciphertext message $c = m^e \bmod N$. It outputs c.

3. $\mathsf{Dec}_{\langle N,d\rangle}(c)$ takes in a ciphertext message c from $\mathbb{Z}/N\mathbb{Z}$, as well as the private key $\langle N, d\rangle$ and computes a plaintext message $m' = c^d \bmod N$. It outputs m'.

We can see from the congruences

$$m' \equiv c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \bmod N$$

that this definition of RSA satisfies correctness of an encryption process — that is, $\mathsf{Dec}(\mathsf{Enc}(m)) = m$ for all possible messages m. For more justification on this definition's security properties, as well as how RSA is used in practice, see [7, Section 10.4] or [12]. Essentially, because there is no known efficient way to find the prime factors of $N = pq$ from knowing only N, and no known way to find $d \bmod \varphi(N)$ (or even find $\varphi(N)$) from knowing only N and e, RSA is believed to be secure for computations with classical computers. If quantum computers ever become practical then RSA is will be broken. At present, the largest number factored with quantum computers by Shor's algorithm is 21, but other quantum computer algorithms have factored much larger numbers as one-time stunts; see https://crypto.stackexchange.com/questions/59795/largest-integer-factored-by-shors-algorithm.

Remark 4.1.2. What keeps RSA (apparently) secure is that for numbers N of the form pq,there is no known method to find $\varphi(N)$ from N other than factoring N. It is not currently known whether factoring N and computing the inverse of $e \bmod \varphi(N)$ given only N and e are equivalent. Miller [9] showed in 1975 that for numbers N of the form pq, factoring N is equivalent to finding the inverse of $e \bmod \varphi(N)$ assuming the Generalized Riemann Hypothesis.

A core part to RSA is the generation of (two) large random primes in Gen. Their product N is recommended to be 2048 bits now, which requires primes of bit-length around 1024, or prime numbers in the range $[2^{1023}, 2^{1024}]$. While these can vary, the main takeaway for us is that modern cryptography uses very large primes.

4.2 Primality Tests

A *primality test* is an algorithm that takes in an integer $N > 1$ and determines whether N is prime or composite. The simplest primality test is dividing the candidate N by every integer from 2 to $\sqrt{N}$. If any divide N, then N must be composite. Otherwise, N is prime. This is called trial division.

Clearly, trial division up to $\sqrt{N}$ is too slow to be useful as a primality test for N. Here is a more refined test due to Fermat.

Definition 4.2.1. For an integer $N \geq 2$, the Fermat primality test first chooses an integer a randomly in $[1, N-1]$. If

$$a^{N-1} \not\equiv 1 \bmod N$$

then N is composite. Otherwise, N may be prime.

This test is based on Fermat's Little Theorem, which states that, for each prime p and all a from 1 to $p-1$, we have $a^{p-1} \equiv 1 \bmod p$. If $a^{N-1} \not\equiv 1 \bmod N$ for some a in $[1, N-1]$ then N must be composite, in which case we call a a *Fermat witness* for N. We note that the Fermat primality test does not determine specifically whether N is prime or composite. It can determine that N is definitely composite if the congruence $a^{N-1} \equiv 1 \bmod N$ doesn't hold for some a in $[1, N-1]$, but the test can only suggest (not prove) a number is prime when compositeness is not revealed after applying the test.

To test N for primality, we may want to run the Fermat test many times with different values of a in $[1, N-1]$. When we run it many times without finding N to be composite, then we may think N is "very likely prime", although it's not clear what that really means if we don't know that composite N always have a definite positive proportion of compositeness witnesses in the range $[1, N-1]$ from the Fermat test.

Theorem 4.2.2. *Let* $W_N = \{1 \leq a \leq N-1 : a^{N-1} \not\equiv 1 \bmod N\}$ *be the set of Fermat witnesses for* N*. If* N *is prime, then* $W_N = \emptyset$*. If* N *is composite and there exists at least one Fermat witness in* $(\mathbb{Z}/N\mathbb{Z})^\times$*, then* $|W_N| \geq (N-1)/2$*.*

Proof. See [13, Theorem 10.1]. □

This appears to give us a very good lower bound: over half the numbers in $[1, N-1]$ are witnesses in the Fermat test on N if N is composite. But that's not what Theorem 4.2.2 says: the theorem includes the assumption that some witness for N is relatively prime to N. This doesn't always happen, and in that case the proportion of witnesses in the Fermat test could be very small.

Example 4.2.3. Let $N = 2{,}301{,}745{,}249$. Performing the Fermat test 100 times with random a in the range $[1, N-1]$, we find no witnesses to this N being composite by the Fermat test: $a^{N-1} \equiv 1 \bmod N$ each time. We'd like to say that Theorem 4.2.2 tells us the probability this N is prime is at least $1 - 1/2^{100}$, which is extremely close to 1. However, N is composite:

$$2{,}301{,}745{,}249 = 727 \cdot 1453 \cdot 2179$$

. The same thing happens with 9,624,742,921 and 113,654,675,587: running the Fermat test on these N with 100 random a in $[1, N-1]$ leads to $a^{N-1} \equiv 1 \bmod N$ each time, but these N are composite:

$$9{,}624{,}742{,}921 = 1171 \cdot 2341 \cdot 3511 \quad \text{and} \quad 113{,}654{,}675{,}587 = 2473 \cdot 3709 \cdot 12391.$$

The proportion of Fermat witnesses for the N here is far less than 1%: it is around 0.25% for 2,301,745,249, 0.16% for 9,624,742,921, and 0.075% for 113,654,675,587.

For a composite number N, an a in $[1, N-1]$ such that $(a, N) > 1$ will always be a Fermat witness since $a^{N-1} \equiv 1 \bmod N$ only if $(a, N) = 1$. There are composite N whose only Fermat witnesses are of that type: integers sharing a common factor with N. Such N are called *Carmichael numbers*. The first few Carmichael numbers are

$$561, \quad 1105, \quad 1729, \quad 2465.$$

All three N in Example 4.2.3 are Carmichael numbers. Finding a Fermat witness for a Carmichael number N requires finding a in $[1, N-1]$ such that $(a, N) > 1$ and that is as slow as deciding if N is composite by doing trial division. For Carmichael numbers N, the proportion of a in $[1, N-1]$ such that $a^{N-1} \not\equiv 1 \bmod N$ is the proportion of a in $[1, N-1]$ such that $(a, N) > 1$. This is $(N-1-\varphi(N))/(N-1) = 1-\varphi(N)/(N-1)$, and that could be extremely small, as we saw in Example 4.2.3.

Theorem 4.2.2 says that a composite N that is not a Carmichael number (meaning N has a Fermat witness relatively prime to N) has over 50% of the numbers less than N being witnesses to N in the Fermat test. Therefore if $a^{N-1} \equiv 1 \bmod N$ for many random values of a, the correct conclusion is not that N is very likely to be prime, but instead that N is very likely to be a prime number or a Carmichael number. Since it is known that there are infinitely many Carmichael numbers [13, p. 308], the Fermat test in fact is not an effective method of primality testing on its own.

4.3 The Miller-Rabin Primality Test

For RSA and other public-key cryptosystems to be practical, we need an efficient and effective primality test: a test for which prime numbers put into the test have no witness to their compositeness and composite numbers put into the test always have a substantial proportion of witnesses to their compositeness. Trial division and the Fermat test have drawbacks in that regard. In the late 1970s and early 1980s, better tests were developed.

The Solovay-Strassen primality test, discovered by Solovay and Strassen in 1977, is based on a generalization of the Legendre symbol from Example 3.1.4 called the Jacobi symbol and it can be applied to odd numbers $n > 1$. (For even n or $n = 1$, deciding primality of n is easy.) We define a round of the Solovay-Strassen test.

Definition 4.3.1. For odd input N, the Solovay-Strassen primality test first chooses an integer a randomly from $[1, N-1]$. If $(\frac{a}{N}) = 0$ or

$$a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \bmod N,$$

then N is composite. Otherwise, N may be prime. Here $(\frac{a}{N})$ is the Jacobi symbol.

Like the Fermat test, the Solovay-Strassen test can be run multiple times with different a to test primality of N. For a in $[1, N-1]$, if $(\frac{a}{N}) = 0$ or $a^{(N-1)/2} \not\equiv (\frac{a}{N}) \bmod N$ then N is definitely composite and we call a a *Solovay-Strassen witness* for N. Odd prime p have no Solovay-Strassen witness, since $a^{(p-1)/2} \equiv (\frac{a}{p}) \not\equiv 0 \bmod p$ for all a in $[1, p-1]$ by Euler's congruence for the Legendre symbol.

Unlike the Fermat test, the Solovay-Strassen test has no analogue of Carmichael numbers: every odd composite number N has a large proportion of Solovay-Strassen witnesses to its compositeness in $[1, N-1]$ in this test.

Theorem 4.3.2 (Solovay-Strassen)**.** *For odd $N > 1$, let W_N be the set of Solovay-Strassen witnesses in $[1, N-1]$. If N is prime then $W_N = \emptyset$. If N is composite then*

$$|W_N| \geq \frac{N-1}{2}.$$

Proof. See [14] and [15]. □

Because the proportion of Solovay-Strassen witnesses for each odd composite N has a positive lower bound that is independent of N (always at least 50%), the Solovay-Strassen test is called a probabilistic primality test. It was the first example of such a test. The Fermat test is not a genuine probabilistic primality test because of Carmichael numbers.

In 1980, two years after the paper of Solovay and Strassen appeared, Rabin's paper [11] came out in which a probabilistic primality test was described based on a test proposed by Miller [9] from 1976. Miller's test was originally in a deterministic form, not using random inputs, and we'll see later that its running time depends on an unsolved problem.

Definition 4.3.3. For odd $N > 1$, write $N - 1 = 2^r d$, where $r \geq 1$ and d is odd. The Miller-Rabin primality test chooses an integer a randomly in $[1, N-1]$ and computes

$$a^d, a^{2d}, \ldots, a^{2^i d}, \ldots, a^{2^{r-1}d} \bmod N. \tag{4.3.1}$$

If the first term in the list is not 1 mod N and the number -1 mod N never occurs in the list, then declare N to be composite. Otherwise, N may be prime.

For a in $[1, N-1]$, if the Miller-Rabin test with a terminates and calls N composite then N really is composite and a is called a *Miller-Rabin witness* for N. Odd prime p have no Miller-Rabin witness.

Remark 4.3.4. Here is motivation for the Miller-Rabin test. The last power in the test is $a^{2^{r-1}d} \equiv a^{(N-1)/2} \bmod N$. If p were an odd prime then $a^{(p-1)/2} \equiv \pm 1 \bmod p$ since $(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \bmod p$ and the only square roots of $1 \bmod p$ are $\pm 1 \bmod p$. If $a^{(p-1)/2} \equiv 1 \bmod p$ and $p \equiv 1 \bmod 4$ then $(a^{(p-1)/4})^2 = a^{(p-1)/2} \equiv 1 \bmod p$ so $a^{(p-1)/4} \equiv \pm 1 \bmod p$. More generally, if $p - 1 = 2^r d$ for $r \geq 1$ and d odd, the terms in the Miller-Rabin sequence $a^d, a^{2d}, \ldots, a^{2^{r-1}d} \bmod p$ either start with $1 \bmod p$ or some term in it is $-1 \bmod p$. So if the Miller-Rabin sequence for an odd number $N > 1$ doesn't start with $1 \bmod N$ and no term is $-1 \bmod N$, N must be composite.

The Miller-Rabin test is very effective because it is efficient to run each round and when N is odd composite there is always a large proportion of witnesses for N. For the large Carmichael numbers in Example 4.2.3, a Miller-Rabin witness was able to be found within 10 random trials for each.

Theorem 4.3.5 (Rabin)**.** *For odd $N > 1$, let W_N be the set of Miller-Rabin witnesses for N in $[1, N-1]$. If N is prime then $W_N = \emptyset$. If N is composite then*

$$|W_N| \geq \frac{3(N-1)}{4}.$$

Proof. See [3, Theorem 3.5.4] or [11, Theorem 1]. □

What this is saying is that the proportion of Miller-Rabin witnesses for odd composite numbers is at least 3/4. So for odd composite N, the probability that we run k rounds of the Miller-Rabin test without finding a witnesses for N is at most $1/4^k$.

The Miller-Rabin test completely replaced the Solovay-Strassen test and is the most commonly used primality test today. This is for three reasons. First, the Miller-Rabin test is a simpler test to describe and run, as the computations for it are based only on repeated squaring. Second, the proportion of Miller-Rabin witnesses for an odd composite number has a guaranteed lower bound that exceeds the guaranteed lower bound of the Solovay-Strassen test. And finally, every Solovay-Strassen witness for an odd composite number is a Miller-Rabin witness for that number, (though the converse is not true in general: $N = 341$ is composite with $a = 2$ as a Miller-Rabin witness, but 2 is *not* a Solovay-Strassen witness for this N. In particular, $(\frac{2}{341}) = -1$ and $2^{(341-1)/2} \equiv -1 \bmod 341$.) That means the Solovay-Strassen test will never involve a witness that wouldn't be found with the Miller-Rabin test. A proof that every Solovay-Strassen witness for N is a Miller-Rabin witness for N is in [3, Theorem 4.2.8].

The Miller-Rabin test was originally described by Miller (before Rabin) using a in $[1, N-1]$ deterministically as $a = 1, 2, 3, \ldots$ until a witness for N is found or the test ends and says N is prime, rather than probabilistically with random a. That Miller's deterministic version of the test can run efficiently (in polynomial time) is based on assuming the Generalized Riemann Hypothesis for Dirichlet L-functions.

Theorem 4.3.6 (Miller)**.** *For odd $N > 1$, let W_N be the set of Miller-Rabin witnesses in $[1, N-1]$. If N is prime then $W_N = \emptyset$. If N is composite and the Generalized Riemann Hypothesis is true for Dirichlet L-functions then there is a witness for N that is $O((\log N)^2)$.*

Proof. See [9, Theorem 2]. □

Unfortunately, Miller did not compute a value for the O-constant in his theorem, and without that such a deterministic test (assuming the Generalized Riemann Hypothesis) is not practical. A few years later Bach [2] made the O-constant in Miller's theorem explicit assuming the Generalized Riemann Hypothesis, and explaining how that works is the goal of our next and final chapter.

Chapter 5

The Generalized Riemann Hypothesis and Primality Tests

In previous chapters, we met the zeta-function, Dirichlet L-functions, and the Riemann Hypothesis and Generalized Riemann Hypothesis for them. In Chapter 4, we saw examples of primality tests that are probabilistic. While these are sufficient for cryptographic uses, it is of interest to see if these tests can be made into deterministic algorithms. We will show how the Generalized Riemann Hypothesis can help us quantify the O-constant in the bound from Theorem 4.3.6.

