The L-functions and Modular Forms Database (LMFDB)

Edgar Costa (MIT)
Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation

December 3, 2021

Slides available at https://researchseminars.org

Motivation for a database and desired features

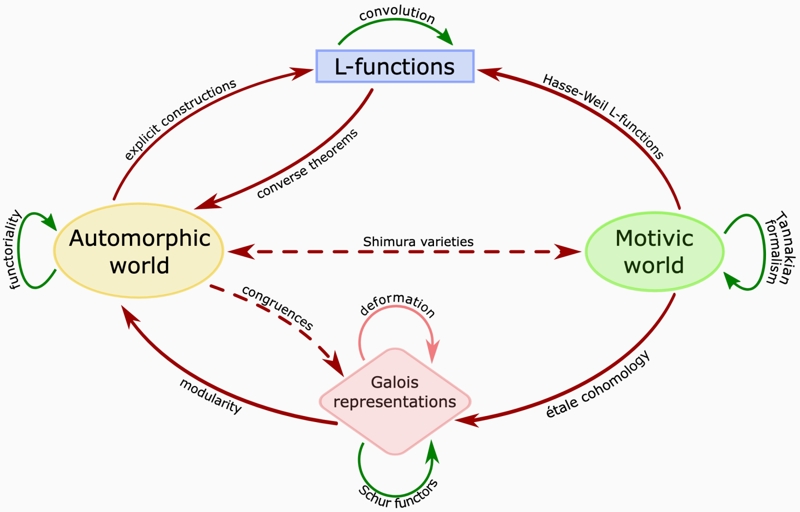
- Number theory has long been, in part, an experimental science.
- Data is often the source of conjectures that lead to theorems.
- Exhaustive enumeration allows one to prove theorems and exposes holes (both in theory and in implementations) by finding all the special cases.
- The database should be easily accessible and comprehensible to as broad an audience as possible, serving both novices and experts.
- All data should have a clear and citable provenance: how it was computed, by whom, to what precision, and under what assumptions, if any.
- Search and aggregation tools are needed to maximize the utility of the data.

The Langlands program

Goal: understand and classify all L-functions

The Langlands program

Goal: understand and classify all L-functions



Riemann zeta function: the prototypical L-function

$$\zeta(s = x + iy) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
$$= \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \cdots = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}$$

Riemann zeta function: the prototypical L-function

$$\zeta(s = x + iy) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
$$= \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \cdots = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}$$

Originally introduced by Euler for $s \in \mathbb{R}$
Used by Chebyshev to study distribution of primes.
Riemann was the first to consider it as a complex function.

The formula above work for $x > 1$, e.g., $\zeta(2) = \sum_{n \geq 1} \frac{1}{n^2} = \pi^2/6$.
Riemann showed it has meromorphic continuation to $\mathbb{C}$.
Furthermore, $\zeta(s)$ has only one simple pole at $s = 1$ with residue 1.

Riemann zeta function: the prototypical L-function

$$\zeta(s = x + iy) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
$$= \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \cdots = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}$$

Originally introduced by Euler for $s \in \mathbb{R}$
Used by Chebyshev to study distribution of primes.
Riemann was the first to consider it as a complex function.

The formula above work for $x > 1$, e.g., $\zeta(2) = \sum_{n \geq 1} \frac{1}{n^2} = \pi^2/6$.
Riemann showed it has meromorphic continuation to $\mathbb{C}$.
Furthermore, $\zeta(s)$ has only one simple pole at $s = 1$ with residue 1.

Riemann also shown the existence of a functional equation.

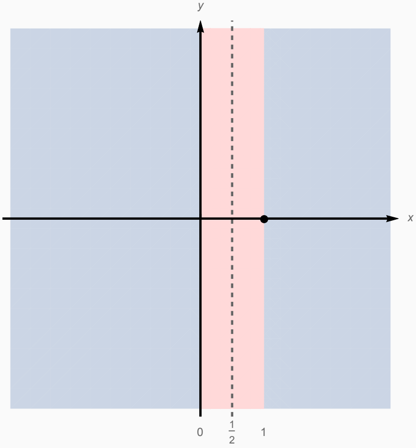
Riemann zeta function

$$\zeta(s = x + iy) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}, \qquad \mathrm{Re}(s) > 1$$

Functional equation relates $s \leftrightarrow 1 - s$

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1 - s) \zeta(1 - s)$$

Easy to compute $\zeta(s)$ for $\mathrm{Re}(s) < 0$.



Riemann zeta function

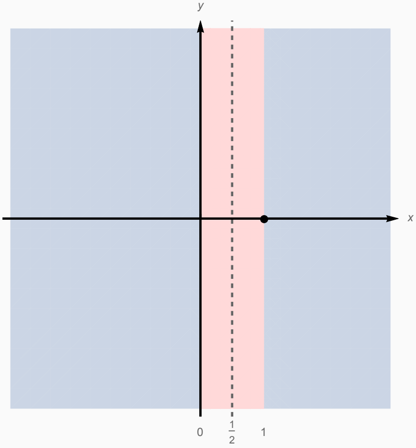
$$\zeta(s = x + iy) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}, \qquad \mathrm{Re}(s) > 1$$

Functional equation relates $s \leftrightarrow 1 - s$

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s)$$

Easy to compute $\zeta(s)$ for $\mathrm{Re}(s) < 0$.
For example:
$\zeta(-n) = (-1)^n B_{n+1}/(n+1)$

$$\Rightarrow \begin{cases} \zeta(-1) = -1/12 & = \text{“}1 + 2 + 3 \cdots\text{”} \\ \zeta(-2n) = 0 & \text{know as the trivial zeros} \end{cases}$$



