Why is the Riemann Hypothesis Important?

Keith Conrad
University of Connecticut

August 11, 2016

1859: Riemann's Address to the Berlin Academy of Sciences

Bericht

über die

zur Bekanntmachung geeigneten Verhandlungen der Königl. Preuſs. Akademie der Wissenschaften zu Berlin

im Monat November 1859.

Vorsitzender Sekretar: Hr. Encke.

---

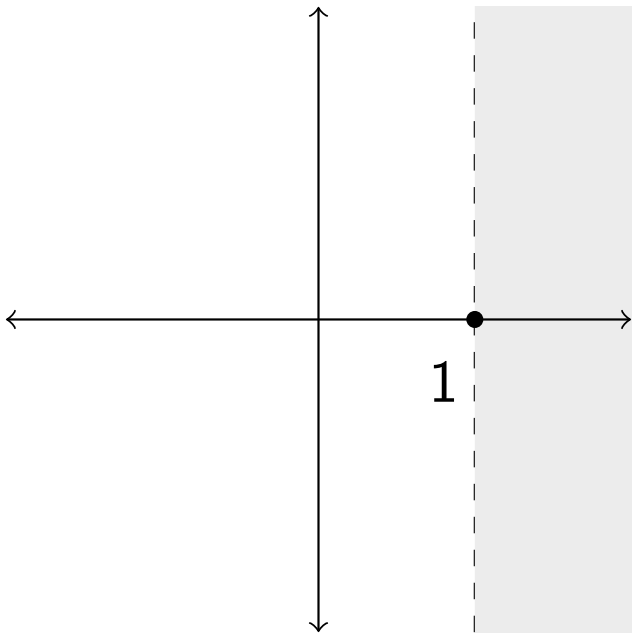
3. Nov. Gesammtsitzung der Akademie.

Hr. Steiner las über einige allgemeine Bestimmungsarten der Curven und Flächen zweiter Ordnung und daraus folgenden Sätzen.

Hierauf trug Hr. Kummer folgende von Hrn. Riemann, Correspondenten der Akademie, mittelst eines an den Sekretar Hrn. Encke gerichteten Schreibens vom 19. October d. J. eingesandte Mittheilung „über die Anzahl der Primzahlen unter einer gegebenen Gröfse" vor:

The Zeta-function

For $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, set $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$.



The Zeta-function

A representation of $\zeta(s)$, for $\mathrm{Re}(s) > 1$, as a product over primes:

$$\begin{aligned}
\prod_p \frac{1}{1-1/p^s} &= \frac{1}{1-1/2^s}\frac{1}{1-1/3^s}\frac{1}{1-1/5^s}\frac{1}{1-1/7^s}\cdots \\
&= \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\cdots\right)\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\cdots \\
&\stackrel{!}{=} 1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\cdots \\
&= \zeta(s).
\end{aligned}$$

This is due to Euler for real $s > 1$ and is called the Euler product.

Euler (1738) first became famous by computing $\zeta(2) = \dfrac{\pi^2}{6}$.

Letting $s \to 1^+$ makes $\zeta(s) \to \infty$, so by Euler product there are infinitely many primes: the first proof in analytic number theory.

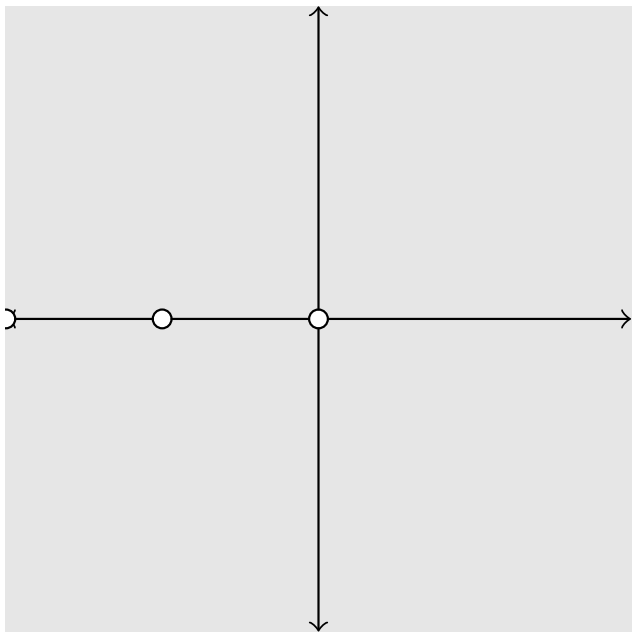
Riemann noted that $\zeta(s)$ for $\mathrm{Re}(s) > 1$ is **analytic** and he analytically continued $\zeta(s)$ to $\mathbf{C} - \{1\}$ using the Gamma function.

The Gamma-function

The Gamma-function is defined on $\mathbf{C}$ by

$$\Gamma(s) = \int_0^\infty x^s e^{-x} \frac{\mathrm{d}x}{x} \text{ for } \mathrm{Re}(s) > 0$$

and $\Gamma(s+1) = s\Gamma(s)$ for other s (integration by parts). It's analytic away from $0, -1, -2, \ldots$ and $\Gamma(n+1) = n!$.



Theorem (Riemann)

The function $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ *is analytic on* $\mathrm{Re}(s) > 1$ *and extends to an analytic function on* $\mathbf{C} - \{1\}$. *The "completed zeta-function"*

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

is analytic on $\mathbf{C} - \{0, 1\}$ *and satisfies the functional equation*

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

Remark. The zeta-function itself satisfies the messier functional equation

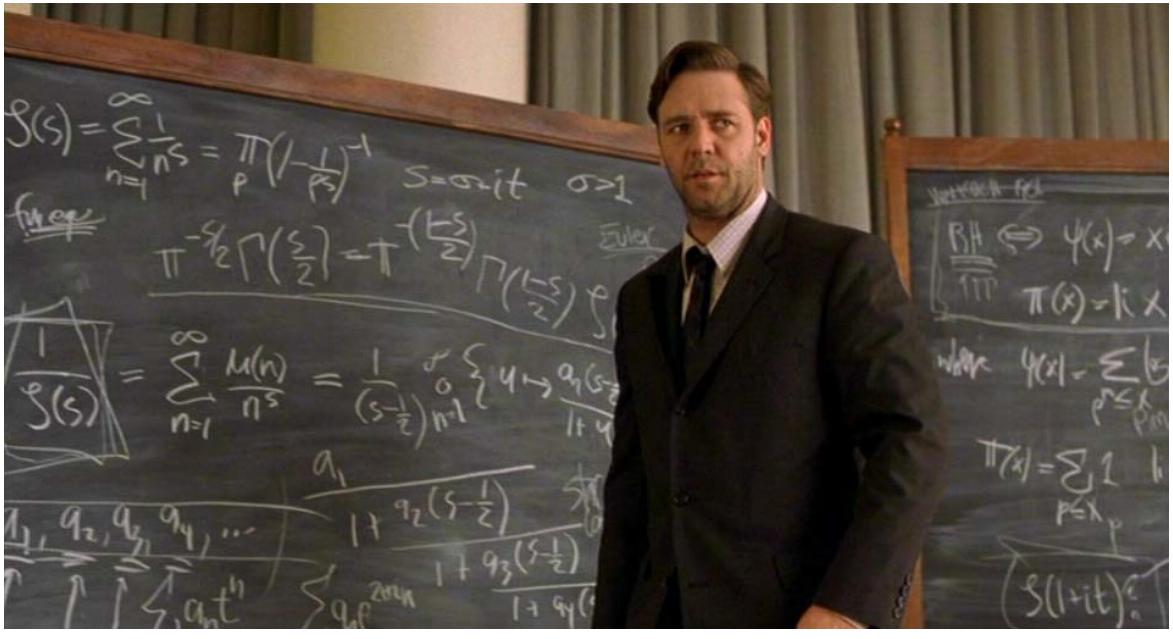
$$\zeta(1 - s) = 2(2\pi)^{-s} \Gamma(s) \cos\left(\frac{\pi s}{2}\right) \zeta(s).$$