5.1 Bounding the size of compositeness witnesses

As stated in Chapter 4, the commonly-used primality tests now are all based on probablistically searching for a witness to the compositeness of a candidate number. When there are known lower bounds on the proportion of witnesses for composite numbers in a certain test, we may be reasonably sure a number is prime if no witnesses to compositeness is found after running that test enough times to make the probability of a false positive (declaring a number prime when it is really composite) less than the chance of a computer error. We can make such a test deterministic if we can bound how many nonwitnesses we need to find for the test before we can say with absolute certainty that the number we are testing is prime.

Let $N > 1$ be an odd composite number. There is a witness to its compositeness in $\{1, 2, \ldots, N-1\}$ for the Fermat test, the Solovay-Strassen test, and the Miller-Rabin test: a factor of N strictly between 1 and N, or really any number strictly between 1 and N whose gcd with N is bigger than 1, will be a witness for each of those tests. Relying on such witnesses to reveal compositeness of N is no better than doing trial division, so we want to take advantage of witnesses to compositeness that are relatively prime to N. Here the Fermat test runs into a problem, because if N is a Carmichael number then its only witnesses for the Fermat test are numbers sharing a factor bigger than 1 with N. In contrast, the Solovay-Strassen test and Miller-Rabin test are guaranteed to have compositness witnesses relatively prime to N, and that leads to the proportion of all numbers below N that are compositeness witnesses for N to be at least 50% or 75% for those respective two tests (Theorems 4.3.2 and 4.3.5).

To make these tests deterministic, we ask how small the first witness for each test can be guaranteed to be, as a function of N. How long could a string of *nonwitnesses* for N be (numbers not witnessing compositeness of N in the test) before we can be sure N is prime?

Nonwitnesses in the Solovay-Strassen test for odd $N > 1$ are the $a \in \mathbb{Z}/N\mathbb{Z}$ such that $a^{(N-1)/2} \equiv (\frac{a}{N}) \equiv \pm 1 \bmod N$. These form a *subgroup* of $(\mathbb{Z}/N\mathbb{Z})^\times$, and it is a proper subgroup if and only if N is composite. For composite N, we mentioned in Section 4.3 that each Solovay-Strassen witness for N is a Miller-Rabin witness for

N, so every Miller-Rabin *nonwitness* for N is a Solovay-Strassen *nonwitness* for N. Therefore when N is composite, the Miller-Rabin nonwitnesses for N are part of a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$, but they do not necessarily fill up a proper subgroup (see Example 5.1.1). When N is prime, no number from 1 to $N-1$ is a Solovay-Strassen witness or Miller-Rabin witness for N, so the subgroup of nonwitnesses for N for each test is all of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Example 5.1.1. Consider $N = 145$ with the unit group $(\mathbb{Z}/145\mathbb{Z})^\times$. The numbers 12 and 17 are not Miller-Rabin witnesses for N: $N - 1 = 144 = 2^4 \cdot 9$, so to test if $a \bmod N$ is a Miller-Rabin witness we look at $a^{2^i 9} \bmod N$ for $0 \leq i \leq 3$.

a	$a^9 \bmod N$	$a^{18} \bmod N$	$a^{36} \bmod N$	$a^{72} \bmod N$
12	12	$144 \equiv -1$	1	1
17	17	$144 \equiv -1$	1	1

However, the product $12 \cdot 17 \equiv 59 \bmod 145$ is a Miller-Rabin witness for N.

a	$a^9 \bmod N$	$a^{18} \bmod N$	$a^{36} \bmod N$	$a^{72} \bmod N$
59	59	1	1	1

Thus the set of Miller-Rabin nonwitnesses for 145 is *not* closed under multiplication in $(\mathbb{Z}/145)^\times$, and thus does not form a proper subgroup. (All three are Solovay-Strassen nonwitnesses for N, since $(\frac{a}{N}) = 1$ for all three of these a, which agrees with the last entry $a^{(N-1)/2} \bmod N$ in the tables above.)

Our task now is group-theoretic: for all odd $N > 1$, if H is a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ and we think of H as a set of integers in $\{1, \ldots, N-1\}$, then we want an upper bound on the smallest number in $\{1, \ldots, N-1\}$ that is not in H. It is okay if that first number is not relatively prime to N, so it is not in H because it is not even in $(\mathbb{Z}/N\mathbb{Z})^\times$.

The following theorem shows bounds of the form $(A\log N+B)^2+1$ for the smallest number not in H are equivalent to similar bounds on the first time a nontrivial primitive Dirichlet character is not 1 (in terms of the modulus).

Theorem 5.1.2. *For constants $A > 0$ and $B \geq 0$, the following conditions are equivalent.*

(1) *For all $N > 1$, each proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ omits a positive integer that is at most $(A\log N + B)^2 + 1$.*

(2) *For all $m > 1$, each primitive Dirichlet character $\chi \bmod m$ has $\chi(a) \neq 1$ for some positive integer $a \leq (A\log m + B)^2 + 1$.*

For some m there is no primitive character mod m (like $m = 6$), but that case easily fits (2), which is quantified over all $m > 1$.

Proof. (1) ⇒ (2): When $\chi \bmod m$ is primitive and $m > 1$, χ is nontrivial, so its kernel is a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. By (1) there is a positive integer $a \leq (A\log m + B)^2 + 1$ not in that proper subgroup, so $\chi(a) \neq 1$. (Perhaps $\chi(a) = 0$, so a is not even in $(\mathbb{Z}/m\mathbb{Z})^\times$.)

(2) ⇒ (1): Let H be a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. We want to find a nontrivial Dirichlet character mod N that is trivial on the subgroup H.

The quotient group $(\mathbb{Z}/N\mathbb{Z})^\times/H$ is a nontrivial finite abelian group, so it is isomorphic to a direct product of nontrivial cyclic groups by the structure theorem for finite abelian groups. Say

$$f\colon (\mathbb{Z}/N\mathbb{Z})^\times/H \to C_1 \times \cdots \times C_r \tag{5.1.1}$$

is an isomorphism for nontrivial cyclic groups C_i. Let $C_1 = \langle g \rangle$, and let $n > 1$ be the order of C_1. Define $\psi\colon C_1 \to S^1$ by $\psi(g^k) = e^{2\pi i k/n}$, where $k \in \mathbb{Z}/n\mathbb{Z}$. The map ψ is an isomorphism from C_1 to the nth roots of unity in S^1. Finally, let χ be the composition

$$(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times/H \to C_1 \to S^1,$$

where the first map is reduction, the second map is the isomorphism (5.1.1) followed by projection to C_1, and the third map is ψ. This is a composition of homomorphisms, so $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to S^1$ is a Dirchlet character. It is trivial on H since the first map is trivial on H, and it is nontrivial at an $a \bmod N$ that under the isomorphism in (5.1.1) corresponds on the right side with an r-tuple whose C_1-component is nontrivial. Thus we have formed a nontrivial character $\chi \bmod N$ that is trivial on the proper subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$.

The character $\chi \bmod N$ might not be primitive. Let $\chi' \bmod m$ be the primitive character that lifts to χ, where $m \mid N$. The character χ' must be nontrivial, as $\chi \bmod N$ is nontrivial, so the primitive character lifting to χ can't have $m = 1$. By (2), $\chi'(a \bmod m) \neq 1$ for a positive integer $a \leq (A \log m + B)^2 + 1$. Since $m \leq N$ we have $a \leq (A \log N + B)^2 + 1$. Also $a \bmod N \notin H$: since χ has value 1 on H, if $a \bmod N \in H$ then $\chi(a \bmod N) = 1$, so $(a, N) = 1$ and $\chi'(a \bmod m) = 1$, which is not true. □

We will see in Section 5.4 that the Generalized Riemann Hypothesis implies part (2) of Theorem 5.1.2 with the specific values $A = 1.125$ and $B = 9.1558$ That is, for those values of A and B every primitive character $\chi \bmod m$ for $m > 1$ doesn't have the value 1 at a positive integer that's at most $(A \log m + B)^2 + 1$. Then for all $N > 1$ each proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ omits a positive integer that's at most

$(A \log N + B)^2 + 1$, so each odd composite $N > 1$ has a witness in the Miller-Rabin test (and in the Solovay-Strassen test) that's at most $(A \log N + B)^2 + 1$. Therefore an odd $N > 1$ is prime if and only if no positive integer up to $(A \log N + B)^2 + 1$ is a Miller-Rabin witness (or Solovay-Strassen witness) for N.

Running the Miller-Rabin test on all positive integers a up to $(A \log N + B)^2 + 1$ is a deterministic algorithm, not a probabilistic algorithm like before (where we ran the test on randomly chosen a) and this makes the Miller-Rabin test a polynomial-time primality test. Specifically, because the Miller-Rabin test for N on one number a in $[1, N-1]$ has running time $O((\log N)^3)$ — first $O(\log N)$ steps to compute the binary expansion of N and then $O((\log N)^2)$ steps to compute powers by repeated squaring – Miller-Rabin applied to all positive integers up to $(A \log N + B)^2 + 1$ has running time

$$O((A \log N + B)^2) \cdot O((\log N)^3) = O((\log N)^5).$$

Remark 5.1.3. Especially if A and B are kept small in these computations, this would make the deterministic Miller-Rabin test more efficient than the AKS test, which is the only unconditionally provable polynomial-time primality test. The AKS test has run-time $O((\log N)^7)$, and in practice it is not used to verify primality.

Getting explicit constants A and B in part (2) of Theorem 5.1.2 is our task now, and this is how the Generalized Riemann Hypothesis finally makes an appearance in our treatment of primality tests.

To find the first $n \geq 1$ such that a primitive Dirichlet character $\chi \bmod m$ has $\chi(n) \neq 1$, suppose $\chi(n) = 1$ when $1 \leq n \leq x$. We want to bound how big x can get.

Perron's formula (Theorem 2.2.9) tells us for $c > 1$ and $x > 1$ that

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{s}\,ds = {\sum_{n\leq x}}^{*}\Lambda(n)$$

and

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{s}\,ds = {\sum_{n\leq x}}^{*}\chi(n)\Lambda(n),$$

where $\Lambda(n)$ is the von Mangoldt function. When $\chi(n) = 1$ for $1 \leq n \leq x$, the two partial sums on the right sides match, so the integrals on the left sides match:

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{s}\,ds = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{s}\,ds.$$

We actually will use not the integral from Perron's formula, which is based on the vertical integral $\int_{c-i\infty}^{c+i\infty}(y^s/s)\,ds$, but a modified integral based on $\int_{c-i\infty}^{c+i\infty}(y^s/s^2)\,ds$.

Lemma 5.1.4. *For $c > 1$ and $y > 0$,*

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^2}\,ds = \begin{cases} 0 & \text{if } 0 < y \leq 1, \\ \log y & \text{if } y \geq 1. \end{cases}$$

Proof. We consider $0 < y < 1$, $y > 1$, and $y = 1$ separately.

Case 1: $0 < y < 1$. Pick $c' > c$. We use the counterclockwise rectangular contour with right side $[c' - iT, c' + iT]$ and left side $[c + iT, c - iT]$ (oriented top to bottom). The integral y^s/s^2 on this rectangle is 0 since the only pole for y^s/s^2 is at the origin, which is outside the rectangle.

Let $\sigma = \mathrm{Re}(s)$ and $t = \mathrm{Im}(s)$. We first consider the horizontal components of our contour, from $c' + iT$ to $c + iT$ and from $c - iT$ to $c' - iT$ (eventually taking $c' \to \infty$

and $T \to \infty$). Because $|y^s/s^2| = y^\sigma/|s|^2 \leq y^\sigma/T^2$, the integrals of y^s/s^2 along the top and bottom of the rectangle each have absolute value bounded above by

$$\int_c^{c'} \frac{y^\sigma}{T^2}\,d\sigma = \frac{y^\sigma}{T^2 \log y}\bigg|_c^{c'} = \frac{y^{c'} - y^c}{T^2 \log y} = \frac{y^c - y^{c'}}{T^2|\log y|} < \frac{y^c}{T^2|\log y|}, \tag{5.1.2}$$

where the third equation makes the numerator and denominator both positive since $0 < y < 1$ and $c' > c$. The upper bound is independent of c' and tends to 0 as $T \to \infty$.

For the integral along the right side of the rectangle, from $c' - iT$ to $c' + iT$,

$$\left|\int_{c'+iT}^{c'-iT} \frac{y^s}{s^2}\,ds\right| \leq \int_{-T}^{T} \frac{y^{c'}}{|c'+it|^2}\,dt = 2y^{c'}\int_0^T \frac{dt}{(c')^2+t^2} < 2y^{c'}\int_0^T \frac{dt}{1+t^2}$$

since $c' > c > 1$. Since $\int_0^\infty dt/(1+t^2) = \pi/2$ by calculus,

$$\left|\int_{c'+iT}^{c'-iT} \frac{y^s}{s^2}\,ds\right| < \pi y^{c'}. \tag{5.1.3}$$

The upper bound is independent of T and tends to 0 as $c' \to \infty$.

Since the integral of y^s/s^2 around the whole rectangle is 0, the integral along the left side is a sum of integrals along the other three sides (suitably oriented), so after dividing by $2\pi i$ in (5.1.2) and (5.1.3) we get

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s^2}\,ds\right| < \frac{1}{2\pi}\left(\frac{2y^c}{T^2|\log y|} + \pi y^{c'}\right) = \frac{y^c}{\pi|\log y|}\frac{1}{T^2} + \frac{1}{2}y^{c'} \tag{5.1.4}$$

for $c' > c$ and $T > 0$. Let $c' \to 0$ to make the second term in the upper bound tend to 0 without changing the integral being bounded. Then let $T \to \infty$ to make the first term in the upper bound tend to 0 and we get the desired vanishing integral for the lemma when $0 < y < 1$.

Case 2: $y > 1$. Pick $c' > 1$. We create a new counterclockwise rectangular contour with right side $[c-iT, c+iT]$ and left side $[-c'+iT, -c'-iT]$ (oriented top to bottom). This contour passes around the origin, where y^s/s^2 has a pole. To determine the residue of y^s/s^2 at $s = 0$,

$$\frac{y^s}{s^2} = \frac{e^{s\log y}}{s^2} = \frac{1}{s^2}\left(1 + (\log y)s + \frac{(\log y)^2}{2}s^2 + \cdots\right) = \frac{1}{s^2} + \frac{\log y}{s} + O(1),$$

so $\operatorname{Res}_{s=0}(y^s/s^2) = \log y$. Therefore the residue theorem tells us the integral of $\frac{1}{2\pi i}(y^s/s^2)$ around the rectangle is $\log y$. To prove the integral in the lemma for $y > 1$ is $\log y$, it suffices to show the sum of the integrals over the top, bottom, and left sides of the rectangle tend to 0 as $c' \to -\infty$ and $T \to \infty$ in a suitable way.