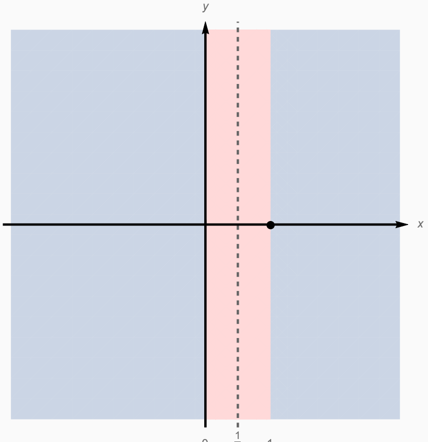
Zeros of the Riemann zeta function

$$\zeta(s = x + iy) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}, \qquad \mathrm{Re}(s) > 1$$

Riemann showed

$$\zeta(s) = 0 \Leftrightarrow \begin{cases} s = -2n \; n \in \mathbb{N} \\ 0 < \mathrm{Re}(s) < 1 \end{cases}$$

conjectured that all nontrivial zeros lie in the critical line $\mathrm{Re}(s) = 1/2$.
One of the Millennium Prize Problems.
https://www.lmfdb.org/zeros/zeta/



Zeros of the Riemann zeta function

$$\zeta(s = x + iy) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}, \qquad \mathrm{Re}(s) > 1$$

Riemann showed

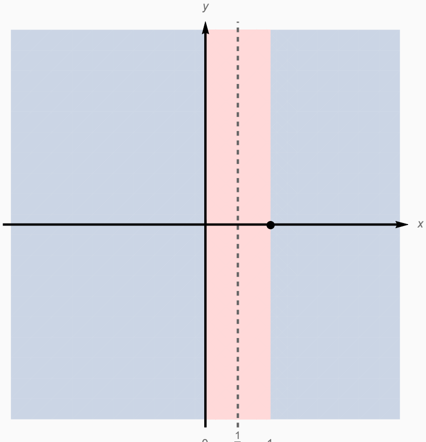
$$\zeta(s) = 0 \Leftrightarrow \begin{cases} s = -2n \; n \in \mathbb{N} \\ 0 < \mathrm{Re}(s) < 1 \end{cases}$$

conjectured that all nontrivial zeros lie in the critical line $\mathrm{Re}(s) = 1/2$.

One of the Millennium Prize Problems.

https://www.lmfdb.org/zeros/zeta/

Riemann also gave a formula how the roots $\zeta(s)$ describe the primes distribution.



How primes are distributed

$$\pi(x) := \#\{p \leq x : p \text{ is prime}\}$$

- Gauss (1791) conjectured $\pi(x) \sim \frac{x}{\log x} \qquad x \to \infty$
- Chebyshev (1848, 1850) $\exists\, A, B > 0$ such that $\frac{Ax}{\log(x)} < \pi(x) < \frac{BX}{\log x}$ for $x \geq 3$. Furthermore, if $\pi(x) \sim \frac{Cx}{\log x}$, then $C = 1$.
- Riemann (1859), using the zeros of $\zeta(s)$, sketched an explicit formula for a normalized prime-counting function $\pi_0(x) = \frac{1}{2} \lim_{h\to 0} \pi(x+h) + \pi(x-h)$.
- Hadamard and de la Vallée Poussin (1896) independently showed

$$\pi(x) \sim \frac{x}{\log x} \qquad x \to \infty$$

$\zeta(s)$ zeros and $\pi(x)$

Hadamard and de la Vallée Poussin (1896) actually established

$$\pi(x) = \mathrm{li}(x) + O\left(xe^{-C\sqrt{\log x}}\right)$$

where $\mathrm{li}(x) := \int_2^x \frac{1}{\log t}\,\mathrm{d}t \sim \frac{x}{\log x}$.

Riemann gives an explicit formula

$$R_0(x) := 1 + \sum_{n\geq 1} \frac{1}{n\zeta(1+n)} \frac{\log(x)^n}{n!}$$

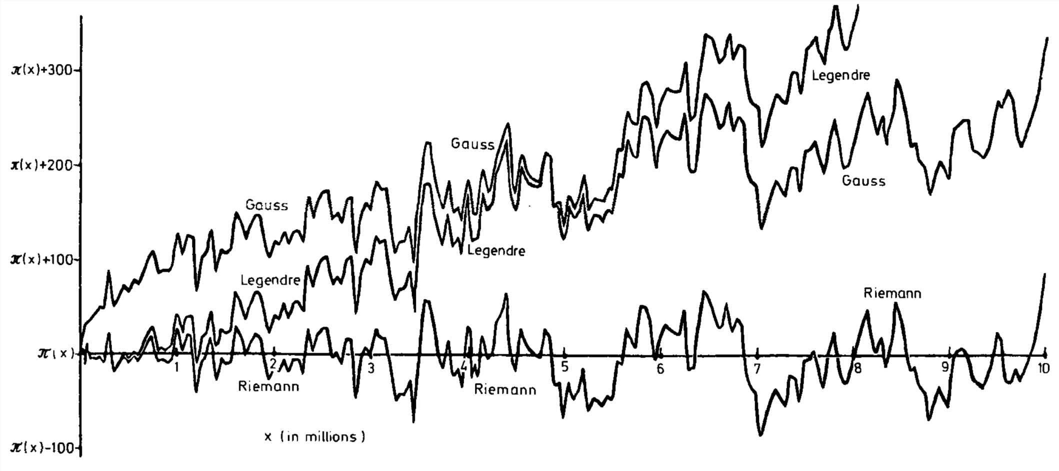
and describes the error term $\pi(x) - R_0(x)$ in terms of