Analytic continuation and functional equation

Functional equation:

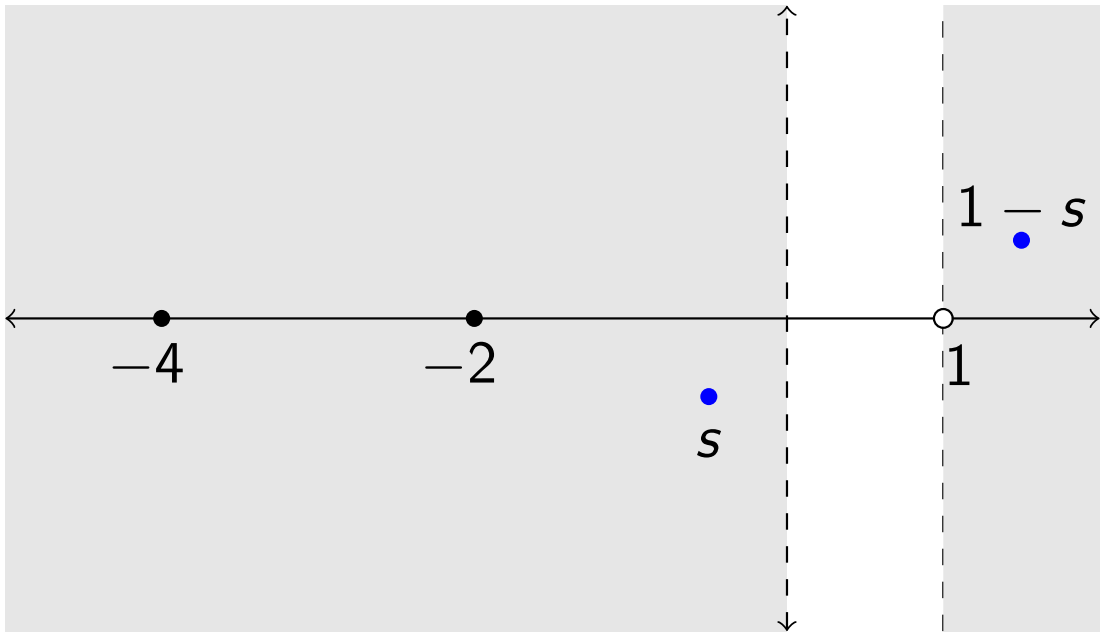
$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Not the functional equation:



Trivial Zeros

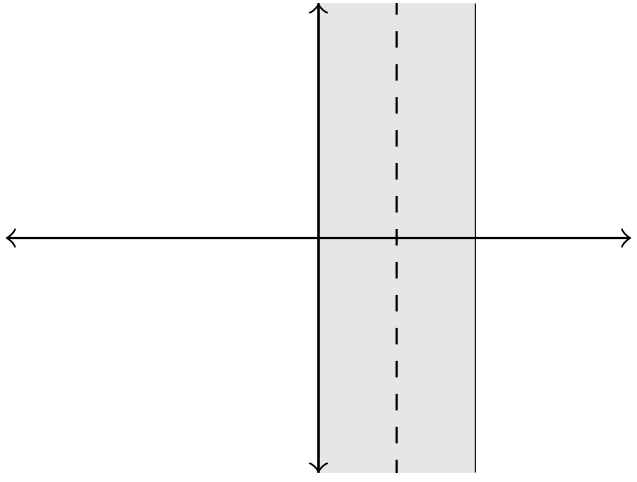
For $\mathrm{Re}(s) > 1, \zeta(s) = \prod_p \frac{1}{1 - 1/p^s} \neq 0$. Also $\pi^{-s/2}\Gamma(s/2) \neq 0$, so $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.



Therefore when $\mathrm{Re}(s) < 0$, $Z(s) = Z(1 - s) \neq 0$. Because $\Gamma(s/2)$ blows up at $s = 0, -2, -4, -6, \ldots$ and $Z(s)$ is finite and nonzero at $s = -2, -4, -6, \ldots$, $\zeta(s) = 0$ when $s = -2$, -4, $-6, \ldots$.
These are called the trivial zeros of $\zeta(s)$.

Nontrivial Zeros

The zeros of $\zeta(s)$ that are not explained by $\Gamma(s/2)$ are called nontrivial. They are in the *critical strip* $0 \leq \mathrm{Re}(s) \leq 1$.



The center line $\mathrm{Re}(s) = \frac{1}{2}$ is called the *critical line*. Since $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ is nonzero outside the critical strip, nontrivial zeros of $\zeta(s)$ = all zeros of $Z(s)$. First three nontrivial zeros with $\mathrm{Im}(s) \geq 0$ are approximately

$$\frac{1}{2} + 14.134725i, \quad \frac{1}{2} + 21.022039i, \quad \frac{1}{2} + 25.010857i.$$

Statement of the Riemann Hypothesis

Wurzeln von $\xi(t) = 0$, multiplicirt mit $2\pi i$. Man findet nun in der That etwa so viel reelle Wurzeln innerhalb dieser Grenzen, und es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien.

Statement of the Riemann Hypothesis

И в самом деле, в указанных пределах содержится, примерно, столько действительных корней; представляется весьма вероятным, что и все корни являются действительными. Во всяком случае было бы желательно найти строгое доказательство этого предложения; после нескольких напрасных, не очень настойчивых попыток разыскать таковое, я временно от них отказался, так как для ближайшей цели моего исследования в этом не представлялось надобности.