We first bound the integral of y^s/s^2 along the top and bottom. Each integral has absolute value at most

$$\int_{-c'}^{c} \left|\frac{y^s}{s^2}\right| d\sigma < \frac{1}{T^2}\int_{-c'}^{c} y^\sigma \, d\sigma = \frac{y^c - y^{-c'}}{T^2 \log y} < \frac{y^c}{T^2 \log y}, \tag{5.1.5}$$

which is analogous to (5.1.2). The upper bound is independent of c' and tends to 0 as $T \to \infty$.

For the integral along the left side $[-c' + iT, -c' - iT]$,

$$\left|\int_{-c'+iT}^{-c-iT} \frac{y^s}{s^2}\, ds\right| \leq \int_{-T}^{T} \frac{y^{-c'}}{(-c')^2 + t^2}\, dt < 2y^{-c'}\int_0^T \frac{1}{1+t^2}\, dt$$

since $c' > 1$. The integral on the right is less than $\pi/2$ just as in the case where

$0 < y < 1$, so

$$\left| \int_{-c'+iT}^{-c-iT} \frac{y^s}{s^2}\, ds \right| < \pi y^{-c'}, \tag{5.1.6}$$

which is analogous to (5.1.3). The upper bound is independent of T and tends to 0 as $c' \to \infty$.

Now we can use the residue theorem for the integral around the rectangle to get

$$\left| \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{y^s}{s^2}\, ds - \log y \right| < \frac{1}{2\pi} \left(\frac{2y^c}{T^2 \log y} + \pi y^{-c'} \right) = \frac{y^c}{\pi \log y} \frac{1}{T^2} + \frac{1}{2} y^{-c'},$$

which is analogous to (5.1.4). Letting $c' \to \infty$ and then $T \to \infty$ produces the desired formula in the lemma when $y > 1$.

Case 3: $y = 1$. We calculate the integral directly. Writing $s = c + it$, so $ds = i\, dt$,

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^2}\, ds = \lim_{T \to \infty} \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{ds}{s^2} = \lim_{T \to \infty} \frac{1}{2\pi} \int_{-T}^{T} \frac{dt}{(c+it)^2}$$

The antiderivative of $1/(c+it)^2$ with respect to t is $i/(c+it)$, so

$$\int_{-T}^{T} \frac{dt}{(c+it)^2} = \left. \frac{i}{c+it} \right|_{-T}^{T} = \frac{i}{c+iT} - \frac{i}{c-iT} = \frac{2T}{c^2+T^2}.$$

This tends to 0 as $T \to \infty$, so

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^2}\, ds = \lim_{T \to \infty} \frac{T}{\pi(c^2+T^2)} = 0. \qquad \square$$

Lemma 5.1.5. *If $f(s) = \sum a_n/n^s$ converges absolutely for $\mathrm{Re}(s) > 1$, then for $c > 1$ and $x > 0$,*

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f(s) \frac{x^s}{s^2}\, ds = \sum_{n \le x} a_n \log(x/n).$$

A key difference between this result and Perron's formula in Theorem 2.2.9 is the denominator being s^2 rather than s. We don't weight the last term in the partial sum if $x \in \mathbb{Z}^+$, as we do in Perron's formula, since $\log(x/n) = 0$ if $x = n$.

Proof. This is proved similarly to Perron's formula:

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f(s)\frac{x^s}{s^2}\,ds &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(\sum_{n\geq 1}\frac{a_n}{n^s}\right)\frac{x^s}{s^2}\,ds \\ &= \sum_{n\geq 1} a_n \frac{1}{2\pi i}\int_{c-\infty}^{c+i\infty}\frac{(x/n)^s}{s^2}\,ds \\ &= \sum_{n\leq x} a_n \log(x/n) \quad \text{by Lemma 5.1.4.}\end{aligned}$$

A more rigorous proof would use truncated integrals $\int_{c-iT}^{c+iT}$ and bounds on integrals on sides of rectangles in the proof of Lemma 5.1.4, and let $T \to \infty$ at the end. □

We will need a modification of the integral in Lemma 5.1.5, using denomiator $(s+b)^2$ for $0 < b < 1$ that will be picked later:

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f(s)\frac{x^s}{(s+b)^2}\,ds.$$

By the change of variables $s \mapsto s - b$ in this integral, we get for $c > 1$ and $x > 0$

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f(s)\frac{x^s}{(s+b)^2}\,ds &= \frac{1}{2\pi i}\int_{c+b-i\infty}^{c+b+i\infty} f(s-b)\frac{x^{s-b}}{s^2}\,ds \\ &= \frac{1}{x^b}\frac{1}{2\pi i}\int_{c+b-i\infty}^{c+b+i\infty} f(s-b)\frac{x^s}{s^2}\,ds \\ &= \frac{1}{x^b}\sum_{n\leq x} a_n n^b \log(x/n) \qquad (5.1.7)\end{aligned}$$

since $f(s-b) = \sum a_n n^b/n^s$ converges absolutely for $\text{Re}(s) > 1 + b$ and $c + b > 1 + b$.

Theorem 5.1.6. *For $c > 1$, $x > 0$, and $0 < b < 1$,*

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{(s+b)^2}\,ds = \frac{1}{x^b}\sum_{n\leq x}\Lambda(n)n^b\log(x/n) \tag{5.1.8}$$

and

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{(s+b)^2}\,ds = \frac{1}{x^b}\sum_{n\leq x}\chi(n)\Lambda(n)n^b\log(x/n). \tag{5.1.9}$$

Proof. In (5.1.7), use the functions $f(s) = -\zeta'(s)/\zeta(s) = \sum\Lambda(n)/n^s$ and $f(s) = -L'(s,\chi)/L(s,\chi) = \sum\chi(n)\Lambda(n)/n^s$. □

Suppose $\chi \bmod m$ is a primitive Dirichlet character such that $\chi(n) = 1$ when $1 \leq n \leq x$. Then the technical-looking sums on the right side of (5.1.8) and (5.1.9) match, so the integrals on the left side match:

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{(s+b)^2}\,ds = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{(s+b)^2}\,ds \tag{5.1.10}$$

for $c > 1$. We will compute these integrals in a second way in order to obtain an upper bound on x, and that will bound how long we could have $\chi(n) = 1$.

Theorem 5.1.7. *For $c > 1$, $x > 1$, $0 < b < 1$, and a nontrivial primitive Dirichlet character χ,*

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{(s+b)^2}\,ds = \frac{x}{(1+b)^2} - \sum_{\rho}\frac{x^\rho}{(\rho+b)^2} - \left(\frac{\zeta'}{\zeta}\right)'(-b)\,\frac{1}{x^b}\\ - \frac{\zeta'}{\zeta}(-b)\,\frac{\log x}{x^b} - \sum_{n\geq 1}\frac{1}{(2n-b)^2x^{2n}}\end{aligned}$$

and

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{(s+b)^2}\,ds = -\sum_{\rho_\chi}\frac{x^{\rho_\chi}}{(\rho_\chi+b)^2} - \left(\frac{L'}{L}\right)'(-b,\chi)\,\frac{1}{x^b}$$
$$-\frac{L'}{L}(-b,\chi)\,\frac{\log x}{x^b} - \begin{cases}\displaystyle\sum_{n\geq 0}\frac{1}{(2n-b)^2x^{2n}} & \chi \textit{ even}\\ \displaystyle\sum_{n\geq 0}\frac{1}{(2n+1-b)^2x^{2n+1}} & \chi \textit{ odd}\end{cases}$$

where ρ and ρ_χ run over the nontrivial zeros of $\zeta(s)$ and $L(s,\chi)$ with multiplicity.

Proof. We will use the residue theorem to calculate these integrals by adding the residues of the respective functions to the left of the line $\mathrm{Re}(s) = c$, pushing the contour of integration to the left rather than to the right because $|x^s| \to 0$ as $\mathrm{Re}(s) \to -\infty$ when $x > 1$. See [6, Theorem 28] for a more complete justification of a similar result with denominator $s(s+1)$. In this proof, we will focus on the calculation of the residues at the poles for both integrands.

We first consider

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{(s+b)^2}\,ds.$$

Recall from Theorem 2.1.5 that the logarithmic derivative $f'(s)/f(s)$ of a meromorphic function $f(s)$ has a pole at $s = a$ only if $f(s)$ has a zero or pole at $s = a$, and $\mathrm{Res}_{s=a}(f'(s)/f(s))$ is the order of vanishing of $f(s)$ at $s = a$ (positive at zeros, negative at poles). Therefore the poles of $(\zeta'/\zeta)(s)(x^s/(s+b)^2)$ are in four places:

(i) the pole of $\zeta(s)$ at $s = 1$,

(ii) the trivial zeros of $\zeta(s)$ at negative even numbers,

(iii) the nontrivial zeros of $\zeta(s)$ in the critical strip,

(iv) the double pole at $s = -b$ introduced by $(s+b)^2$ in the denominator.

Since $c > 1$, all poles in (i), (ii), (iii), and (iv) are to the left of the line $\mathrm{Re}(s) = c$.

At $s = 1$, $\zeta'(s)/\zeta(s)$ has a pole with residue -1 since $\zeta(s)$ has a simple pole there by Theorem 1.2.1. Therefore the residue of the integrand at $s = 1$ is

$$-(-1)\frac{x}{(1+b)^2} = \frac{x}{(1+b)^2}. \tag{5.1.11}$$

Trivial zeros of $\zeta(s)$ at $s = -2n$, for $n \geq 1$, are simple, so the residue of $(\zeta'/\zeta)(s)$ at $s = -2n$ is 1, which makes the residue of the integrand at $s = -2n$ equal to

$$\frac{-x^{-2n}}{(-2n+b)^2} = \frac{-1}{(2n-b)^2 x^{2n}}. \tag{5.1.12}$$

Similarly, the residue of the integrand at a nontrivial zero ρ of $\zeta(s)$ is

$$-\operatorname{ord}_{s=\rho}(\zeta(s))\frac{x^\rho}{(\rho+b)^2}. \tag{5.1.13}$$

It is expected that nontrivial zeros of $\zeta(s)$ have order 1, so $\operatorname{ord}_{s=\rho}(\zeta(s))$ should be 1.

For a function $f(s)$ analytic at $s = -b$, $f(s) = f(-b) + f'(-b)(s+b) + O((s+b)^2)$ near b, so

$$\operatorname{Res}_{s=-b} \frac{f(s)}{(s+b)^2} = f'(-b).$$

Apply this to $f(s) = -(\zeta'(s)/\zeta(s))x^s$. Using the product rule,

$$\begin{aligned}\operatorname{Res}_{s=-b}\left(-\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{(s+b)^2}\right) &= -\left(\frac{\zeta'}{\zeta}\right)'(-b)\,x^{-b} - \frac{\zeta'}{\zeta}(-b)\,x^{-b}\log x \\ &= -\left(\frac{\zeta'}{\zeta}\right)'(-b)\,\frac{1}{x^b} - \frac{\zeta'}{\zeta}(-b)\,\frac{\log x}{x^b}. \end{aligned} \tag{5.1.14}$$

Adding together all the residues in (5.1.11), (5.1.12), (5.1.13), (5.1.14) gives us the terms in the first equation of the theorem. The first term accounts for the pole at $s = 1$, the second term accounts for poles at nontrivial zeros of $\zeta(s)$ *when we sum over nontrivial zeros with multiplicity*, the third and fourth terms account for the double pole at $s = -b$, and the final sum accounts for poles at trivial zeros of $\zeta(s)$.

The calculation of

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\frac{x^s}{(s+b)^2}\,ds$$

for a nontrivial primitive Dirichlet character χ is done in a similar way. Let $\delta \in \{0, 1\}$ be the parity of χ. We have three types of poles to account for:

(i) the trivial zeros of $L(s,\chi)$ at at $-2n-\delta$ for $n \geq 0$,

(ii) the nontrivial zeros of $L(s,\chi)$ in the critical strip,

(iii) the double pole at $s = -b$ introduced by $(s+b)^2$ in the denominator.

This list differs from that for $\zeta(s)$ in two ways: no pole at $s = 1$ and if $\delta = 0$ there is a trivial zero of $L(s,\chi)$ at $s = 0$. The lack of a pole at $s = 1$ is crucial.

At the trivial zero $-2n-\delta$, similarly to (5.1.12) the integrand has residue

$$\frac{-x^{-2n-\delta}}{(-2n-\delta+b)^2} = \frac{-1}{(2n+\delta-b)^2x^{2n+\delta}}. \tag{5.1.15}$$

At a nontrivial zero ρ_χ in the critical strip, we calculate the residue of the integrand similarly to (5.1.13) and get value

$$-\operatorname{ord}_{s=\rho_\chi}(L(s,\chi))\frac{x^{\rho_\chi}}{(\rho_\chi+b)^2}. \tag{5.1.16}$$

At $s = -b$, compute the residue as in (5.1.14) to get

$$\operatorname{Res}_{s=-b}\left(-\frac{L'(s,\chi)}{L(s,\chi)}\frac{x^s}{(s+b)^2}\right) = -\left(\frac{L'}{L}\right)'(-b,\chi)\,\frac{1}{x^b} - \frac{L'}{L}(-b,\chi)\,\frac{\log x}{x^b}. \qquad (5.1.17)$$

Adding up the residues in (5.1.15), (5.1.16), and (5.1.17), we get the second formula in the theorem. The first sum accounts for poles at the nontrivial zeros *when we sum over nontrivial zeros with multiplicity*, the second and third terms account for the double pole at $s = -b$, and the final sum accounts for the poles at trivial zeros.