$$\sum_\rho \mathrm{li}(x^\rho),$$

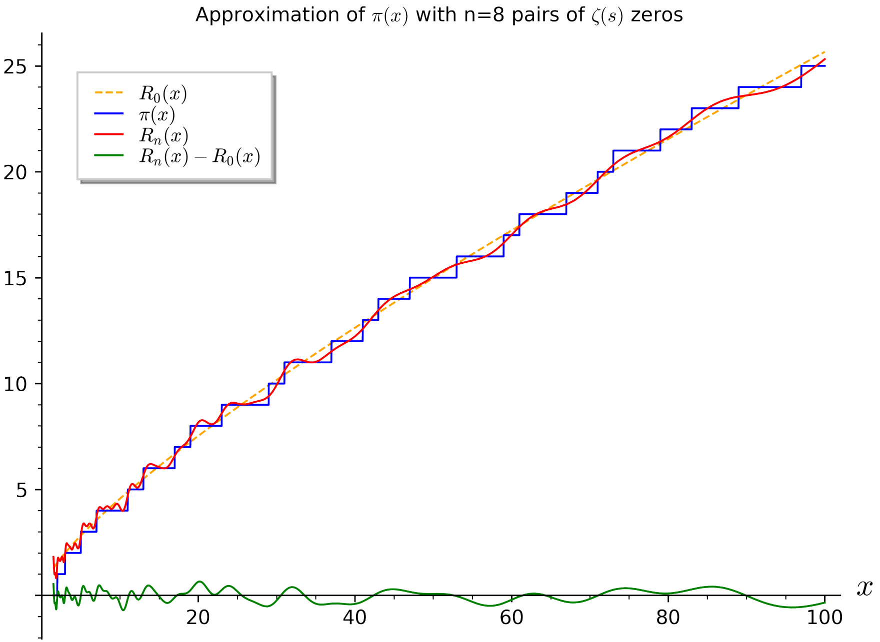
where one sums of the roots ρ in the critical strip. Thus it is not surprising that

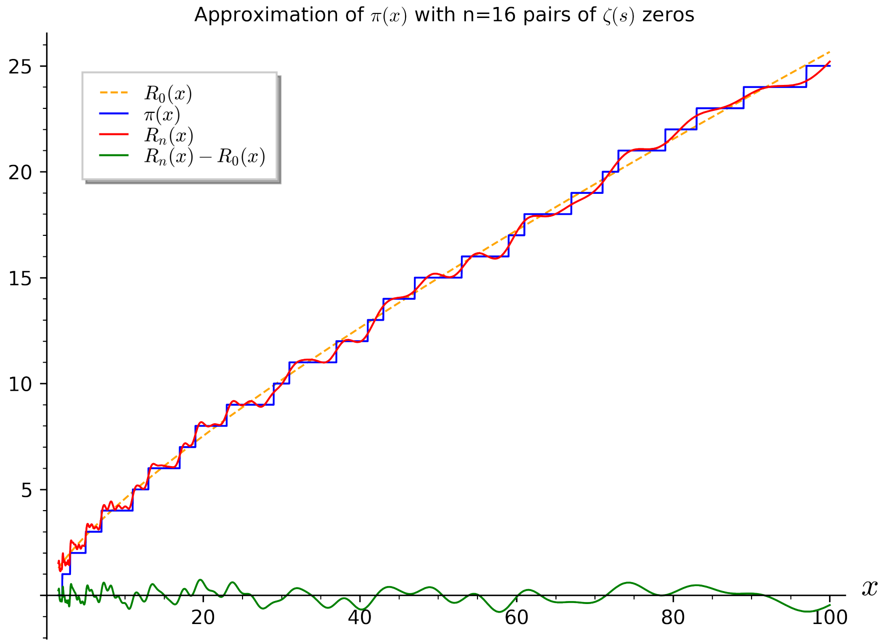
$$\mathrm{Re}(\rho) = \frac{1}{2} \Leftrightarrow \pi(x) = \mathrm{li}(x) + O\left(x^{1/2+\epsilon}\right)$$

Comparison by Zagier (1977)