Statement of the Riemann Hypothesis

に等しい。この積分は又この領域にある $\xi(t)=0$ 根の個数に $2\pi i$ をかけたものに等しい。実際この領域内にはほぼこの程度の多さの実根がある。全ての根が実数であることはかなり確かなことである。もちろんこれについては確かな証明が望まれる。しかし私は，粗雑ながらも若干試みたがよい成果を得なくて，これについての探求を当分の間しなかった。それは私の研究の一番直接の目的にとって無用におもわれたからだ。

Statement of the Riemann Hypothesis

the number of roots of $\xi(t) = 0$ in the domain multiplied by $2\pi i$. One finds in fact about this many real roots within these bounds and it is very likely that all of the roots are real. One would of course like to have a rigorous proof of this, but I have put aside the search for such a proof after some fleeting vain attempts because it is not necessary for the immediate objective of my investigation.

Here $\xi(t)$ is essentially $Z(1/2 + it)$, which is **real-valued** for real t.

Riemann Hypothesis: Nontrivial zeros of $\zeta(s)$ have $\mathrm{Re}(s) = \frac{1}{2}$.
Equivalently, all zeros of $Z(s)$ have $\mathrm{Re}(s) = \frac{1}{2}$: all zeros of $Z(1/2 + it)$ are real.

What was Riemann's investigation?

Riemann's Investigation

Riemann set out a program for proving the prime number theorem:

$$\pi(x) = \#\{\text{primes} \leq x\} \stackrel{?}{\sim} \frac{x}{\log x} \quad \text{as } x \to \infty.$$

This had first been conjectured publicly by Legendre (1796).

x	$\pi(x)$	$x/\log x$	Ratio
10^2	25	21.7	1.15
10^4	1229	1085.7	1.13
10^6	78498	72382.4	1.08
10^8	5761455	5428681.0	1.06
10^{10}	455052511	434294481.9	1.04

Gauss (before Legendre) developed a probabilistic model which suggested to him that

$$\pi(x) \stackrel{?}{\sim} \mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t} \sim \frac{x}{\log x}.$$

Riemann's Investigation

Riemann set out a program for proving the prime number theorem:

$$\pi(x) = \#\{\text{primes} \leq x\} \stackrel{?}{\sim} \frac{x}{\log x} \quad \text{as } x \to \infty.$$

This had first been conjectured publicly by Legendre (1796).

x	$\pi(x)$	$\mathrm{Li}(x)$	$\pi(x)/\mathrm{Li}(x)$
10^2	25	29.0	.859
10^4	1229	1245.0	.987
10^6	78498	78626.5	.998
10^8	5761455	5762208.3	.9998
10^{10}	455052511	455055613.5	.999993

Gauss (before Legendre) developed a probabilistic model which suggested to him that

$$\pi(x) \stackrel{?}{\sim} \mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t} \sim \frac{x}{\log x}.$$

Riemann's Investigation

Riemann compared two product representations of $\zeta(s)$: its Euler product over the primes and its factorization over its zeros:

$$\zeta(s) = \prod_p \frac{1}{1-1/p^s} = \frac{1}{2}\left(\frac{2\pi}{e}\right)^s \frac{1}{s-1} \prod_{\zeta(\rho)=0} \left(1-\frac{s}{\rho}\right)^{m_\rho} e^{m_\rho s/\rho}.$$

These two products are the basic reason why information about zeros of $\zeta(s)$ can lead to information about prime numbers! Applying an integral transform to both formulas implies for $x > 2$

$$\sum_{p^k \le x} \log p = x - \sum_{\zeta(\rho)=0} m_\rho \frac{x^\rho}{\rho} - \log(2\pi).$$

The prime number theorem can be expressed in terms of growth of the left side. Since $|x^\rho| = x^{\mathrm{Re}(\rho)}$, estimating size of middle term compared to x needs knowledge of $\mathrm{Re}(\rho)$.

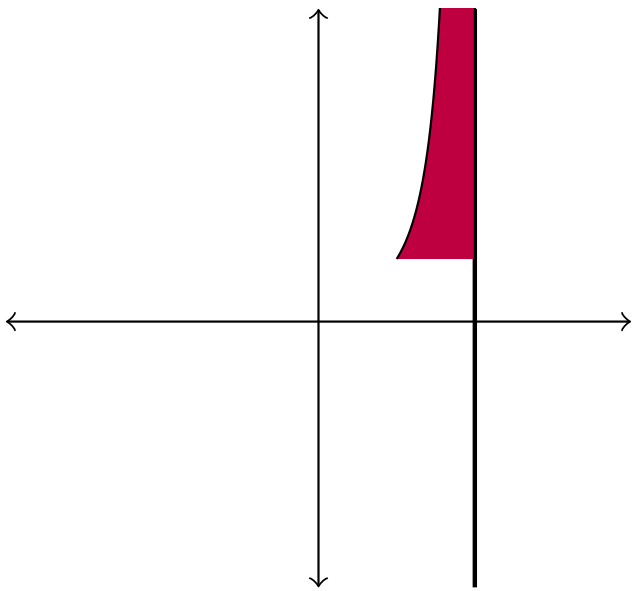
Zero-Free Regions

The proof of the prime number theorem (1896) did not use RH.

Theorem (Wiener, 1932)

The prime number theorem is equiv. to $\zeta(s) \neq 0$ *for* $\mathrm{Re}(s) = 1$.

This is what a known zero-free region in upper part of critical strip looks like (for large imaginary parts).



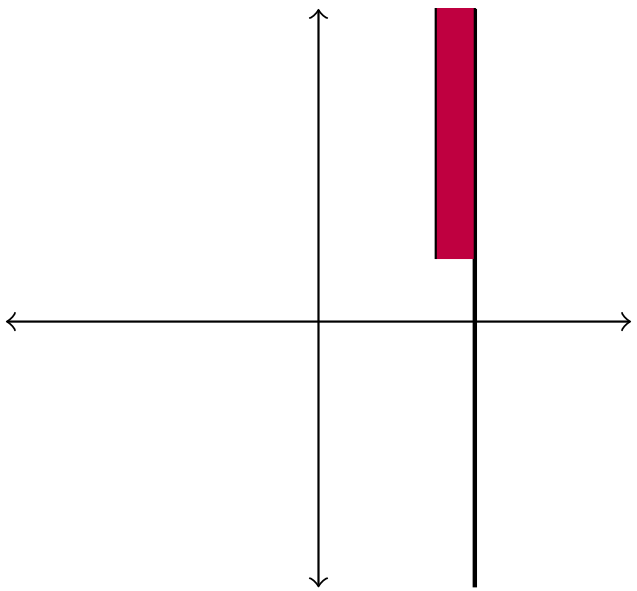
Zero-Free Regions

The proof of the prime number theorem (1896) did not use RH.

Theorem (Wiener, 1932)

The prime number theorem is equiv. to $\zeta(s) \neq 0$ *for* $\mathrm{Re}(s) = 1$.

No zero-free region of the form $\{\mathrm{Re}(s) > 1 - \varepsilon\}$ is known. Find one and become famous! Too bad $\mathrm{Re}(s) = 1$ is not compact.