The sum over n on the right side of the equation involving ζ'/ζ starts at $n = 1$, while the sum over n on the right side of the equation involving L'/L starts at $n = 0$ because the trivial zeros of the zeta-function start at -2 while the trivial zeros of $L(s,\chi)$ for nontrivial primitive χ start at either 0 (if $\delta = 0$) or -1 (if $\delta = 1$). □

If a primitive Dirichlet character χ mod m satisfies $\chi(n) = 1$ when $1 \leq n \leq x$, then (5.1.10) is true, so the right sides of the equations in Theorem 5.1.7 are equal:

$$\frac{x}{(1+b)^2} - \sum_{\rho}\frac{x^\rho}{(\rho+b)^2} - \left(\frac{\zeta'}{\zeta}\right)'(-b)\,\frac{1}{x^b} - \frac{\zeta'}{\zeta}(-b)\,\frac{\log x}{x^b} - \sum_{n\geq 1}\frac{1}{(2n-b)^2x^{2n}}$$

equals

$$-\sum_{\rho_\chi}\frac{x^{\rho_\chi}}{(\rho_\chi+b)^2} - \left(\frac{L'}{L}\right)'(-b,\chi)\,\frac{1}{x^b} - \frac{L'}{L}(-b,\chi)\,\frac{\log x}{x^b} - \begin{cases}\displaystyle\sum_{n\geq 0}\frac{1}{(2n-b)^2x^{2n}} & \chi \text{ even}\\ \displaystyle\sum_{n\geq 0}\frac{1}{(2n+1-b)^2x^{2n+1}} & \chi \text{ odd.}\end{cases}$$

Set these long expressions equal to each other and move all the terms except $x/(1+b)^2$

to the right side:

$$
\begin{aligned}
\frac{x}{(1+b)^2} &= \sum_{\rho} \frac{x^{\rho}}{(\rho+b)^2} - \sum_{\rho_\chi} \frac{x^{\rho_\chi}}{(\rho_\chi+b)^2} \\
&\quad \left(\frac{\zeta'}{\zeta}\right)'(-b)\,\frac{1}{x^b} + \frac{\zeta'}{\zeta}(-b)\,\frac{\log x}{x^b} - \left(\frac{L'}{L}\right)'(-b,\chi)\,\frac{1}{x^b} - \frac{L'}{L}(-b,\chi)\,\frac{\log x}{x^b} \\
&\quad + \sum_{n\geq 1} \frac{1}{(2n-b)^2 x^{2n}} - \begin{cases} \displaystyle\sum_{n\geq 0} \frac{1}{(2n-b)^2 x^{2n}} & \chi \text{ even} \\ \displaystyle\sum_{n\geq 0} \frac{1}{(2n+1-b)^2 x^{2n+1}} & \chi \text{ odd.} \end{cases}
\end{aligned}
$$

For even χ, the terms in the sums over n cancel out except at $n = 0$, leaving just $-1/b^2$. For odd χ, the two sums over n combine to form the alternating series

$$
\sum_{k\geq 1} \frac{(-1)^k}{(k-b)^2 x^k} = -\frac{1}{(1-b)^2 x} + \frac{1}{(2-b)^2 x^2} - \frac{1}{(3-b)^2 x^3} + + \frac{1}{(4-b)^2 x^2} - \cdots
$$

whose successive terms are strictly decreasing in absolute value, so the absolute value of the sum is less than the absolute value of the first term:

$$
\left| \sum_{k\geq 1} \frac{(-1)^k}{(k-b)^2 x^k} \right| < \frac{1}{(1-b)^2 x} < \frac{1}{(1-b)^2}
$$

since $x > 1$. This bound is $1/(b-\delta)^2$ for $\delta = 0$ and 1, so by the triangle inequality,

$$
\begin{aligned}
\frac{x}{(1+b)^2} &\leq \sum_{\rho} \frac{x^{\mathrm{Re}(\rho)}}{|\rho+b|^2} + \sum_{\rho_\chi} \frac{x^{\mathrm{Re}(\rho_\chi)}}{|\rho_\chi+b|^2} \\
&\quad + \left| \left(\frac{\zeta'}{\zeta}\right)'(-b) \right| \frac{1}{x^b} + \left| \frac{\zeta'}{\zeta}(-b) \right| \frac{\log x}{x^b} \\
&\quad + \left| \left(\frac{L'}{L}\right)'(-b,\chi) \right| \frac{1}{x^b} + \left| \frac{L'}{L}(-b,\chi) \right| \frac{\log x}{x^b} + \frac{1}{(b-\delta)^2}.
\end{aligned}
$$

Finally it is time to *assume the Generalized Riemann Hypothesis*. It implies $\mathrm{Re}(\rho) = 1/2$ and $\mathrm{Re}(\rho_\chi) = 1/2$ for nontrivial zeros of ρ and ρ_χ, so

$$\begin{aligned}\frac{x}{(1+b)^2} \leq {} & \left(\sum_\rho \frac{1}{|\rho+b|^2} + \sum_{\rho_\chi} \frac{1}{|\rho_\chi+b|^2}\right)\sqrt{x} \\ & + \left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right|\frac{1}{x^b} + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{\log x}{x^b} \\ & + \left|\left(\frac{L'}{L}\right)'(-b,\chi)\right|\frac{1}{x^b} + \left|\frac{L'}{L}(-b,\chi)\right|\frac{\log x}{x^b} + \frac{1}{(b-\delta)^2}.\end{aligned}$$

This shows x can't get too large: on the left side is an x and on the right side is $\sqrt{x}$ and other terms that are bounded for $x > 1$: $1/x^b < 1$ and $(\log x)/x^b \leq 1/(be)$ (the maximum value is at $x = \sqrt[b]{e}$ by calculus), so

$$\begin{aligned}\frac{x}{(1+b)^2} \leq {} & \left(\sum_\rho \frac{1}{|\rho+b|^2} + \sum_{\rho_\chi} \frac{1}{|\rho_\chi+b|^2}\right)\sqrt{x} + \left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| \\ & + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be} + \left|\left(\frac{L'}{L}\right)'(-b,\chi)\right| + \left|\frac{L'}{L}(-b,\chi)\right|\frac{1}{be} + \frac{1}{(b-\delta)^2}.\end{aligned} \tag{5.1.18}$$

Until now b has been arbitrary in $(0, 1)$. To make things concrete, set $b = 1/2$. Then $1/(b-\delta)^2 = 4$ for $\delta = 0$ and 1, so (5.1.18) becomes

$$\begin{aligned}\frac{4}{9}x \leq {} & \left(\sum_\rho \frac{1}{|\rho+\frac{1}{2}|^2} + \sum_{\rho_\chi} \frac{1}{|\rho_\chi+\frac{1}{2}|^2}\right)\sqrt{x} + \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| \\ & + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} + 4.\end{aligned} \tag{5.1.19}$$

The sum over ρ and the terms involving the zeta-function are concrete numbers, having nothing to do with x or χ. In Section 5.2 we'll see $-(L'/L)(-1/2, \chi) =$

$\log m + O(1)$, $(L'/L)'(-1/2,\chi) = O(1)$, and that the Generalized Riemann Hypothesis implies the sum over ρ_χ is $O(\log m)$, where all three O-constants are absolute (they do not depend on χ or m). Therefore (5.4.1) tells us if $\chi(n) = 1$ for $1 \leq n \leq x$,

$$\frac{4}{9}x = O((\log m)\sqrt{x}) + O(\log m) \implies \sqrt{x} = O(\log m) \implies x = O((\log m)^2). \quad (5.1.20)$$

So the Generalized Riemann Hypothesis implies every primitive Dirichlet character $\chi \bmod m$ can be 1 on all integers in $[1, x]$ only when $x = O((\log m)^2)$, so $\chi(a) \neq 1$ at some integer that is $O((\log m)^2)$. Combining this with Theorem 5.1.2, the Generalized Riemann Hypothesis implies the first witnesses in the Miller-Rabin test and Solovay-Strassen test for every odd composite number N are $O((\log N)^2)$. That shows the Miller-Rabin test and Solovay-Strassen test are polynomial-time primality tests *in principle*, but to make them so in practice (assuming the Generalized Riemann Hypothesis) we want to make the O-constant in (5.1.20) explicit.

Remark 5.1.8. While we bounded $1/x^b$ by 1 and $(\log x)/x^b$ by $1/(be)$ for $x > 1$, we could do it differently. The function $1/x^b$ is decreasing for $x > 1$ and the function $(\log x)/x^b$ is decreasing for $x > \sqrt[b]{e}$, so for an integer $n_0 > \sqrt[b]{e}$ and all $x \geq n_0$ we could bound $1/x^b$ by $1/n_0^b$ and $(\log x)/x^b$ by $(\log n_0)/n_0^b$. Then, for the calculations in Section 5.4, we use these bounds instead of 1 and $1/(be)$, achieving a different, tighter bound on x (in terms of the modulus m of χ) if $x \geq n_0$. Then every nontrivial primitive character is not 1 at some positive integer that is either less than n_0 or is less than the tighter bound we could have worked out. That could then be translated into an upper bound on the first Miller-Rabin witness for odd composite numbers: it is less than n_0 or less than a bound related to the estimates with primitive Dirichlet characters. For our work, we will use the bounds 1 and $1/(be)$.

5.2 Intermediate calculations

To bound the terms on the right side of (5.1.19) using explicit numbers, we will need values of several functions at $-1/2$ and (for the sums over nontrivial zeros) $\pm 1/4$. Such values (and a few more) are in the next theorem. We express values at specific negative numbers in terms of values at $s > 1$, where $\Gamma(s)$, $\zeta(s)$, and $L(s, \chi)$ are given by their initial definitions as absolutely convergent integrals or sums.

Theorem 5.2.1. *We have the following numerical formulas.*

(1) $\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) + 4 = \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) + \pi.$

(2) $\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) - \pi = \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - 4.$

(3) $\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) = \frac{\pi^2}{2} - 4.$

(4) $\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) = \log(\pi) - 2 - \frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) = \log(\pi) + 2 - \pi - \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right).$

(5) $\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right) = \left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right) - 4$

(6) *For a nontrivial primitive character* $\chi \bmod m$*,*

$$-\frac{L'}{L}\left(-\frac{1}{2}, \chi\right) = \log\left(\frac{m}{2\pi}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) + (-1)^{\delta}\frac{\pi}{2} + \frac{L'}{L}\left(\frac{3}{2}, \overline{\chi}\right). \tag{5.2.1}$$

(7) *For a nontrivial primitive character* $\chi \bmod m$*,*

$$\left(\frac{L'}{L}\right)'\left(-\frac{1}{2}, \chi\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) - \frac{\pi^2}{2} + \left(\frac{L'}{L}\right)'\left(\frac{3}{2}, \overline{\chi}\right). \tag{5.2.2}$$

Proof. (1) The first formula for $(\Gamma'/\Gamma)(-1/4)$ comes from setting $s = -1/4$ in (2.4.1):

$$\frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) = \frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - 4 \Longrightarrow \frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) + 4.$$

The second formula for $(\Gamma'/\Gamma)(-1/4)$ in (1) comes from setting $s = -1/4$ in (2.4.2):

$$\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - \pi\cot\left(-\frac{\pi}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) + \pi.$$

(2) Setting $s = 1/4$ in (2.4.2),

$$\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) - \pi.$$

Setting $s = 1/4$ in (2.4.1) and moving terms around,

$$\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) = \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - 4.$$

(3) Differentiating (2.4.1),

$$\left(\frac{\Gamma'}{\Gamma}\right)'(s+1) = \left(\frac{\Gamma'}{\Gamma}\right)'(s) - \frac{1}{s^2}, \tag{5.2.3}$$

so setting $s = 1/2$,

$$\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1}{2}\right) - 4. \tag{5.2.4}$$

Differentiating (2.4.2),

$$\left(\frac{\Gamma'}{\Gamma}\right)'(s) = -\left(\frac{\Gamma'}{\Gamma}\right)'(1-s) + \pi^2\csc^2(\pi s),$$

so setting $s = 3/2$

$$\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) = -\left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{1}{2}\right) + \pi^2. \tag{5.2.5}$$

To get rid of $(\Gamma'/\Gamma)'(-1/2)$ here, set $s = -1/2$ in (5.2.3) to find

$$\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1}{2}\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{1}{2}\right) - 4,$$

so (5.2.5) becomes

$$\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) = -\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1}{2}\right) - 4 + \pi^2.$$

Using this to write $(\Gamma'/\Gamma)'(1/2)$ in terms of $(\Gamma'/\Gamma)'(3/2)$ and substituting the result into the right side of (5.2.4), we get the formula for $(\Gamma'/\Gamma)'(3/2)$ in (3).

(4) Setting $s = -1/2$ in (2.4.3),

$$\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) = \log(\pi) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{3}{4}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right).$$

Substituting in here the first formula for $(\Gamma'/\Gamma)(-1/4)$ from (1), we get the first equation in (4). Writing $(\Gamma'/\Gamma)(3/4)$ in terms of $(\Gamma'/\Gamma)(5/4)$ using (1) leads to the second equation in (4).

(5) Set $s = -1/2$ in (2.4.4):

$$\begin{aligned}\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right) &= \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{4}\right) - \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{1}{4}\right) + \left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right)\\ &= \left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right) - \frac{1}{4}\left(\left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{1}{4}\right) - \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{4}\right)\right).\end{aligned}$$

To calculate $(\Gamma'/\Gamma)'(-1/4) - (\Gamma'/\Gamma)'(3/4)$, set $s = -1/4$ in (5.2.3):

$$\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{4}\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{1}{4}\right) - 16,$$

Therefore $(\Gamma'/\Gamma)'(-1/4) - (\Gamma'/\Gamma)'(3/4) = 16$, so we get (5).

(6) Recall from Theorem 3.3.9 the ugly functional equations for $L(s, \chi)$:

$$L(1-s,\chi) = \frac{2W(\chi)}{\sqrt{m}}\left(\frac{2\pi}{m}\right)^{-s}\Gamma(s)\cos\left(\frac{\pi}{2}(s-\delta)\right)L(s,\overline{\chi})$$

for $s \in \mathbb{C}$. Take logarithmic derivative of both sides. Products go to sums and we get

$$-\frac{L'}{L}(1-s,\chi) = \log\left(\frac{m}{2\pi}\right) + \frac{\Gamma'}{\Gamma}(s) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(s-\delta)\right) + \frac{L'}{L}(s,\overline{\chi}). \tag{5.2.6}$$

Setting $s = 3/2$ in (5.2.6) and taking cases if δ is 0 and 1,

$$-\frac{L'}{L}\left(-\frac{1}{2},\chi\right) = \log\left(\frac{m}{2\pi}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) + (-1)^{\delta}\frac{\pi}{2} + \frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right).$$

(7) Differentiating (5.2.6), setting $s = 3/2$, and taking cases if δ is 0 or 1,

$$\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) - \frac{\pi^2}{2} + \left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right). \qquad \square$$

The following exact formulas for sums over nontrivial zeros use the Generalized Riemann Hypothesis.