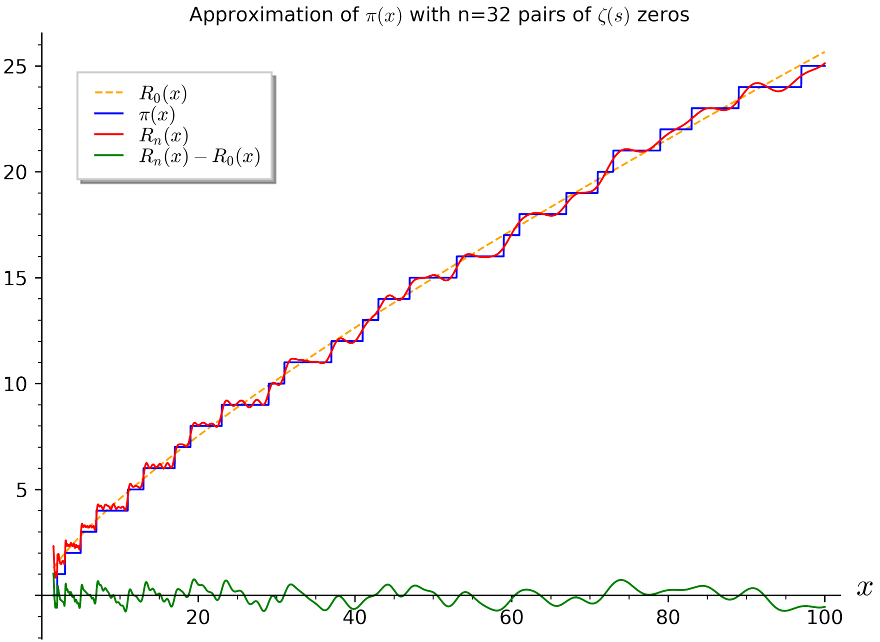


$x/(\log x - 1.08366)$ vs $\mathrm{li}(x)$ vs $R_0(x)$

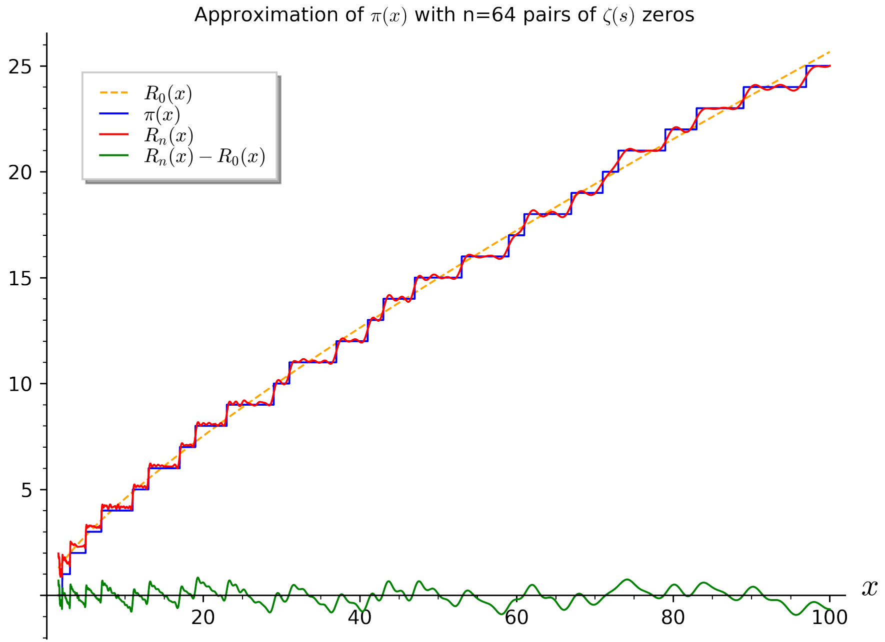

Approximation of $\pi(x)$ with n=8 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x



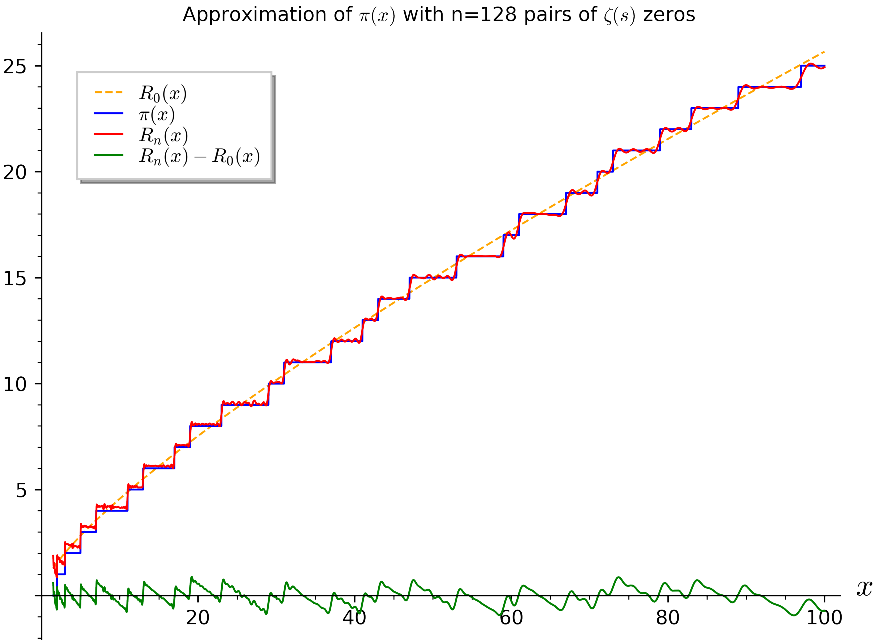
Approximation of $\pi(x)$ with n=16 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x