Using Riemann Hypothesis: $\pi(x)$ vs. $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x)$	$\pi(x) - \mathrm{Li}(x)$
10^2	25	29.0	-4.0
10^4	1229	1245.0	-16.0
10^6	78498	78626.5	-128.5
10^8	5761455	5762208.3	-753.3
10^{10}	455052511	455055613.5	-3102.5

Is $\pi(x) < \mathrm{Li}(x)$ for all $x > 2$? No: Littlewood (1914) showed $\pi(x) > \mathrm{Li}(x)$ infinitely often. What is an example?

Skewes (1933): RH implies $\pi(x) > \mathrm{Li}(x)$ for some $x < 10^{10^{10^{34}}}$.

Skewes (1955): $\pi(x) > \mathrm{Li}(x)$ for some $x < 10^{10^{10^{963}}}$ (RH not used). This upper bound has been reduced to around 10^{316}, must be above 10^{19}. Still no example is known.

Beyond RH: Simplicity of Zeros

Conjecture: The nontrivial zeros of $\zeta(s)$ are simple.

Here is a question of Polya which involves this conjecture.

Set $\text{Even}(x) = \#\{n \leq x : n \text{ has an even number of prime factors}\}$ and $\text{Odd}(x) = \#\{n \leq x : n \text{ has an odd number of prime factors}\}$. For example, $12 = 2^2 \cdot 3$ has three prime factors.

x	1	2	3	4	5	6	7	8	9	10
$\text{Even}(x)$	1	1	1	2	2	3	3	3	4	5
$\text{Odd}(x)$	0	1	2	2	3	3	4	5	5	5

- Polya (1919) conjectured $\text{Even}(x) \leq \text{Odd}(x)$ for all $x \geq 2$.
- Ingham (1942) showed this implies RH and simplicity of nontrivial zeros of $\zeta(s)$ and **Q**-linear dependence of positive imaginary parts of the zeros. Unlikely!
- Least counterexample is $x = 906,150,257$ (Tanaka, 1980).

Why Believe RH?

Here are two pieces of evidence in the direction of RH:

- Numerical evidence looks impressive, *e.g.*, Gourdon–Demichel (2004) checked first 10^{13} zeros of $\zeta(s)$ are on critical line.
- For $\varepsilon > 0$, 0% of nontrivial zeros of $\zeta(s)$ satisfy $\mathrm{Re}(s) \geq \frac{1}{2} + \varepsilon$.

Hilbert's 23 problems and the Clay Millenium Prize problems both include RH, and the official problem descriptions both emphasize that RH is the simplest case of a **generalized Riemann hypothesis** for functions resembling $\zeta(s)$. The generalized Riemann hypothesis is much more important for applications than the Riemann hypothesis!

What are other zeta-like functions and concrete problems that they can be applied to?

Generalizing the zeta-function

There are many functions similar to $\zeta(s)$ which each have, or are *expected* to have, the following properties:

1. a series expansion $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ for $\mathrm{Re}(s) > 1$,
2. an Euler product of some degree $d \geq 1$: for $\mathrm{Re}(s) > 1$,

$$f(s) = \prod_p \frac{1}{1 + c_{p,1}/p^s + \cdots + c_{p,d}/p^{ds}},$$

3. analytic continuation to $\mathbf{C}$ or $\mathbf{C} - \{1\}$ (with suitable growth),
4. a completed function

$$F(s) = A^s \prod_{i=1}^{m} \Gamma(\lambda_i s + \mu_i) f(s)$$

   satisfying $F(1-s) = w\overline{F(\overline{s})}$ where $|w| = 1$,
5. **Generalized Riemann Hypothesis (GRH)**: all nontrivial zeros of $f(s)$ are on the line $\mathrm{Re}(s) = \frac{1}{2}$.

Example: Dirichlet L-functions

A *Dirichlet L-function* is any infinite series of the form $\sum_{n\geq 1} \frac{\chi(n)}{n^s}$, where $\{\chi(n)\}$ is a periodic and totally multiplicative sequence with $\chi(1) = 1$. When $\chi(n) = 1$ for all n the series is $\zeta(s)$.

n	1	2	3	4	5	6	7	8	9	10
$\chi_4(n)$	1	0	-1	0	1	0	-1	0	1	0
$\chi_5(n)$	1	i	$-i$	-1	0	1	i	$-i$	-1	0
$\chi_5^2(n)$	1	-1	-1	1	0	1	-1	-1	1	0

We set

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

For $\mathrm{Re}(s) > 1$, the series and product converge and $L(s,\chi) \neq 0$.

Functional Equation for $L(s, \chi_5)$

n	1	2	3	4	5	6	7	8	9	10
$\chi_5(n)$	1	i	$-i$	-1	0	1	i	$-i$	-1	0

For $\mathrm{Re}(s) > 1$,

$$L(s, \chi_5) = 1 + \frac{i}{2^s} - \frac{i}{3^s} - \frac{1}{4^s} + \frac{1}{6^s} + \frac{i}{7^s} + \cdots.$$

The function $\Lambda(s, \chi_5) = 5^{s/2}\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s, \chi_5)$ is analytic on $\mathbf{C}$ (no problem at $s = 0, 1$) and satisfies the functional equation

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

where $w = \sqrt[4]{-(3+4i)/5} \approx .85 - .52i$; $|w| = 1$.

The function $L(s, \chi_5)$ is nonzero for $\mathrm{Re}(s) > 1$ by its Euler product. From the functional equation for $\Lambda(s, \chi_5)$, $L(s, \chi_5) = 0$ at $s = -1, -3, -5, \ldots$, which are called the trivial zeros of $L(s, \chi_5)$.

Generalized Riemann Hypothesis for Dirichlet L-functions

Any $L(s,\chi)$ has a completed form $\Lambda(s,\chi)$ satisfying a functional equation $\Lambda(1-s,\chi) = w\overline{\Lambda(\overline{s},\chi)}$, where $|w| = 1$.

Generalized Riemann Hypothesis for $L(s,\chi)$: all nontrivial zeros of $L(s,\chi)$ (equiv., all zeros of $\Lambda(s,\chi)$) are on the line $\mathrm{Re}(s) = \frac{1}{2}$.

1	χ_4	χ_5	χ_5^2
$\frac{1}{2} + 14.1347i$	$\frac{1}{2} + 6.0209i$	$\frac{1}{2} + 6.1835i$	$\frac{1}{2} + 6.6484i$
$\frac{1}{2} + 21.0220i$	$\frac{1}{2} + 10.2437i$	$\frac{1}{2} + 8.4572i$	$\frac{1}{2} + 9.8314i$
$\frac{1}{2} + 25.0108i$	$\frac{1}{2} + 12.5880i$	$\frac{1}{2} + 12.6749i$	$\frac{1}{2} + 11.9588i$

Using GRH: Goldbach's conjecture (1742)

Even Goldbach conjecture: all even $n \geq 4$ are a sum of 2 primes.
Odd Goldbach conjecture: all odd $n \geq 7$ are a sum of 3 primes.

Even conj. implies odd conj. (n odd implies $n-3$ is even).