Theorem 5.2.2. *For $0 < b < 1$ and a primitive Dirichlet character $\chi \bmod m$, the*

Generalized Riemann Hypothesis for $\zeta(s)$ *and* $L(s,\chi)$ *implies*

$$\sum_{\rho} \frac{1}{|\rho+b|^2} = \frac{1}{1/2+b}\left(\frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{-b}{2}\right) - \frac{\zeta'}{\zeta}(-b) + \frac{1}{b} + \frac{1}{b+1}\right)$$

and

$$\sum_{\rho_\chi} \frac{1}{|\rho_\chi+b|^2} = \frac{1}{1/2+b}\left(\frac{1}{2}\log\left(\frac{\pi}{m}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{-b+\delta}{2}\right) - \mathrm{Re}\left(\frac{L'}{L}(-b,\chi)\right)\right),$$

where $\delta \in \{0,1\}$ *is the parity of* χ *and the sums run over nontrivial zeros counted with multiplicity.*

Proof. A more general formula of this kind is in [2, Lemma 5.6], where the Riemann Hypothesis is used to write

$$\frac{1}{\rho+b} + \frac{1}{\overline{\rho}+b} = \frac{2b+1}{|\rho+b|^2}$$

and similarly with ρ replaced by a nontrivial zero of $L(s,\chi)$ assuming the Generalized Riemann Hypothesis. Both sides should be multiplied by the order of the zero when we sum over all nontrivial zeros counting multiplicity. We will explain how to rewrite the formulas in our theorem in a way that matches [2, Lemma 5.6].

First we will rewrite the right side of both formulas in our theorem. Taking the logarithmic derivatives of both sides of the functional equations of the completed zeta-function and completed L-function,

$$\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) + \frac{\zeta'}{\zeta}(s) = \log\pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1-s}{2}\right) - \frac{\zeta'}{\zeta}(1-s)$$

and

$$\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\delta}{2}\right)+\frac{L'}{L}(s,\chi)=\log\left(\frac{\pi}{m}\right)-\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1-s+\delta}{2}\right)-\frac{L'}{L}(1-s,\overline{\chi})$$

Using $s=-b$ in these equations and taking real parts on both sides of the second equation, the right side of the first formula in the theorem is

$$\frac{1}{1/2+b}\left(-\frac{1}{2}\log\pi+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right)+\frac{\zeta'}{\zeta}(1+b)+\frac{1}{b}+\frac{1}{b+1}\right) \tag{5.2.7}$$

and the right side of the second formula in the theorem is

$$\frac{1}{1/2+b}\left(-\frac{1}{2}\log\left(\frac{\pi}{m}\right)+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b+\delta}{2}\right)+\operatorname{Re}\left(\frac{L'}{L}(1+b,\overline{\chi})\right)\right). \tag{5.2.8}$$

What we really need is not the individual formulas in this theorem, but their sum, since it is the sum of two sums over nontrivial zeros of $\zeta(s)$ and $L(s,\chi)$ that occurs on the right side of (5.1.18) and its special case (5.1.19) when $b=1/2$. Adding (5.2.7) and (5.2.8) produces the formula on the right side of [2, Lemma 5.6] with the following translation of notation from [2, pp. 360, 362]: ρ runs over nontrivial zeros of $\zeta(s)$ and $L(s,\chi)$ (with multiplicity), $\Delta=1$, $A_\chi=m$, $n=1$, $\alpha=1-\delta$, $\psi(s)=(\Gamma'/\Gamma)(s)$, and lastly

$$\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right)+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b+\delta}{2}\right)=\left(1-\frac{\delta}{2}\right)\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right)+\frac{\delta}{2}\frac{\Gamma'}{\Gamma}\left(1+\frac{b}{2}\right)$$

by a direct comparison when δ is 0 and 1. □

Now we can justify the bound $x=O((\log m)^2)$ in (5.1.20). It was based on

- $-\dfrac{L'}{L}\left(-\dfrac{1}{2},\chi\right) = \log m + O(1)$,
- $\left(\dfrac{L'}{L}\right)'\left(-\dfrac{1}{2},\chi\right) = O(1)$,
- $\displaystyle\sum_{\rho_\chi} \frac{1}{|\rho_\chi + 1/2|^2} = O(\log m)$ assuming the Generalized Riemann Hypothesis.

In (5.2.1) and (5.2.2) are formulas for $-(L'/L)(-1/2,\chi)$ and $(L'/L)'(-1/2,\chi)$. The right sides of those formulas use $(L'/L)(3/2,\overline{\chi})$ and $(L'/L)'(3/2,\overline{\chi})$, which are absolutely convergent Dirichlet series:

$$\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right) = -\sum_{n\geq 1}\frac{\overline{\chi}(n)\Lambda(n)}{n^{3/2}}, \quad \left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right) = \sum_{n\geq 1}\frac{\overline{\chi}(n)\Lambda(n)\log n}{n^{3/2}}.$$

Since $|\overline{\chi}(n)| \leq 1$,

$$\left|\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right| \leq \sum_{n\geq 1}\frac{\Lambda(n)}{n^{3/2}}, \quad \left|\left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\right| \leq \sum_{n\geq 1}\frac{\Lambda(n)\log n}{n^{3/2}}. \tag{5.2.9}$$

Therefore the right side of (5.2.1) is $\log m + O(1)$ and the right side of (5.2.2) is $O(1)$.

Assuming the Generalized Riemann Hypothesis. the second formula in Theorem 5.2.2 at $b = 1/2$ implies $\sum_{\rho_\chi} 1/|\rho_\chi + 1/2|^2 = -(1/2)\log m + O((L'/L)(-1/2,\chi))$ since $|\operatorname{Re}(z)| \leq |z|$. From $-(L'/L)(-1/2,\chi) = \log m + O(1)$, $\sum_{\rho_\chi} 1/|\rho_\chi + 1/2|^2 = O(\log m)$.

5.3 An explicit bound

Being more careful with estimates, we can convert the O-constants in our bounds into explicit numbers that fit the roles of A and B in part (2) of Theorem 5.1.2, leading to the next result.

Theorem 5.3.1. *For $m > 1$ and primitive $\chi \bmod m$, the Generalized Riemann Hypothesis implies $\chi(n) \neq 1$ for some positive integer n such that*

$$n \leq (1.125 \log(m) + 9.1558)^2 + 1.$$

If χ is not primitive, then the above bound still holds for m being the modulus of the primitive character of which χ is a lift.

The proof for this is in Section 5.4 for even χ and Appendix A.1 for odd χ. The bound we get for the least n such that $\chi(n) \neq 1$ when χ is even is a bit smaller than the bound when χ is odd.

Applying Theorem 5.3.1 to Theorem 5.1.2, each proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ omits an integer $n \leq (1.125 \log(m) + 9.1558)^2 + 1$. So for odd composite N, the proper subgroup of Solovay-Strassen nonwitnesses in $(\mathbb{Z}/N\mathbb{Z})^\times$ (which contains the Miller-Rabin nonwitnesses) omits an integer that is at most $(1.125 \log(N) + 9.1558)^2 + 1$. Therefore, if we assume the Generalized Riemann Hypothesis, we only have to search for witnesses for the Miller-Rabin test or Solovay-Strassen test on an odd $N > 1$ up to $(1.125 \log(N) + 9.1558)^2 + 1$. In this range, all odd composite N have a witness for both tests and all odd prime N do not.

Our proof of Theorem 5.3.1 is based on work of Bach [2, p. 373], who was more careful with estimates in a few places and achieved the upper bound

$$x \leq 2(\log m)^2.$$

Comparing Theorem 5.3.1 to the bound by Bach, we can find for which values of m

our calculated bound is lower than $2(\log m)^2$. Setting

$$(1.125 \log m + 9.1558)^2 + 1 = 2(\log m)^2,$$

the bound we work out becomes sharper for m above approximately 5.6×10^{13}, or about 56 trillion. For the size of primes that are used in cryptography (on the order of 10^{300}), our bound gives a shorter range to test for deterministic primality testing than the bound $2(\log m)^2$, assuming the Generalized Riemann Hypothesis. In practice, the Miller-Rabin test is used around 50 times as a probabilistic test.

Example 5.3.2. In Rabin's paper [11, p. 136], $N = 2^{400} - 593$ is an example of a number expected to be prime by the probabilistic form of the Miller-Rabin test. Since

$$(1.125 \log(N) + 9.1558)^2 + 1 \approx 103088.24,$$

the Generalized Riemann Hypothesis implies N is prime if it has no Miller-Rabin witnesses in the interval $[1, 103088]$. It took a personal computer 37 seconds to run the Miller-Rabin test for N on that range of values, concluding that N is prime under the Generalized Riemann Hypothesis. Bach's bound for this number is $2(\log N)^2 \approx 153744.96$.

Bach showed in [2, Theorem 1] that the coefficient 2 in his bound can be taken arbitrarily close to 1 from above for sufficiently large m: for each $\varepsilon > 0$ and all sufficiently large m depending on ε, each primitive character mod m is not 1 at some positive integer below $(1 + \varepsilon)(\log m)^2$. We will explain this in Section 5.5.

5.4 Bounding x for even characters

Let's return to (5.1.19): it tells us that if the Generalized Riemann Hypothesis is true and a primitive character χ mod m, where $m > 1$, has $\chi(n) = 1$ for $1 \leq n \leq x$ then

$$\begin{align}
\frac{4}{9}x &\leq \left(\sum_{\rho} \frac{1}{|\rho+\frac{1}{2}|^2} + \sum_{\rho_\chi} \frac{1}{|\rho_\chi+\frac{1}{2}|^2}\right)\sqrt{x} + \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| \tag{5.4.1}\\
&\qquad + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} + 4 \nonumber\\
&= A_\chi\sqrt{x} + B_\chi, \tag{5.4.2}
\end{align}$$

where A_χ and B_χ are the following positive numbers:

$$A_\chi = \sum_{\rho} \frac{1}{\left|\rho+\frac{1}{2}\right|^2} + \sum_{\rho_\chi} \frac{1}{\left|\rho_\chi+\frac{1}{2}\right|^2},$$

$$B_\chi = \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} + 4.$$

The numbers A_χ and B_χ are independent of x, so the inequality $(4/9)x \leq A_\chi x + B_\chi$ puts an upper bound on x that depends on χ. The following two theorems give us upper bounds on A_χ and B_χ that depend on χ only through its modulus.

Theorem 5.4.1. *For nontrivial primitive even* χ mod m*,*

$$A_\chi < \frac{1}{2}\log(m) + 0.436076.$$

Proof. By Theorem 5.2.2 at $b = 1/2$, the two series in the definition of A_χ are

$$\sum_{\rho} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} = \frac{1}{2}\log(\pi) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) + 2 + \frac{2}{3},$$
$$\sum_{\rho_\chi} \frac{1}{\left|\rho_\chi + \frac{1}{2}\right|^2} = \frac{1}{2}\log(\pi) - \frac{1}{2}\log(m) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \mathrm{Re}\left(\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right)$$

Adding these formulas together,

$$A_\chi = \log(\pi) + \frac{8}{3} - \frac{1}{2}\log(m) - \frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) - \mathrm{Re}\left(\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right). \quad (5.4.3)$$

From Theorem 5.2.1,

$$\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) + \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) = \log(\pi) + 2 - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right), \quad (5.4.4)$$

and $(\zeta'/\zeta)(3/2)$ can be computed using the absolutely convergent Dirichlet series for $(\zeta'/\zeta)(s)$ at $s = 3/2$, since $3/2 > 1$. Substituting (5.4.4) into (5.4.3) and simplifying,

$$A_\chi = -\frac{1}{2}\log(m) + \frac{2}{3} + \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) - \mathrm{Re}\left(\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right). \quad (5.4.5)$$

To bound the negative of the real part of $(L'/L)(-1/2, \chi)$, we could use the inequality $-\mathrm{Re}(z) \le |z|$ for $z = (L'/L)(-1/2, \chi)$, but that brings in an absolute value sooner than necessary. Instead, let's apply the functional equation for L-functions to express $(L'/L)(-1/2, \chi)$ in terms of $(L'/L)(3/2, \overline{\chi})$: using (5.2.1) with $\delta = 0$,

$$-\frac{L'}{L}\left(-\frac{1}{2}, \chi\right) = \log(m) - \log(2\pi) + \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) + \frac{\pi}{2} + \frac{L'}{L}\left(\frac{3}{2}, \overline{\chi}\right).$$

All terms on the right side are real except perhaps the last term, so when we take the real part of both sides,

$$-\operatorname{Re}\left(\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right)=\log(m)-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\pi}{2}+\operatorname{Re}\left(\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right). \quad (5.4.6)$$

Using the right side of (5.4.6) in place of the last term in (5.4.5) and using the bound $\operatorname{Re}(z)\le|z|$ for $z=(L'/L)(3/2,\overline{\chi})$, we get

$$\begin{aligned}A_\chi &= -\frac{1}{2}\log(m)+\frac{2}{3}+\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)+\log(m)-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\pi}{2}+\operatorname{Re}\left(\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right)\\ &\le \frac{1}{2}\log(m)+\frac{2}{3}+\frac{\pi}{2}-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)+\left|\left(\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right)\right|.\end{aligned}$$

Using the Dirichlet series for $(L'/L)(3/2,\overline{\chi})$, $|(L'/L)(3/2,\overline{\chi})|\le|(\zeta'/\zeta)(3/2)|$. So

$$A_\chi\le\frac{1}{2}\log(m)+\frac{2}{3}+\frac{\pi}{2}-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)+\left|\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|. \quad (5.4.7)$$

Since $(\zeta'/\zeta)(s)<0$ for $s>1$, by its Dirichlet series (all terms are negative), the last two terms in (5.4.7) *cancel*. Using the estimate $(\Gamma'/\Gamma)(3/2)\approx 0.036489973978$, we get $2/3+\pi/2-\log(2\pi)+(\Gamma'/\Gamma)(3/2)\approx .436075901$, so

$$A_\chi<\frac{1}{2}\log(m)+0.436076. \qquad \square$$

Theorem 5.4.2. *For nontrivial primitive even* $\chi \bmod m$*,*

$$B_\chi<\frac{2}{e}\log(m)+14.55429899.$$

Proof. Recall that we had defined

$$B_\chi = \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} + 4.$$

From Theorem 5.2.1, we have estimates for the first two terms:

$$\left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| = \left|\left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right) - 4\right| \approx 0.1450370843, \tag{5.4.8}$$

$$\left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} = \left|\log(\pi) + 2 - \pi - \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|\frac{2}{e} \approx 1.27714948. \tag{5.4.9}$$