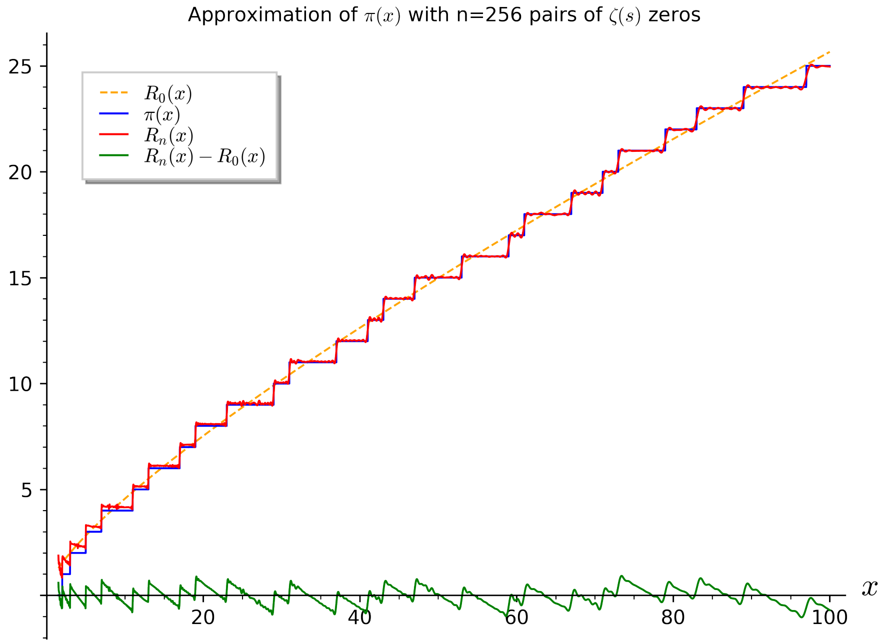
Approximation of $\pi(x)$ with n=32 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x

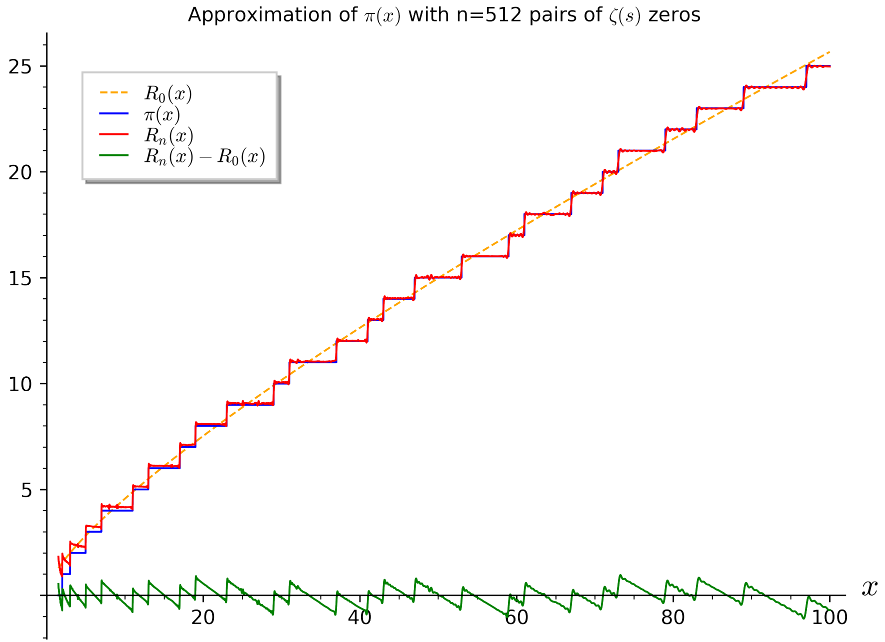


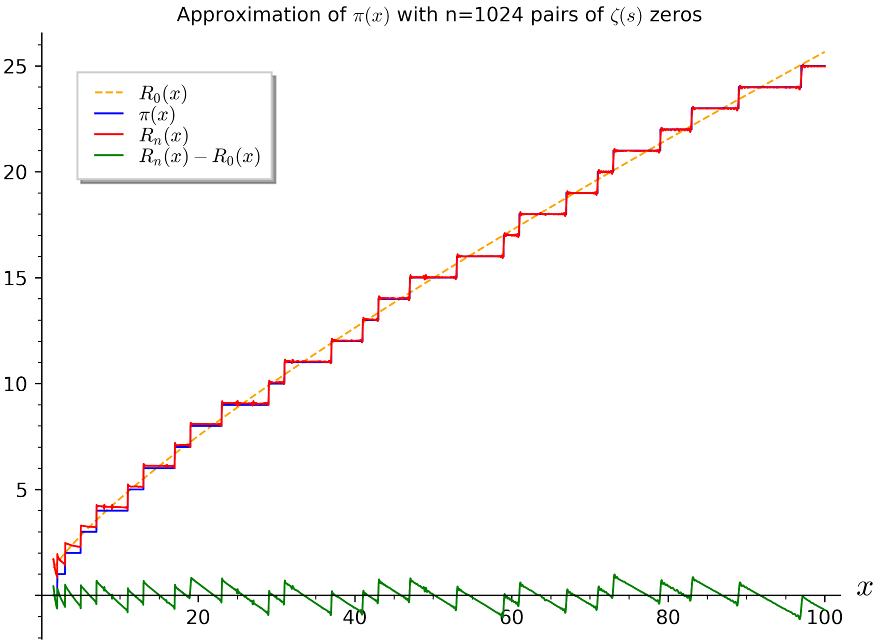
Approximation of $\pi(x)$ with n=64 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x