Theorem (Hardy–Littlewood, 1923)

Odd Goldbach conjecture true for $n \gg 0$ if all Dirichlet L-functions are nonzero on a common right half-plane $\mathrm{Re}(s) \geq \frac{3}{4} - \varepsilon$.

Theorem (Vinogradov, 1937)

Odd Goldbach conjecture true for $n \gg 0$ unconditionally.

Theorem (Deshouillers–Effinger–te Riele–Zinoviev, 1997)

Odd Goldbach conjecture true for $n \geq 7$ under GRH for all Dirichlet L-functions.

In the last theorem, GRH used for $n > 10^{20}$, computers for rest.
Helfgott (2013) settled odd Goldbach without GRH.

Using GRH: Polynomial-time Primality Test

Theorem (Miller, 1976)

There is a polynomial-time primality test if GRH is true for all Dirichlet L-functions.

It would suffice to have **common** zero-free region $\mathrm{Re}(s) > 1 - \varepsilon$ for all Dirichlet L-functions. The run-time for Miller's test can be made explicit in terms of ε.

Theorem (Agrawal–Kayal–Saxena, 2002)

There is a polynomial-time primality test, unconditionally.

The AKS test is not Miller's test. Still not known that Miller's test runs in polynomial time without assuming GRH.

Interlude: Scope of GRH

The functions which should satisfy GRH include

- Riemann zeta-function $\zeta(s)$,
- Dirichlet L-function $L(s, \chi)$,
- Zeta-function of a number field (like $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt[3]{2})$),
- L-function of a modular form,
- L-function of elliptic curve over $\mathbf{Q}$,
- L-function of representation of a Galois group $\mathrm{Gal}(K/\mathbf{Q})$.

It is not just GRH that is an open problem here: analytic continuation to $\mathbf{C}$ and a functional equation can be a hard theorem or still be unknown!

For example, the analytic continuation and functional equation of L-functions of elliptic curves over $\mathbf{Q}$, in general, were proved by the ideas going into Wiles's proof of Fermat's Last Theorem.

The L-function of a modular form

If $f = \sum_{n \geq 0} a_n q^n$ is a modular form of weight k, its L-function is

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

This does not involve the constant term of f. Since $a_n = O(n^{k-1})$, $L(s, f)$ converges absolutely for $\mathrm{Re}(s) > k$.

Theorem

The completed L-function $\Lambda(s, f) = (2\pi)^{-s}\Gamma(s)L(s, f)$ has a meromorphic continuation to $\mathbf{C}$ except for simple poles at $s = 0$ and $s = k$ with residues $\pm a_0$, and $\Lambda(k - s, f) = (-1)^{k/2}\Lambda(s, f)$.

We expect $\Lambda(s, f)$ to satisfy the Riemann hypothesis (all its zeros are on $\mathrm{Re}(s) = k/2$) if f is *normalized cuspidal eigenform* for the Hecke operators, which is when $L(s, f)$ has Euler product.

Example. Eigenform $\Delta(\tau)$ has weight 12 and first three zeros of $\Lambda(s, \Delta(\tau))$ are $6 + it$ for $t \approx 9.223$, 13.907, 17.442.

Using GRH: Artin's Primitive Root Conjecture

Theorem. (Gauss) For each prime p, the group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic.

Example. The group $(\mathbf{Z}/7\mathbf{Z})^\times = \{1, 2, 3, 4, 5, 6\}$ has generator 3:

$$3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1.$$

Question. If $a \in \mathbf{Z}$ is not 0 or ± 1, is a mod p a generator of $(\mathbf{Z}/p\mathbf{Z})^\times$ for infinitely many primes p?

Example. Gauss conjectured for $a = 10$ the answer is "Yes". Elementary school meaning: $\dfrac{1}{p}$ has decimal period $p - 1$ infinitely often (try $p = 7$).

Nonexample. If $a = 9$ then $a^{(p-1)/2} = 3^{p-1} \equiv 1 \bmod p$ when $p \neq 3$, so answer is "No" when $a = 9$.

Conjecture. (Artin, 1927) If $a \in \mathbf{Z}$ is not 0, -1, or a perfect square then a mod p generates $(\mathbf{Z}/p\mathbf{Z})^\times$ for infinitely many p.

Using GRH: Artin's Primitive Root Conjecture

Theorem (Hooley, 1967)

For each $a \neq 0, -1$, or a perfect square, Artin's conjecture for a is correct if GRH is true for a **specific family** *of zeta-functions of number fields depending on a.*

The GRH-dependence was later relaxed by Gupta, Murty, Murty, Heath-Brown.

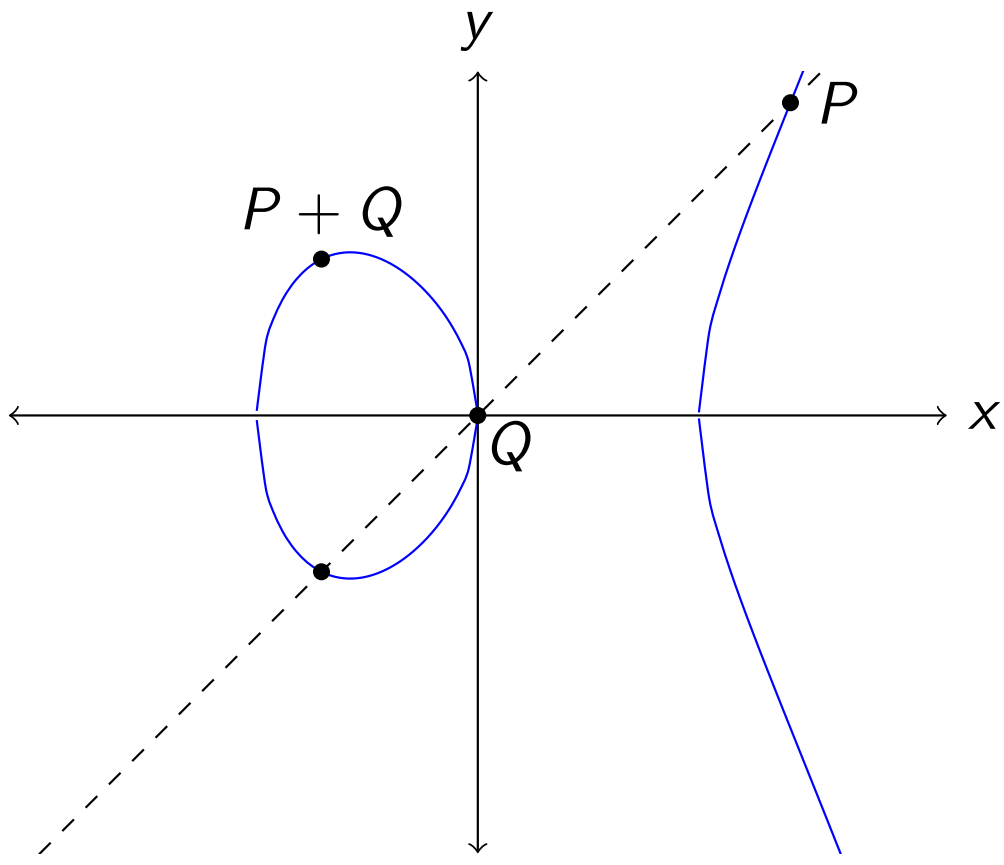
Example. Unconditionally, at least one of $a = 2$, 3, or 5 is a generator for $(\mathbf{Z}/p\mathbf{Z})^\times$ for infinitely many p. (Surely for all three!)