To estimate the terms involving L-functions, we use (5.2.1) with $\delta = 0$ and (5.2.2):

$$\frac{L'}{L}\left(-\frac{1}{2},\chi\right) = \log(2\pi) - \log(m) - \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) - \frac{\pi}{2} - \frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right) \tag{5.4.10}$$

$$\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right) = \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) - \frac{\pi^2}{2} + \left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right) \tag{5.4.11}$$

Recall $(\Gamma'/\Gamma)(3/2) \approx 0.036489973978$ from the end of the proof of Theorem 5.4.1. In Theorem 5.2.1 we showed that $(\Gamma'/\Gamma)'(3/2) - \pi^2/2 = -4$. Using these and the triangle inequality in (5.4.10) and (5.4.11),

$$\begin{aligned}\left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right| &\le \log m + \left|\log(2\pi) - \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) - \frac{\pi}{2}\right| + \left|\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right| \\ &\approx \log m + 0.2305907656 + \left|\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right| \\ &\approx \log m + 0.2305907656 + 1.5052353557 \\ &< \log m + 1.735826122 \end{aligned} \tag{5.4.12}$$

and

$$\left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| \le 4 + \left|\left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\right| \le 4 + \left|\left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right)\right|.$$

Since $|(\zeta'/\zeta)'(3/2)| \approx 3.8549629156$, adding 4 to this implies

$$\left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| < 7.8549629157. \tag{5.4.13}$$

Putting (5.4.8), (5.4.9), (5.4.12), and (5.4.13) into the definition of B_χ, we get

$$B_\chi < \frac{2}{e}\log(m) + 14.55429899. \qquad \square$$

Feeding the bounds on A_χ and B_χ in Theorems 5.4.1 and 5.4.2 into the inequality $(4/9)x \le A_\chi\sqrt{x} + B_\chi$,

$$\begin{aligned} x &\le \frac{9}{4}A_\chi\sqrt{x} + \frac{9}{4}B_\chi \\ &< \left(\frac{9}{8}\log(m) + \frac{9}{4}0.436076\right)\sqrt{x} + \frac{9}{4}\left(\frac{2}{e}\log(m) + 14.55429899\right) \\ &< \left(\frac{9}{8}\log(m) + 0.981171\right)\sqrt{x} + \left(\frac{9}{2e}\log(m) + 32.74717273\right). \end{aligned}$$

Let $y = \sqrt{x}$, so we are looking at the quadratic inequality

$$y^2 - \left(\frac{9}{8}\log(m) + 0.981171\right)y - \left(\frac{9}{2e}\log(m) + 32.74717273\right) < 0.$$

We now look at this problem in the form

$$y^2 - (C\log(m) + D)y - (C'\log(m) + D') < 0, \tag{5.4.14}$$

where $C = 9/8$, $D = 0.981171$, $C' = 9/(2e)$, and $D' = 32.74717273$. Such y must be less than the larger real root of the quadratic polynomial in y on the left side of the inequality, so

$$y < \frac{(C\log(m) + D) + \sqrt{(C\log(m) + D)^2 + 4(C'\log(m) + D')}}{2}. \tag{5.4.15}$$

To simplify the expression under the square root, we complete the square:

$$\begin{aligned}
&(C\log(m) + D)^2 + 4(C'\log(m) + D') \\
&= C^2(\log(m))^2 + 2CD\log(m) + D^2 + 4C'\log(m) + 4D' \\
&= C^2\left((\log(m))^2 + 2\left(\frac{CD + 2C'}{C^2}\right)\log(m) + \frac{D^2 + 4D'}{C^2}\right) \\
&= C^2\left(\left(\log(m) + \frac{CD + 2C'}{C^2}\right)^2 + \frac{D^2 + 4D'}{C^2} - \frac{(CD + 2C')^2}{C^4}\right) \\
&= C^2\left(\left(\log(m) + \frac{CD + 2C'}{C^2}\right)^2 + \frac{4}{C^2}\left(D' - D\frac{C'}{C} - \left(\frac{C'}{C}\right)^2\right)\right).
\end{aligned}$$

Using the values of C, D, C', and D' above, $D' - D(C'/C) - (C'/C)^2 \approx 29.13$, which is positive. Since $\sqrt{a+b} < \sqrt{a} + \sqrt{b}$ for positive a and b, from (5.4.15) we get

$$\begin{aligned}
y &< \frac{C}{2}\log(m) + \frac{D}{2} + \frac{C}{2}\left(\sqrt{\left(\log(m) + \frac{CD + 2C'}{C^2}\right)^2} + \frac{2}{C}\sqrt{D' - D\frac{C'}{C} - \left(\frac{C'}{C}\right)^2}\right) \\
&= \frac{C}{2}\log(m) + \frac{D}{2} + \frac{C}{2}\left(\log(m) + \frac{CD + 2C'}{C^2}\right) + \sqrt{D' - D\frac{C'}{C} - \left(\frac{C'}{C}\right)^2} \\
&= C\log(m) + \left(D + \frac{C'}{C} + \sqrt{D' - D\frac{C'}{C} - \left(\frac{C'}{C}\right)^2}\right).
\end{aligned} \tag{5.4.16}$$

Using the values for C, D, C', and D', the expression in parentheses is around 7.850651, so $y < 1.125\log(m) + 7.850652$. Since $y = \sqrt{x}$, squaring both sides gives us an upper bound on x:

$$x < (1.125\log(m) + 7.80652)^2.$$

The calculations for odd characters, which have some different estimates due to $\delta = 1$, are in Appendix A.1. It turns out that the bound on x for odd characters is larger: $x < (1.125\log(m) + 9.1558)^2$. In order to have a single bound for the even and odd cases, we use the larger of the two bounds. So if we assume the Generalized Riemann Hypothesis, an overall bound on x when $\chi(n) = 1$ for $1 \leq n \leq x$ and χ is a nontrivial primitive character mod m (even or odd) is

$$x < (1.125\log(m) + 9.1558)^2. \tag{5.4.17}$$

5.5 Reducing the coefficient of log m

In Section 5.4 and Appendix A.1 we compute a bound on the maximum possible x such that $\chi(n) = 1$ for all integers n in $[1, x]$ when χ is a nontrivial primitive character, assuming the Generalized Riemann Hypothesis. We did this through the use of Theorems 5.1.7 and 5.2.2 with $b = 1/2$ in order to get an explicit upper bound on x. Let's return to the setting of arbitrary b in $(0, 1)$, to see how varying b affects the upper bound on x.

In Appendix A.2 we will show that x is less than

$$\left(\frac{(1+b)^2}{1+2b}\log m + \left(D_{b,\delta} + \frac{1}{be} + \frac{2}{e} + \sqrt{D'_{b,\delta} - \frac{(be+2b^2e)D_{b,\delta} - 1 - 4b - 4b^2}{b^2e^2}}\right)\right)^2, \tag{5.5.1}$$

where

$$D_{b,\delta} = \frac{(1+b)^2}{1+2b}\left[\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) + 2\frac{\Gamma'}{\Gamma}(1+b) - \frac{\Gamma'}{\Gamma}\left(1+\frac{-b+\delta}{2}\right)\right.$$
$$\left. -\pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - 2\log(2\pi) - \frac{2}{b-\delta} + \frac{2}{b} + \frac{2}{b+1}\right]$$

and

$$D'_{b,\delta} = \left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be} + \left|\left(\frac{\Gamma'}{\Gamma}\right)'(1+b) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi}{2}(1+b-\delta)\right)\right|$$
$$+ \left|\left(\frac{\zeta'}{\zeta}\right)'(1+b)\right| + \left|\frac{\zeta'}{\zeta}(1+b)\right|\frac{1}{be}$$
$$+ \left|\frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - \log(2\pi)\right|\frac{1}{be} + \frac{1}{(b-\delta)^2}.$$

In (5.5.1), the coefficient of $\log(m)$ for $b = 1/2$ is the familiar $9/8 = 1.125$ that we have seen before. As a function of b, $(1+b)^2/(1+2b)$ for $0 \le b \le 1$ is increasing and continuous, so for b near 0 this value is very close to 1 from above. Therefore by bounding x using b close to 0 instead of $b = 1/2$, we can make the coefficient of $\log(m)$ arbitrarily close to 1. At the same time, the complicated expression after the $\log(m)$-term in (5.5.1), which depends on b, gets very large as b gets close to 0: it is a sum of positive terms and the second term is $1/(be)$.

Remark 5.5.1. At $b = 1/2$, using the numerical values $(\zeta'/\zeta)(3/2) \approx -1.5052353557$ and $(\zeta'/\zeta)'(3/2) \approx 3.854962915676$ from computer software gives us

$$D_{1/2,0} \approx 0.981171, \qquad D'_{1/2,0} \approx 14.554299,$$

and

$$D_{1/2,1} \approx 1.649942, \qquad D'_{1/2,1} \approx 16.865753$$

which implies the (overall) bound $x < (1.125 \log m + 7.196162)^2$. That is slightly smaller than the bound on x in (5.4.17).

In Appendix A.2, we calculate the values of $|(\zeta'/\zeta)(s)|$ and $|(\zeta'/\zeta)'(s)|$ at select points with $\mathrm{Re}(s) > 1$. We present those here:

b	$s = b+1$	$(\zeta'/\zeta)(s)$	$(\zeta'/\zeta)'(s)$
$1/4$	$5/4$	-3.4666544812	15.835789189977
$1/2$	$3/2$	-1.5052353557	3.854962915676
$3/4$	$7/4$	-0.8727702750	1.6487381284572

We use these to calculate different bounds on x when $\chi(n) = 1$ for $1 \le n \le x$ and χ is a nontrivial primitive even character mod m. (The case of odd χ changes the constants only slightly, as it did when we considered $b = 1/2$). Using computational software, here are approximate values for $D_{b,0}$ and $D'_{b,0}$.

b	$D_{b,0}$	$D'_{b,0}$
$1/4$	4.588669478	62.95641488
$1/2$	0.981171	14.554299
$3/4$	-10.9928266	7.8091676

With these, we can calculate constants in the bound on x using each b and $\delta = 0$: Let $A_{b,\delta}$ and $B_{b,\delta}$ be the coefficient of $\log m$ and the constant term in (5.5.1), respectively. Then for even χ we have $x < (A_{b,0} \log m + B_{b,0})^2$ for the following b.

b	A_b	B_b	$x < (A_{b,0} \log m + B_{b,0})^2$
$1/4$	1.042	13.028103	$x < (1.042 \log m + 13.028103)^2$
$1/2$	1.125	6.497279	$x < (1.125 \log m + 6.497279)^2$
$3/4$	1.225	2.177631	$x < (1.225 \log m + 2.177631)^2$

Example 5.5.2. Using $N = 2^{400} - 593$ from Example 5.3.2, let's see how the above bounds affect how many x we must check up to in a deterministic Miller-Rabin test for N. The number $-1 \bmod N$ is a Miller-Rabin nonwitness for N, so a nontrivial Dirichlet character mod N that is trivial on a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ containing the Miller-Rabin nonwitnesses for N will be a nontrivial even character mod N. That character is the lift of a nontrivial primitive even character mod m for some m dividing N. Since $m \leq N$, the x-bounds in the table plus 1 with $\log m$ replaced by $\log N$ is how far we have to search for Miller-Rabin witnesses for N if the Generalized Riemann Hypothesis is true.

1. For $b = 1/4$, we see $(1.042 \log N + 13.028103)^2 + 1 \approx 91163.8$, so the Generalized Riemann Hypothesis implies that N is prime if it has no Miller-Rabin witnesses in the interval $[1, 91163]$.

2. For $b = 1/2$, we see $(1.125 \log N + 6.497279)^2 + 1 \approx 101388.1$, so the Generalized Riemann Hypothesis implies that N is prime if it has no Miller-Rabin witnesses in the interval $[1, 101388]$.

3. For $b = 3/4$, we see $(1.225 \log N + 2.177631)^2 + 1 \approx 116841.7$, so the Generalized Riemann Hypothesis implies that N is prime if it has no Miller-Rabin witnesses in the interval $[1, 116841]$.

For this N, using the first bound results in the least number of computations among the three choices of b.

How does the choice of b affect $A_{b,\delta}$ and $B_{b,\delta}$ in the bound $x < (A_{b,\delta} \log m + B_{b,\delta})^2$ when $b \to 0$ and $b \to 1$? When $b \to 0$, the coefficient of $\log m$ gets smaller, and in fact $A_{0,\delta} = 1$. However, the constant term $B_{b,\delta}$ grows, and in fact it will get arbitrarily large since terms in $D_{b,\delta}$ and $D'_{b,\delta}$ have poles at $b = 0$ that are not canceled out. If instead we let $b \to 1$, then the coefficient of $\log m$ tends to $4/3 \approx 1.333$ and there are no poles in the terms making up $B_{b,0}$ at $b = 0$, but terms in $B_{b,1}$ have poles at $b = 1$ that don't get canceled out.

Since $(1+b)^2/(1+2b)$ is increasing from 1 at $b = 0$ to $4/3$ at $b = 1$, for $\varepsilon \in (0, 1/3)$ we may choose small $b \in (0, 1)$ satisfying

$$\frac{(1+b)^2}{1+2b} < 1 + \varepsilon.$$

Writing this as a quadratic inequality in the positive number b, it is equivalent to $0 < b < \varepsilon + \sqrt{\varepsilon(1+\varepsilon)}$. (For example, $b = 2\varepsilon$ fits this inequality.) For such b, we have the bound $x < ((1+\varepsilon)\log m + C_\varepsilon)^2$ for a constant C_ε depending on ε. In this way we can get an arbitrarily small coefficient of $\log m$ at the cost of a constant term getting larger. In effect, this will get us a very efficient primality test for sufficiently large N (depending on ε), but it may not be a good bound for smaller N. In general, a smaller coefficient of $\log N$ and a larger constant term means we will have tighter bounds on large N but worse bounds on small N.

Appendix A

Further calculations

A.1 Bounding x for odd characters

For odd primitive χ mod m, if $\chi(n) = 1$ for $1 \leq n \leq x$ then (5.1.19) at $b = 1/2$ is

$$\begin{aligned}\frac{4}{9}x \leq &\left(\sum_{\rho} \frac{1}{|\rho + \frac{1}{2}|^2} + \sum_{\rho_\chi} \frac{1}{|\rho_\chi + \frac{1}{2}|^2}\right)\sqrt{x} + \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| &\text{(A.1.1)}\\ &+ \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2}, \chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right|\frac{2}{e} + 4,\\ = A_\chi\sqrt{x} + B_\chi, & &\text{(A.1.2)}\end{aligned}$$

where A_χ and B_χ are the following positive numbers:

$$\begin{aligned}A_\chi &= \sum_{\rho} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} + \sum_{\rho_\chi} \frac{1}{\left|\rho_\chi + \frac{1}{2}\right|^2},\\ B_\chi &= \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2}, \chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right|\frac{2}{e} + 4.\end{aligned}$$

This is the same inequality as for even χ, but when χ is odd our estimates on terms involving χ will be a bit different than in the even case due to the different functional equation for $L(s, \chi)$ when χ is odd.