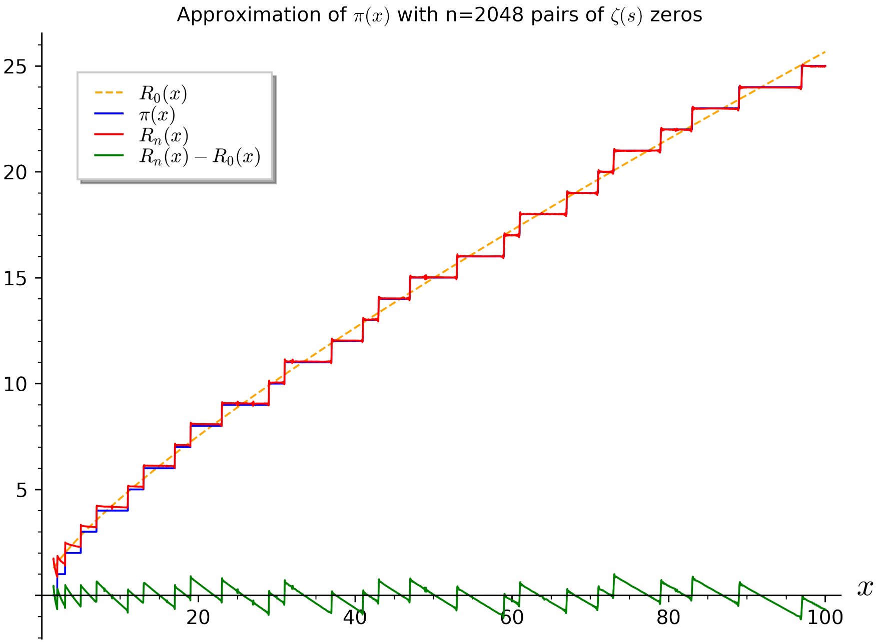
Approximation of $\pi(x)$ with n=128 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x

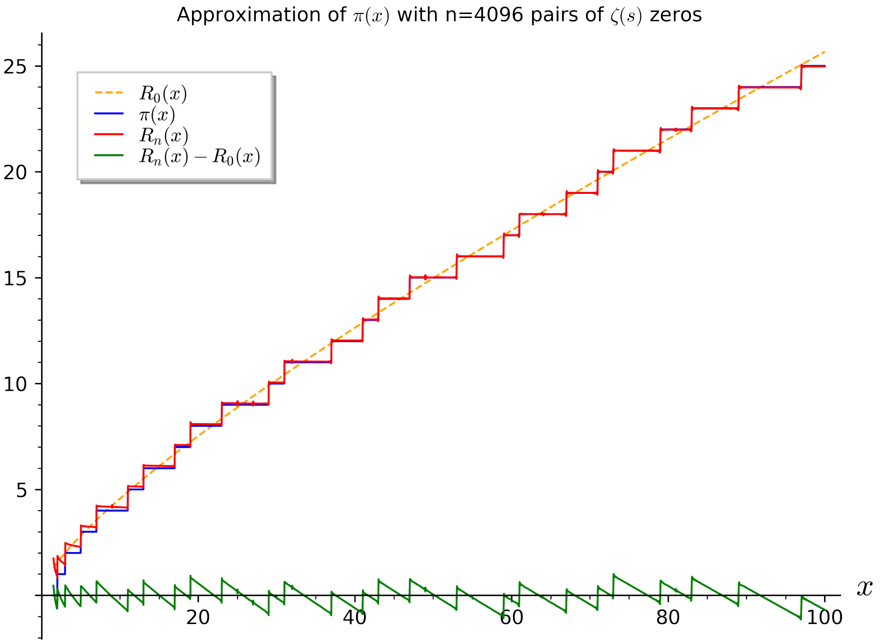

Approximation of $\pi(x)$ with n=256 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x


Approximation of $\pi(x)$ with n=512 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x

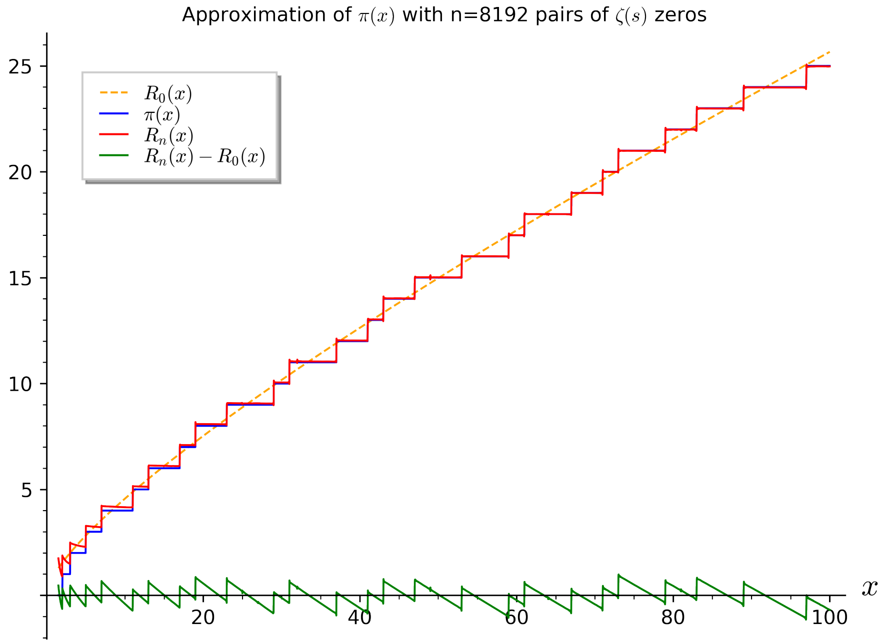


Approximation of $\pi(x)$ with n=1024 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x