Although Artin's conjecture (as stated here) has been proved true for most a unconditionally it is not known for any one specific a.

Using GRH: Elliptic Artin Conjecture

An elliptic curve over $\mathbf{Q}$ is a smooth curve with equation $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Q}$. Rational solutions $E(\mathbf{Q})$ are an abelian group.

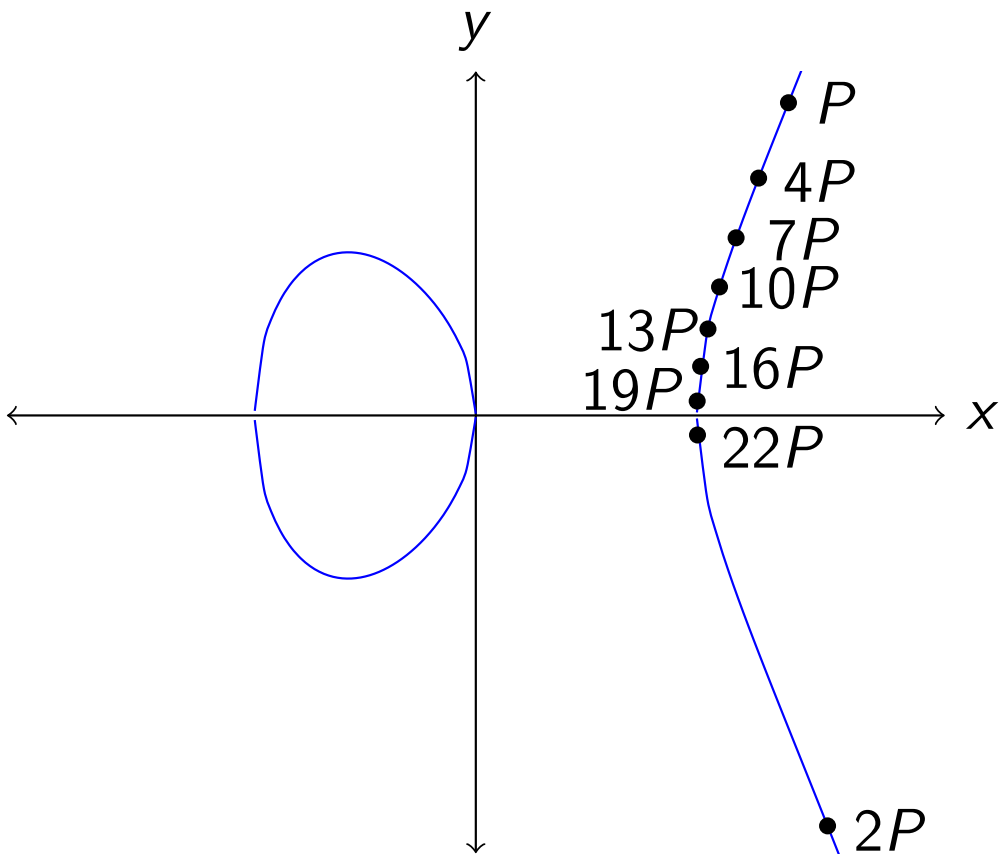
Example. On $y^2 = x^3 - 2x$, set $P = (2, 2)$ and $Q = (0, 0)$.



Using GRH: Elliptic Artin Conjecture

An elliptic curve over $\mathbf{Q}$ is a smooth curve with equation $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Q}$. Rational solutions $E(\mathbf{Q})$ are an abelian group.

Example. On $y^2 = x^3 - 2x$, set $P = (2, 2)$ and $Q = (0, 0)$.



Using GRH: Elliptic Artin Conjecture

For most primes p, the reduced equation

$$E : y^2 \equiv x^3 + ax + b \bmod p$$

is an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$ and its solutions $E(\mathbf{Z}/p\mathbf{Z})$ form a finite abelian group.
The collection of groups $E(\mathbf{Z}/p\mathbf{Z})$ is analogous to the collection of groups $(\mathbf{Z}/p\mathbf{Z})^\times$.

Question (Lang–Trotter): If a point $P \in E(\mathbf{Q})$ has infinite order, does it generate $E(\mathbf{Z}/p\mathbf{Z})$ for infinitely many p?

Example: Let $E : y^2 = x^3 - 2x$ and $P = (2, 2)$. Working modulo 3, $E(\mathbf{Z}/3\mathbf{Z}) = \{(0, 0), (2, 1), (2, 2) \bmod 3\}$. This is $2\overline{P}$, $3\overline{P}$, $\overline{P}$.
The group $E(\mathbf{Z}/p\mathbf{Z})$ is generated by $\overline{P}$ for $p = 3, 5, 11, 19, \ldots$, although it's not known that the list continues indefinitely.

Using GRH: Elliptic Artin Conjecture

Are we even certain that the groups $E(\mathbf{Z}/p\mathbf{Z})$ are cyclic for infinitely many p? (Compare to: $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic for all p.)

Obstruction: If $x^3 + ax + b$ has **all** rational roots then for $p \gg 0$ the group of solutions to $y^2 \equiv x^3 + ax + b \bmod p$ includes more than one point of order 2, so it is *not* cyclic.

Example. For the elliptic curve $E : y^2 = x^3 - x$, $E(\mathbf{Z}/p\mathbf{Z})$ is not cyclic for any $p > 2$.

Theorem (Serre)

If $E(\mathbf{Q})$ is infinite, $x^3 + ax + b$ has irrational root, and GRH is true for zeta-functions of a **specific family** *of number fields depending on E, then $E(\mathbf{Z}/p\mathbf{Z})$ is cyclic for infinitely many p.*

Gupta and Murty later proved this unconditionally (no use of GRH).

Using GRH: Elliptic Artin Conjecture

Conjecture (Lang–Trotter). *If $P \in E(\mathbf{Q})$ has infinite order and $x^3 + ax + b$ has an irrational root then $\overline{P}$ generates $E(\mathbf{Z}/p\mathbf{Z})$ for infinitely many p.*

Theorem (Serre)

The Lang–Trotter conjecture for E and P is true if GRH is true for the zeta-functions of a **specific family** *of number fields depending on E and P.*

Without using GRH, Gupta and Murty showed for certain E that **some** point in $E(\mathbf{Q})$ is a generator of $E(\mathbf{Z}/p\mathbf{Z})$ for infinitely many p. The ideas here led to their work on the original Artin conjecture (*e.g.*, 2, 3, or 5 generates $(\mathbf{Z}/p\mathbf{Z})^\times$ infinitely often).