The following two lemmas give explicit bounds on A_χ and B_χ.

Lemma A.1.1. *For odd primitive* $\chi \bmod m$*,* $A_\chi < (1/2)\log(m) + 0.8652795743$.

Proof. We use Theorem 5.2.2 at $b = 1/2$ to estimate the sums in A_χ:

$$\sum_\rho \frac{1}{\left|\rho + \frac{1}{2}\right|^2} = \frac{1}{2}\log(\pi) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) + 2 + \frac{2}{3}$$

and

$$\sum_{\rho_\chi} \frac{1}{\left|\rho_\chi + \frac{1}{2}\right|^2} = \frac{1}{2}\log(\pi) - \frac{1}{2}\log(m) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) - \mathrm{Re}\left(\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right).$$

Adding these two together,

$$A_\chi = \log(\pi) + \frac{8}{3} - \frac{1}{2}\log(m) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) - \mathrm{Re}\left(\frac{L'}{L}\left(-\frac{1}{2}, \chi\right)\right).$$

Using the formulas for $(\Gamma'/\Gamma)(-1/4)$, $(\Gamma'/\Gamma)(1/4)$, and $(\zeta'/\zeta)(-1/2)$ in Theorem 5.2.1, we get

$$-\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{1}{4}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) - \frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right) = \frac{\pi}{2} - \log(\pi) + \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right). \tag{A.1.3}$$

The number $3/2$ is in the half-plane of absolute convergence for the Dirichlet series for $(\zeta'/\zeta)(s)$, so we can estimate its value there computationally.

This leaves us with bounding the real part of the logarithmic derivative of the

L-function. Using the identity in (5.2.1), we can pull the real parts out as follows:

$$\begin{aligned}-\operatorname{Re}\left(\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right) &= -\operatorname{Re}\left(-\log(m)+\log(2\pi)-\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)-\frac{\pi}{2}-\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right)\\ &= \log(m)-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)-\frac{\pi}{2}+\operatorname{Re}\left(\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right).\end{aligned}$$

Substituting this formula and (A.1.3) into the last term of the expression for A_χ, we get

$$A_\chi = \frac{1}{2}\log(m)+\frac{8}{3}-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)+\operatorname{Re}\left(\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right).$$

Since $\operatorname{Re}(z) \le |\operatorname{Re}(z)| \le |z|$ for complex z, we can bound the sum above by replacing the final term by $|(L'/L)(3/2,\overline{\chi})|$. Since $3/2 > 1$, comparing the Dirichlet series for $(L'/L)(s)$ and $(\zeta'/\zeta)(s)$ at $s = 3/2$ shows $|(L'/L)(3/2,\overline{\chi})| \le |(\zeta'/\zeta)(3/2)|$. Therefore

$$A_\chi \le \frac{1}{2}\log(m)+\frac{8}{3}-\log(2\pi)+\frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right)+\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)+\left|\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|.$$

Since $(\zeta'/\zeta)(s) < 0$ for $s > 1$, by its Dirichlet series, the last two terms above *cancel* Using the estimate $(\Gamma'/\Gamma)(3/2) \approx 0.036489973978$, we get $8/3 - \log(2\pi) + (\Gamma'/\Gamma)(3/2) \approx 0.8652795742$, so

$$A_\chi < \frac{1}{2}\log(m) + 0.8652795743. \qquad \square$$

Lemma A.1.2. *For odd primitive* $\chi \bmod m$*,* $B_\chi < (2/e)\log(m) + 16.86575368$*.*

Proof. Let's recall the definition of B_χ:

$$B_\chi = \left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| + \left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} + \left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| + \left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} + 4.$$

From Theorem 5.2.1, we have formulas for the first two terms. To estimate the L-function terms, we use identities for logarithmic derivatives of L-functions in (5.2.1) and (5.2.2) for odd primitive χ to get

$$\frac{L'}{L}\left(-\frac{1}{2},\chi\right) = \log(2\pi) - \log(m) - \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) + \frac{\pi}{2} - \frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)$$

$$\begin{aligned}\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right) &= \left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{3}{2}\right) - \frac{\pi^2}{2} + \left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\\ &= -4 + \left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\end{aligned}$$

since $(\Gamma'/\Gamma)'(3/2) - \pi^2/2 = -4$ by Theorem 5.2.1. We also previously computed $(\Gamma'/\Gamma)(3/2) \approx 0.036489973978$. Using this and then the triangle inequality,

$$\left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right| \leq \log(m) + \left|\log(2\pi) - \frac{\Gamma'}{\Gamma}\left(\frac{3}{2}\right) + \frac{\pi}{2}\right| + \left|\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right|$$

The number inside the absolute values on the right is around 3.372183419, so

$$\left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right| < \log(m) + 3.37218342 + \left|\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right|.$$

Also by the triangle inequality,

$$\left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| \leq 4 + \left|\left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\right|.$$

Using Dirichlet series at 3/2,

$$\left|\frac{L'}{L}\left(\frac{3}{2},\overline{\chi}\right)\right| \leq \left|\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|, \quad \left|\left(\frac{L'}{L}\right)'\left(\frac{3}{2},\overline{\chi}\right)\right| \leq \left|\left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right)\right|.$$

Using the estimates $|(\zeta'/\zeta)(3/2)| \approx 1.5052353557$ and $(\zeta'/\zeta)'(3/2) \approx 3.8549629156$, we can bound the individual parts of B_χ:

$$\begin{aligned}
\left|\left(\frac{\zeta'}{\zeta}\right)'\left(-\frac{1}{2}\right)\right| &= \left|\left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right) - 4\right| < 0.1450370844,\\
\left|\frac{\zeta'}{\zeta}\left(-\frac{1}{2}\right)\right|\frac{2}{e} &= \left|\log(\pi) + 2 - \pi - \frac{\Gamma'}{\Gamma}\left(\frac{5}{4}\right) - \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|\frac{2}{e} < 1.27714949,\\
\left|\left(\frac{L'}{L}\right)'\left(-\frac{1}{2},\chi\right)\right| &\leq 4 + \left|\left(\frac{\zeta'}{\zeta}\right)'\left(\frac{3}{2}\right)\right| < 7.8549629157,\\
\left|\frac{L'}{L}\left(-\frac{1}{2},\chi\right)\right|\frac{2}{e} &< \left[\log(m) + 3.37218342 + \left|\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)\right|\right]\frac{2}{e}\\
&< \frac{2}{e}\log(m) + 3.5886041872.
\end{aligned}$$

Adding these all together (with the additional 4 from the beginning), we have a final bound:

$$B_\chi < \frac{2}{e}\log(m) + 16.86575368. \qquad \square.$$

Using the upper bounds on A_χ and B_χ for odd primitive $\chi \bmod m$, we get an upper bound on x:

$$x < \sqrt{x}\left(\frac{9}{8}\log(m) + 1.94687904218\right) + \left(\frac{9}{2e}\log(m) + 37.94794579\right). \tag{A.1.4}$$

Let $y = \sqrt{x}$. Then we may form a quadratic inequality

$$y^2 - \left(\frac{9}{8}\log(m) + 1.94687904218\right)y - \left(\frac{9}{2e}\log(m) + 37.94794579\right) < 0.$$

As in the case of even characters, view this inequality as a special case of

$$y^2 - (C\log(m) + D)y - (C'\log(m) + D') < 0,$$

where $C = 9/8$, $D = 1.94687904218$, $C' = 9/(2e)$, and $D' = 37.94794579$. The argument leading to (5.4.16) remains valid here, so

$$y < C\log(m) + \left(D + \frac{C'}{C} + \sqrt{D' - D\frac{C'}{C} - \frac{C'^2}{C^2}}\right) < \frac{9}{8}\log(m) + 9.15579293.$$

Since $y = \sqrt{x}$, we get the bound

$$x < (1.125\log(m) + 9.15579293)^2 < (1.125\log(m) + 9.1558)^2.$$

A.2 General b Calculations

We want to calculate the maximum value of x satisfying

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s)\,\frac{x^s}{(s+b)^2}\,ds = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^s}{(s+b)^2}\,ds,$$

keeping b general in the interval $(0,1)$ throughout our calculations. We will consider $\zeta(s)$ and $\zeta'(s)$ to be calculable in the region $\mathrm{Re}(s) > 1$ and $\Gamma(s)$ and $\Gamma'(s)$ to be calculable in the region $\mathrm{Re}(s) > 0$, as each is defined in their respective regions by an absolutely convergent formula (series or integral). We will bound the L-function by the zeta function when possible, but we will keep $\delta \in \{0,1\}$ general.

Assume the Generalized Riemann Hypothesis, so $|x^\rho| = |x^{\rho_\chi}| = \sqrt{x}$ for all nontrivial zeros ρ of the zeta function and all nontrivial zeros ρ_χ of the L-function of the primitive character χ. By Theorem 5.1.7, we can express the above integrals as the sums of their residues. Specifically, our calculations from Section 5.1 are entirely general up to (5.1.18), which we start with here:

$$\begin{aligned}\frac{x}{(1+b)^2} &\le \left(\sum_{\rho}\frac{1}{|\rho+b|^2}+\sum_{\rho_\chi}\frac{1}{|\rho_\chi+b|^2}\right)\sqrt{x}+\left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| \\ &\quad +\left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be}+\left|\left(\frac{L'}{L}\right)'(-b,\chi)\right|+\left|\frac{L'}{L}(-b,\chi)\right|\frac{1}{be}+\frac{1}{(b-\delta)^2} \\ &= A_{b,\chi}\sqrt{x}+B_{b,\chi},\end{aligned}$$

where

$$A_{b,\chi}=\sum_{\rho}\frac{1}{|\rho+b|^2}+\sum_{\rho_\chi}\frac{1}{|\rho_\chi+b|^2} \tag{A.2.1}$$

and

$$B_{b,\chi}=\left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right|+\left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be}+\left|\left(\frac{L'}{L}\right)'(-b,\chi)\right|+\left|\frac{L'}{L}(-b,\chi)\right|\frac{1}{be}+\frac{1}{(b-\delta)^2}. \tag{A.2.2}$$

All terms in $B_{b,\chi}$ are positive, and the second term, which is independent of χ, tends to ∞ as $b \to 0^+$ since $(\zeta'/\zeta)(0) \in \mathbb{C}^\times$, so $B_{b,\chi} \to \infty$ as $b \to 0^+$.

Lemma A.2.1. *For $0 < b < 1$ and a nontrivial primitive character $\chi \bmod m$,*

$$\begin{aligned}A_{b,\chi} < \frac{1}{1+2b}\log m+\frac{1}{1+2b}&\left[\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right)+2\frac{\Gamma'}{\Gamma}(1+b)-\frac{\Gamma'}{\Gamma}\left(1+\frac{-b+\delta}{2}\right)\right. \\ &\left.-\pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right)-2\log(2\pi)-\frac{2}{b-\delta}+\frac{2}{b}+\frac{2}{b+1}\right].\end{aligned}$$

Proof. By Theorem 5.2.2, $A_{b,\chi}$ equals

$$\frac{1}{1+2b}\left[2\log\pi-\log m-\frac{\Gamma'}{\Gamma}\left(-\frac{b}{2}\right)-\frac{\Gamma'}{\Gamma}\left(\frac{-b+\delta}{2}\right)-2\frac{\zeta'}{\zeta}(-b)-2\operatorname{Re}\left(\frac{L'}{L}(-b,\chi)\right)+\frac{2}{b}+\frac{2}{b+1}\right].$$

Substitute into this the formula

$$\frac{\zeta'}{\zeta}(-b) = \log \pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{b}{2}\right) - \frac{\zeta'}{\zeta}(1+b)$$

from (2.4.3) when $s = -b$: $A_{b,\chi}$ equals

$$\frac{1}{1+2b}\left[-\log m - \frac{\Gamma'}{\Gamma}\left(\frac{-b+\delta}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) + 2\frac{\zeta'}{\zeta}(1+b) - 2\,\mathrm{Re}\left(\frac{L'}{L}(-b,\chi)\right) + \frac{2}{b} + \frac{2}{b+1}\right].$$

Substitute into the last term the formula

$$-\frac{L'}{L}(-b,\chi) = \log m - \log(2\pi) + \frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(1+b-\delta)\right) + \frac{L'}{L}(1+b,\overline{\chi})$$

from (5.2.6) when $s = 1+b$: all terms in this equation are real-valued except the L-function expressions on the left and right, so

$$\begin{aligned} A_{b,\chi} = \frac{1}{1+2b}\Bigg[&\log m - 2\log(2\pi) - \frac{\Gamma'}{\Gamma}\left(\frac{-b+\delta}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) + 2\frac{\Gamma'}{\Gamma}(1+b) \\ &-\pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right) + 2\frac{\zeta'}{\zeta}(1+b) - 2\,\mathrm{Re}\left(\frac{L'}{L}(1+b,\overline{\chi})\right) + \frac{2}{b} + \frac{2}{b+1}\Bigg]. \end{aligned}$$

In this formula, the sum of the zeta and L-function terms at $1+b$ is negative: for real $s > 1$,

$$\frac{\zeta'}{\zeta}(s) - \mathrm{Re}\left(\frac{L'}{L}(s,\overline{\chi})\right) = \sum_{n \geq 1} \frac{-1 + \mathrm{Re}(\overline{\chi}(n))}{n^s} < 0$$

since $\mathrm{Re}(\overline{\chi}(n)) \leq 1$ with equality if and only if $\overline{\chi}(n) = 1$ and $\overline{\chi}(n) \neq 1$ for some n

since χ is nontrivial. Thus

$$A_{b,\chi} < \frac{1}{1+2b}\left[\log m - 2\log(2\pi) - \frac{\Gamma'}{\Gamma}\left(\frac{-b+\delta}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) + 2\frac{\Gamma'}{\Gamma}(1+b) \right.$$
$$\left. -\pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right) + \frac{2}{b} + \frac{2}{b+1}\right],$$

The Γ-term at $(-b+\delta)/2$ can be rewritten using Γ-function values at a positive number whether δ is 0 or 1 by the formula $(\Gamma'/\Gamma)(s) = (\Gamma'/\Gamma)(s+1) - 1/s$ from (2.4.1) at $s = (-b+\delta)/2$:

$$A_{b,\chi} < \frac{1}{1+2b}\left[\log m - 2\log(2\pi) - \frac{\Gamma'}{\Gamma}\left(1+\frac{-b+\delta}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) \right.$$
$$\left. +2\frac{\Gamma'}{\Gamma}(1+b) - \pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - \frac{2}{b-\delta} + \frac{2}{b} + \frac{2}{b+1}\right]. \qquad \square$$

Lemma A.2.2. *For $0 < b < 1$,*

$$B_{b,\chi} \le \frac{1}{be}\log m + \left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be} + \left|\left(\frac{\Gamma'}{\Gamma}\right)'(1+b) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi}{2}(1+b-\delta)\right)\right|$$
$$+\left|\left(\frac{\zeta'}{\zeta}\right)'(1+b)\right| + \left|\frac{\zeta'}{\zeta}(1+b)\right|\frac{1}{be}$$
$$+\left|\frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - \log(2\pi)\right|\frac{1}{be} + \frac{1}{(b-\delta)^2},$$

where

$$\left(\frac{\zeta'}{\zeta}\right)'(-b) = \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1+b}{2}\right) - \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(1-\frac{b}{2}\right) - \frac{1}{b^2} + \left(\frac{\zeta'}{\zeta}\right)'(1+b)$$

and

$$\frac{\zeta'}{\zeta}(-b) = \log\pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(1-\frac{b}{2}\right) - \frac{1}{b} - \frac{\zeta'}{\zeta}(1+b)\,.$$

Proof. Let's recall the definition (A.2.2) of $B_{b,\chi}$:

$$B_{b,\chi} = \left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be} + \left|\left(\frac{L'}{L}\right)'(-b,\chi)\right| + \left|\frac{L'}{L}(-b,\chi)\right|\frac{1}{be} + \frac{1}{(b-\delta)^2}.$$

The first, second, and fifth terms here are in the inequality in the lemma. We will check the formulas in the lemma for the first two terms and then get upper bounds on the third and fourth terms involving L-function values.