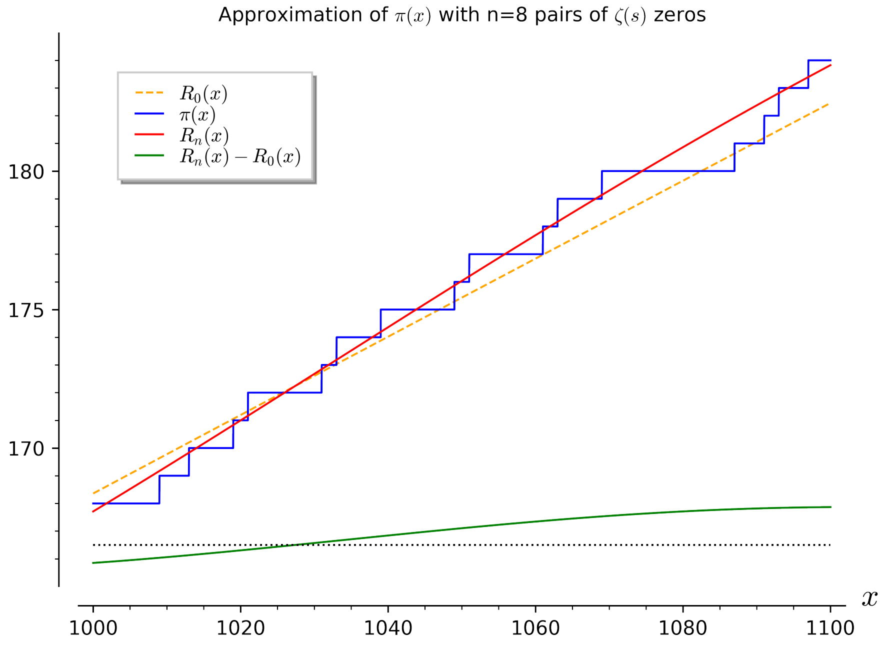

Approximation of $\pi(x)$ with n=2048 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x



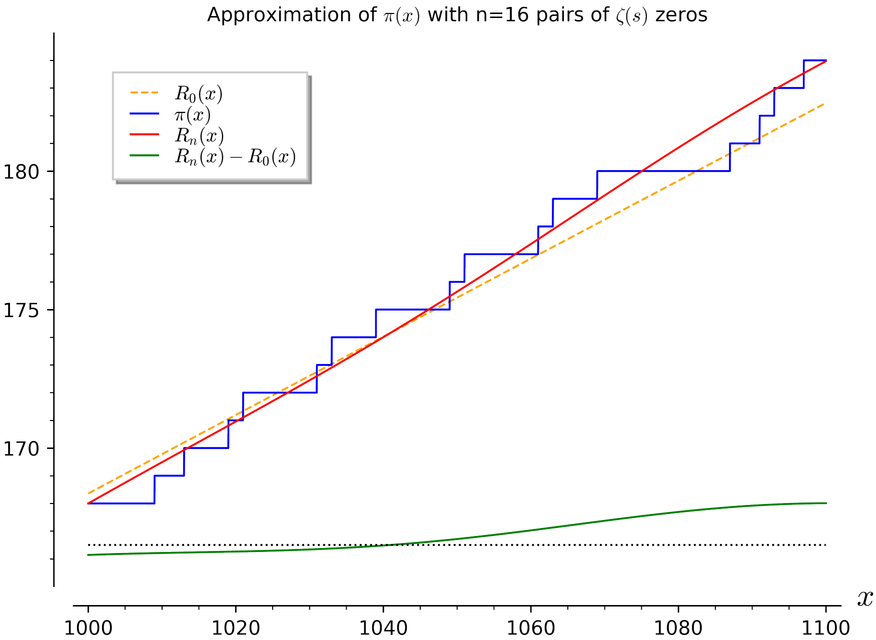
Approximation of $\pi(x)$ with n=4096 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x



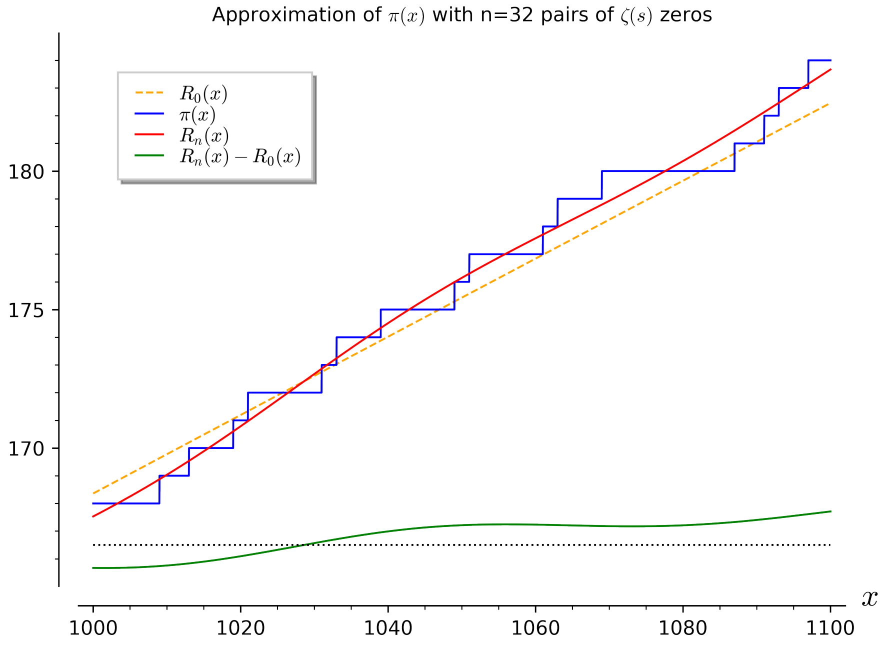
Approximation of $\pi(x)$ with n=8192 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
25
20
15
10
5
20
40
60
80
100
x