Why Believe GRH (Besides Numerical Data)?

- It has a *proved* analogue in characteristic p.
  Example. Zeta-function of curve $y^2 = x^3 - 2x$ over $\mathbf{Z}/5\mathbf{Z}$ is

$$\frac{1 - 4 \cdot 5^{-s} + 5 \cdot 5^{-2s}}{(1 - 5^{-s})(1 - 5 \cdot 5^{-s})} = \frac{(1 - (2+i)5^{-s})(1 - (2-i)5^{-s})}{(1 - 5^{-s})(1 - 5 \cdot 5^{-s})},$$

  so s is zero $\Rightarrow 5^s = 2 \pm i \Rightarrow 5^{\mathrm{Re}(s)} = \sqrt{5} \Rightarrow \mathrm{Re}(s) = \frac{1}{2}$.
- The proof of GRH in characteristic p uses an interpretation of the zeros as eigenvalues of a special operator (and substantial ideas from algebraic geometry).
- Hilbert and Polya asked if there is a self-adjoint operator on a Hilbert space whose eigenvalues are the zeros of $Z(1/2 + it)$. Eigenvalues of a self-adjoint operator are real.
- Meyer (2006), following work of Connes (1999), introduced spaces (though not Hilbert spaces) and operators whose eigenvalues correspond naturally to the zeros of functions for which GRH is expected.

A Bad Approach to GRH

Warning: GRH can't be a formal consequence of an analytic continuation and functional equation "of zeta-type".

Let $Q(x,y) = x^2 + 5y^2$, so $Q(x,y) > 0$ for $(x,y) \neq (0,0)$. The zeta-function of Q is defined to be

$$\zeta_Q(s) = \sum_{(x,y)\in \mathbf{Z}^2}{}' \frac{1}{Q(x,y)^s} = \sum_{(x,y)\in \mathbf{Z}^2}{}' \frac{1}{(x^2+5y^2)^s},$$

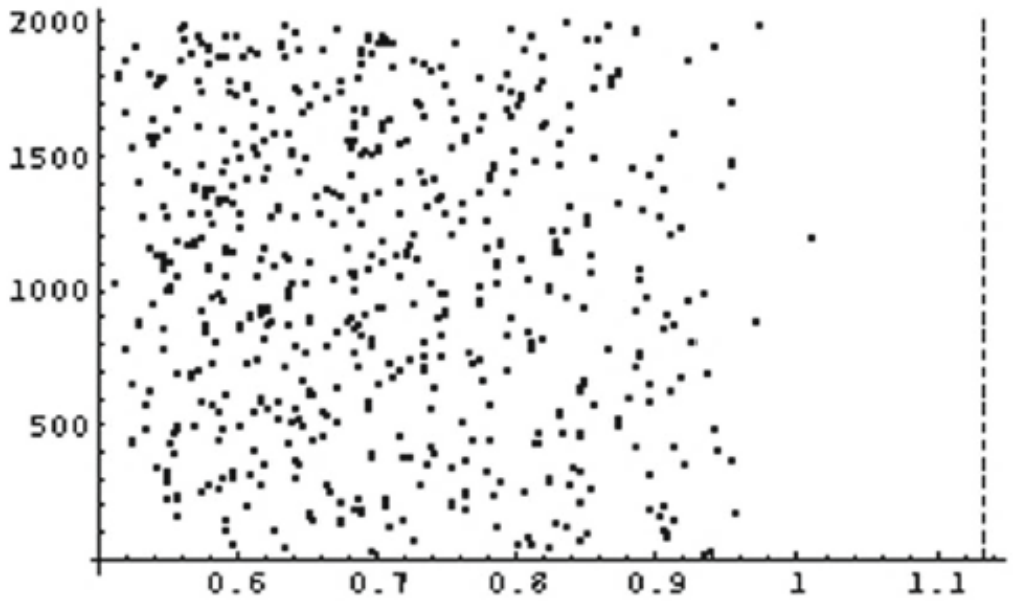
for $\mathrm{Re}(s) > 1$. It is analytic there.

The product $Z_Q(s) = 20^{s/2}(2\pi)^{-s}\Gamma(s)\zeta_Q(s)$ extends analytically to $\mathbf{C} - \{0,1\}$ and satisfies the functional equation

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

Zeros of $\zeta_Q(s)$

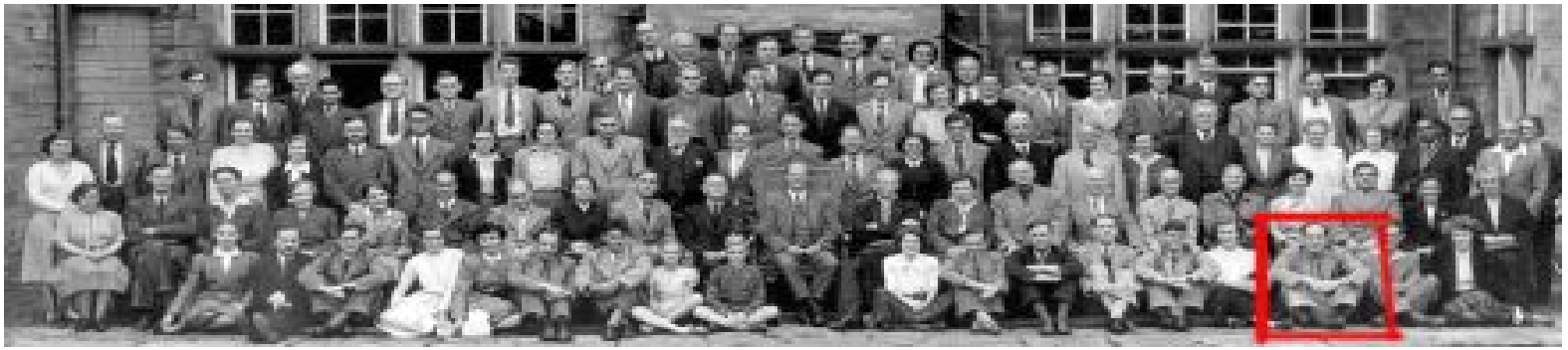
H. S. A. Potter and E. C. Titchmarsh (1935): the function $\zeta_Q(s)$ has zeros on $\mathrm{Re}(s) = 1/2$ and also zeros with $\mathrm{Re}(s) > \frac{1}{2}$ or even $\mathrm{Re}(s) > 1$. (No Euler product!)



Zeros of $\zeta_Q(s)$

H. S. A. Potter and E. C. Titchmarsh (1935): the function $\zeta_Q(s)$ has zeros on $\mathrm{Re}(s) = 1/2$ and also zeros with $\mathrm{Re}(s) > \frac{1}{2}$ or even $\mathrm{Re}(s) > 1$. (No Euler product!)