First term. Letting $s=-b$ in (2.4.4), we have

$$\left(\frac{\zeta'}{\zeta}\right)'(-b) = \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1+b}{2}\right) - \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(-\frac{b}{2}\right) + \left(\frac{\zeta'}{\zeta}\right)'(1+b)\,.$$

By differentiating (2.4.1),

$$\left(\frac{\Gamma'}{\Gamma}\right)'(s) = \left(\frac{\Gamma'}{\Gamma}\right)'(s+1) + \frac{1}{s^2}.$$

Set $s=-b/2$ in this and substitute it into the formula for $(\zeta'/\zeta)'(-b)$ to get

$$\left(\frac{\zeta'}{\zeta}\right)'(-b) = \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(\frac{1+b}{2}\right) - \frac{1}{4}\left(\frac{\Gamma'}{\Gamma}\right)'\left(1-\frac{b}{2}\right) - \frac{1}{b^2} + \left(\frac{\zeta'}{\zeta}\right)'(1+b)\,. \quad \text{(A.2.3)}$$

Second term. By letting $s=-b$ in (2.4.3),

$$\frac{\zeta'}{\zeta}(-b) = \log\pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(-\frac{b}{2}\right) - \frac{\zeta'}{\zeta}(1+b)\,.$$

Use the formula $(\Gamma'/\Gamma)(s) = (\Gamma'/\Gamma)(s+1) - 1/s$ from (2.4.1) at $s = -b/2$ to get

$$\frac{\zeta'}{\zeta}(-b) = \log \pi - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(1 - \frac{b}{2}\right) - \frac{1}{b} - \frac{\zeta'}{\zeta}(1+b)\,. \tag{A.2.4}$$

Third term. From the derivative of (5.2.6), we have

$$\left(\frac{L'}{L}\right)'(1-s,\chi) = \left(\frac{\Gamma'}{\Gamma}\right)'(s) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi(s-\delta)}{2}\right) + \left(\frac{L'}{L}\right)'(s,\overline{\chi})\,.$$

Letting $s = 1+b$, we have by the triangle inequality

$$\begin{aligned}\left|\left(\frac{L'}{L}\right)'(-b,\chi)\right| &\leq \left|\left(\frac{\Gamma'}{\Gamma}\right)'(1+b) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi}{2}(1+b-\delta)\right)\right| + \left|\left(\frac{L'}{L}\right)'(1+b,\overline{\chi})\right| \\ &\leq \left|\left(\frac{\Gamma'}{\Gamma}\right)'(1+b) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi}{2}(1+b-\delta)\right)\right| + \left|\left(\frac{\zeta'}{\zeta}\right)'(1+b)\right| \end{aligned}\tag{A.2.5}$$

since $|(L'/L)'(s,\overline{\chi})| \leq |(\zeta'/\zeta)'(s)|$ for $s > 1$.

Fourth term. From (5.2.6) at $s = 1+b$,

$$-\frac{L'}{L}(-b,\chi) = \log m - \log(2\pi) + \frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(1+b-\delta)\right) + \frac{L'}{L}(1+b,\overline{\chi})\,.$$

Using the triangle inequality and the bound $|(L'/L)(s,\overline{\chi})| \leq |(\zeta'/\zeta)(s)|$ for real $s > 1$,

$$\begin{aligned}\left|\frac{L'}{L}(-b,\chi)\right| \leq \log m &+ \left|\frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi(1+b-\delta)}{2}\right) - \log(2\pi)\right| \\ &+ \left|\frac{\zeta'}{\zeta}(1+b)\right|.\end{aligned}\tag{A.2.6}$$

Fifth term. The final term in $B_{b,\chi}$, $1/(b-\delta)^2$, is fine as is.

Applying (A.2.3), (A.2.4), (A.2.5), and (A.2.6) to the definition of $B_{b,\chi}$ gives us the upper bound on $B_{b,\chi}$ in the lemma. □

To review, when χ mod m is a nontrivial primitive character with parity δ, $\chi(n) = 1$ for $1 \leq n \leq x$, and b is a parameter in $(0,1)$,

$$\frac{x}{(1+b)^2} \leq A_{b,\chi}\sqrt{x} + B_{b,\chi}, \tag{A.2.7}$$

where $A_{b,\chi}$ and $B_{b,\chi}$ are defined in (A.2.1) and (A.2.2) and are bounded above in terms of b, δ, and $\log m$ in Lemmas A.2.1 and A.2.2, respectively. Multiply both sides of (A.2.7) by $(1+b)^2$ and use the bounds on $A_{b,\chi}$ and $B_{b,\chi}$ from those lemmas to get

$$x < (C_b \log m + D_{b,\delta})\sqrt{x} + C'_b \log m + D'_{b,\delta}, \tag{A.2.8}$$

where $C_b = (1+b)^2/(1+2b)$, $C'_b = (1+b)^2/(be)$, and $D_{b,\delta}$ and $D'_{b,\delta}$ are the very complicated expressions from the bounds in Lemmas A.2.1 and A.2.2 that appear after the $\log m$ term:

$$\begin{aligned} D_{b,\delta} = \frac{(1+b)^2}{1+2b}\Bigg[&\frac{\Gamma'}{\Gamma}\left(\frac{1+b}{2}\right) + 2\frac{\Gamma'}{\Gamma}(1+b) - \frac{\Gamma'}{\Gamma}\left(1 + \frac{-b+\delta}{2}\right) \\ &-\pi\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - 2\log(2\pi) - \frac{2}{b-\delta} + \frac{2}{b} + \frac{2}{b+1}\Bigg], \end{aligned} \tag{A.2.9}$$

$$\begin{aligned} D'_{b,\delta} = &\left|\left(\frac{\zeta'}{\zeta}\right)'(-b)\right| + \left|\frac{\zeta'}{\zeta}(-b)\right|\frac{1}{be} + \left|\left(\frac{\Gamma'}{\Gamma}\right)'(1+b) - \frac{\pi^2}{4}\sec^2\left(\frac{\pi}{2}(1+b-\delta)\right)\right| \\ &+ \left|\left(\frac{\zeta'}{\zeta}\right)'(1+b)\right| + \left|\frac{\zeta'}{\zeta}(1+b)\right|\frac{1}{be} \\ &+ \left|\frac{\Gamma'}{\Gamma}(1+b) - \frac{\pi}{2}\tan\left(\frac{\pi}{2}(1+b-\delta)\right) - \log(2\pi)\right|\frac{1}{be} + \frac{1}{(b-\delta)^2}, \end{aligned} \tag{A.2.10}$$

where formulas for $(\zeta'/\zeta)'(-b)$ and $(\zeta'/\zeta)(-b)$ in terms of zeta-function values at $1+b$ are given in Lemma A.2.2.

As we did for the calculations where $b = 1/2$, let $y = \sqrt{x}$ to turn (A.2.8) into the quadratic inequality

$$y^2 - (C_b \log m + D_{b,\delta})y - (C_b' \log m + D_{b,\delta}') < 0.$$

To get an upper bound on y, and then on $x = y^2$, carry out the same steps as in the passage from the inequality (5.4.14) to the upper bound (5.4.16), getting

$$y < C_b \log m + \left(D_{b,\delta} + \frac{C_b'}{C_b} + \sqrt{D_{b,\delta}' - D_{b,\delta}\frac{C_b'}{C_b} - \frac{{C_b'}^2}{{C_b}^2}} \right) \tag{A.2.11}$$

provided that

$$D_{b,\delta}' - D_{b,\delta}\frac{C_b'}{C_b} - \frac{{C_b'}^2}{{C_b}^2} \geq 0 \tag{A.2.12}$$

for $0 < b < 1$ and $\delta \in \{0, 1\}$.

Remark A.2.3. At $b = 1/2$, the left side of (A.2.12) is positive (when $\delta = 0$, the left side is approximately 16.3587). Positivity can be checked at $b = 1/4$, $1/2$, and $3/4$ using zeta-values in the table below. Note that only $D_{b,\delta}'$ has ζ-terms.

b	$s = b + 1$	$(\zeta'/\zeta)(s)$	$(\zeta'/\zeta)'(s)$
$1/4$	$5/4$	-3.4666544812	15.835789189977
$1/2$	$3/2$	-1.5052353557	3.854962915676
$3/4$	$7/4$	-0.8727702750	1.6487381284572

We can check positivity of the left side (A.2.12) as $b \to 0^+$ and as $b \to 1^-$:

- Terms in $D_{b,\delta}$ that blow up at $b = 0$ only have at most a simple pole there, such as $2/b$, while some terms in $D_{b,\delta}'$ have a double pole at $b = 0$, such as $(\zeta'/\zeta)'(1 + b)$ (and $1/(b - \delta)^2$ when $\delta = 0$) and the double-pole terms don't cancel out. Therefore $D'_{b,\delta}$ grows at a faster rate as $b \to 0^+$ than $D_{b,\delta}$ as $b \to 0^+$, which means the left side of (A.2.12) tends to ∞ as $b \to 0^+$.

- When $\delta = 0$, all terms in $D_{b,\delta}$ and $D'_{b,\delta}$ are continuous at $b = 1$. At $b = 1$, we have $D_{1,0} \approx -0.591855$ and $D'_{1,0} \approx 6.105455$. Using these values (and $C'_1/C_1 = 3/e$), the left side of (A.2.12) is approximately 5.540631. Because this is positive, by continuity the left side of (A.2.12) is positive for b near 1 when $\delta = 0$.

  When $\delta = 1$, $D_{b,\delta}$ has some terms at $b = 1$ with at worst a simple pole (such as $2/(b-\delta)$), while $D'_{b,\delta}$ has the single double-pole term $1/(b-\delta)^2$, so the left side of (A.2.12) tends to ∞ as $b \to 1^-$ if $\delta = 1$.

Since $C'_b/C_b = 1/(be) + 2/e = (2b+1)/(be)$, substituting this into the bound (A.2.11) and writing $y = \sqrt{x}$, we have a final bound on x:

$$x < \left(\frac{(1+b)^2}{1+2b} \log m + \left(D_{b,\delta} + \frac{1}{be} + \frac{2}{e} + \sqrt{D'_{b,\delta} - \frac{(2b+1)(D_{b,\delta}be + 2b + 1)}{b^2e^2}} \right) \right)^2 ,$$

where $D_{b,\delta}$ and $D'_{b,\delta}$ are defined by (A.2.9) and (A.2.10).

Bibliography

[1] T. M. Apostol, “Analytic Number Theory,” Springer-Verlag, New York, 1976.

[2] E. Bach, *Explicit Bounds for Primality Testing and Related Problems*, Math. Comp. **191** (1990), 355–380.

[3] R. Crandall and C. Pomerance, “Prime Numbers: A Computational Perspective,” 2nd ed., Springer, New York, 2005.

[4] H. Davenport, “Multiplicative Number Theory,” 2nd ed., Springer-Verlag, New York, 1980.

[5] E. Hlawka, J. Schoissengeier, and R. Tascher, “Geometric and Analytic Number Theory,” Springer-Verlag, New York, 1991.

[6] A. E. Ingham, “The Ditribution of Prime Numbers,” Cambridge University Press, Cambridge, 1932.

[7] J. Katz and Y. Lindell, “Introduction to Modern Cryptography,” 2nd ed., CRC Press, Boca Raton, 2014.

[8] A. W. Knapp, “Elliptic Curves,” Princeton University Press, Princeton, 1992.

[9] G. Miller, *Riemann's Hypothesis and Tests for Primality*, J. Computer and Systems Sciences **13** (1976), 300-317.

[10] M. Overholt, "A Course in Analytic Number Theory," American Mathematical Society, Providence, 2014.

[11] M. O. Rabin, *Probabilistic Algorithm for Testing Primality*, J. Number Theory **12** (1980), 128-138.

[12] R. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21** (1978), 120-126.

[13] V. Shoup, "A Computational Introduction to Number Theory and Algebra," 2nd ed., Cambridge University Press, Cambridge, 2008.

[14] R. M. Solovay and V. Strassen, *A Fast Monte-Carlo Test for Primality*, SIAM Journal on Computing **6** (1977), 84-85.

[15] R. M. Solovay and V. Strassen, *Erratum: A Fast Monte-Carlo Test for Primality*, SIAM Journal on Computing **7** (1978), 1.

[16] N. Stanford, "Dirichlet's Theorem and Applications" (2013). University of Connecticut Honors Scholar Theses. 286. https://opencommons.uconn.edu/srhonors_theses/286

[17] E. M. Stein and R. Shakarchi, "Complex Analysis," Princeton University Press, Princeton, 2003.