British mathematician named H. S. A. Potter...

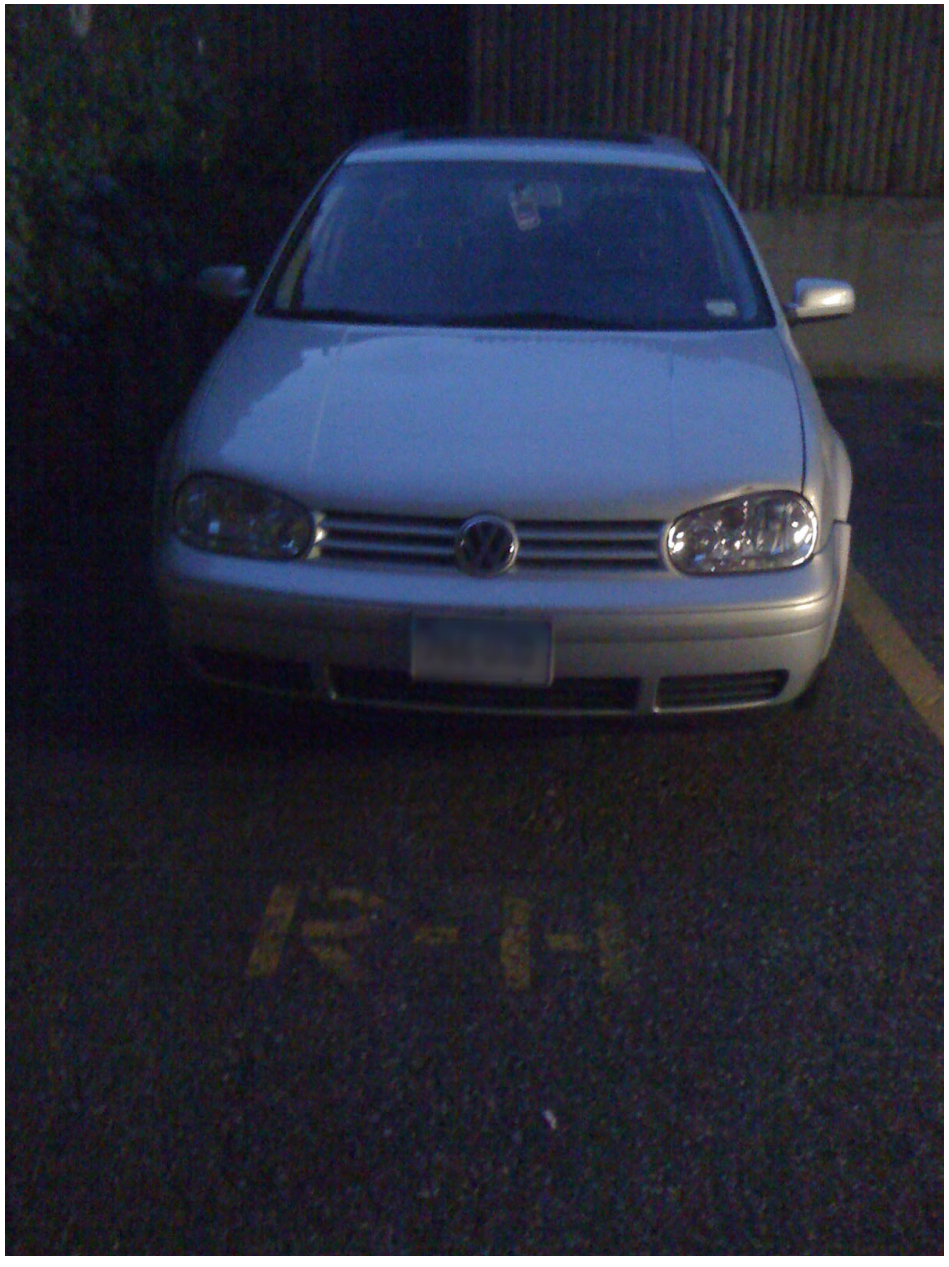


Harold Stanley Arthur Potter (1908?–2004).

- Ph.D. at Oxford under Titchmarsh on $\zeta_Q(s)$, 1933?
- Member IAS, 1933–1935.
- Univ. Aberdeen, 1936–retirement.
- President of Edinburgh Mathematical Society, 1953.

Summary

- The prime numbers are related to the zeros of $\zeta(s)$ because $\zeta(s)$ can be written as a product in two ways: over the primes and over its zeros.
- RH has its own applications, but it is important more because it is the simplest case of GRH.
- Most applications of GRH require it for *infinite* families.
- A zero-free region of the form $\mathrm{Re}(s) > 1 - \varepsilon$ would be a huge advance and have applications.
- GRH has been an excellent guide to what is probably true: theorems proved with it may later be proved unconditionally by other methods.



Questions?

Verifying the Riemann Hypothesis

Since $\zeta(s)$, $\pi^{-s/2}$, and $\Gamma(s/2)$ are real-valued for real $s > 1$, they all satisfy $f(s) = \overline{f(\overline{s})}$, so $Z(s) = \overline{Z(\overline{s})}$. If $s = 1/2 + it$ for real t,

$$\begin{aligned} Z\left(\frac{1}{2} + it\right) &= \overline{Z\left(\overline{\frac{1}{2} + it}\right)} \\ &= \overline{Z\left(\frac{1}{2} - it\right)} \\ &= \overline{Z\left(1 - \left(\frac{1}{2} - it\right)\right)} \\ &= \overline{Z\left(\frac{1}{2} + it\right)}. \end{aligned}$$

Therefore $Z(s)$ is real-valued on the critical line. Nontrivial zeros of $\zeta(s)$ on the critical line can be detected by finding sign changes in $Z(1/2 + it)$. May assume $t \geq 0$ since $Z(1/2 - it) = Z(1/2 + it)$.

Verifying the Riemann Hypothesis Numerically

To count nontrivial zeros in critical strip up to height T

1. integrate $(s(1-s)Z(s))'/(s(1-s)Z(s))$ around region to count zeros of $Z(s)$ inside,
2. compute $Z(1/2+it)$ for $0 < t < T$ and count sign changes,
3. when the two numbers match, we have proved the Riemann hypothesis up to height T.

The contour integral counts multiple zeros multiply often, so this method only works if all nontrivial zeros are simple.

Verifying the Generalized Riemann Hypothesis Numerically

For a completed Dirichlet L-function $\Lambda(s, \chi)$, whose zeros are the nontrivial zeros of $L(s, \chi)$, the functional equation is

$$\Lambda(1 - s, \chi) = w\overline{\Lambda(\overline{s}, \chi)},$$

with $|w| = 1$.

Writing $w = u^2$, the functional equation implies $\frac{1}{u}\Lambda(s, \chi)$ is real-valued on the critical line, so its simple zeros on that line can be found by locating sign changes. Therefore a process like that for $Z(s)$ can be used.