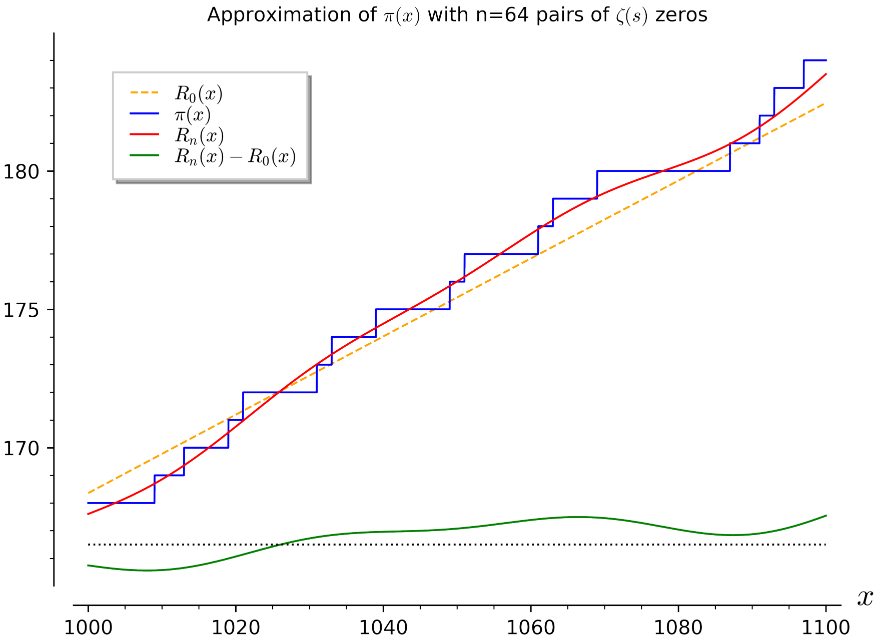


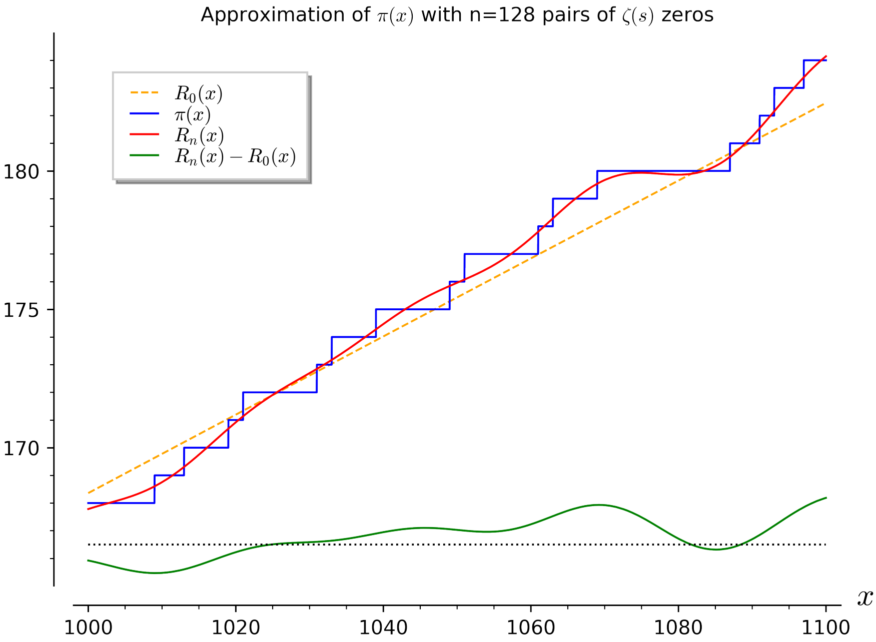
Approximation of $\pi(x)$ with n=8 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

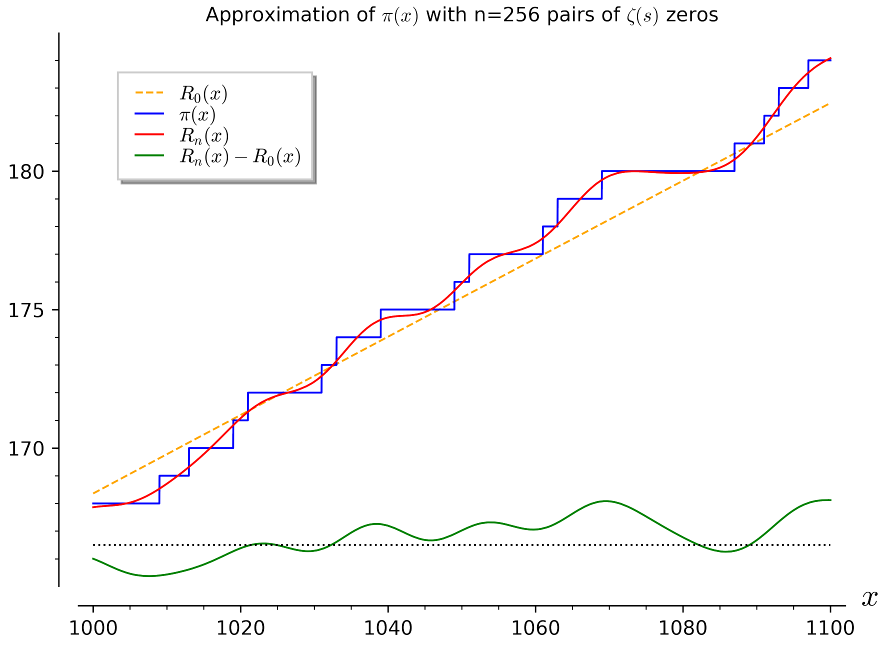


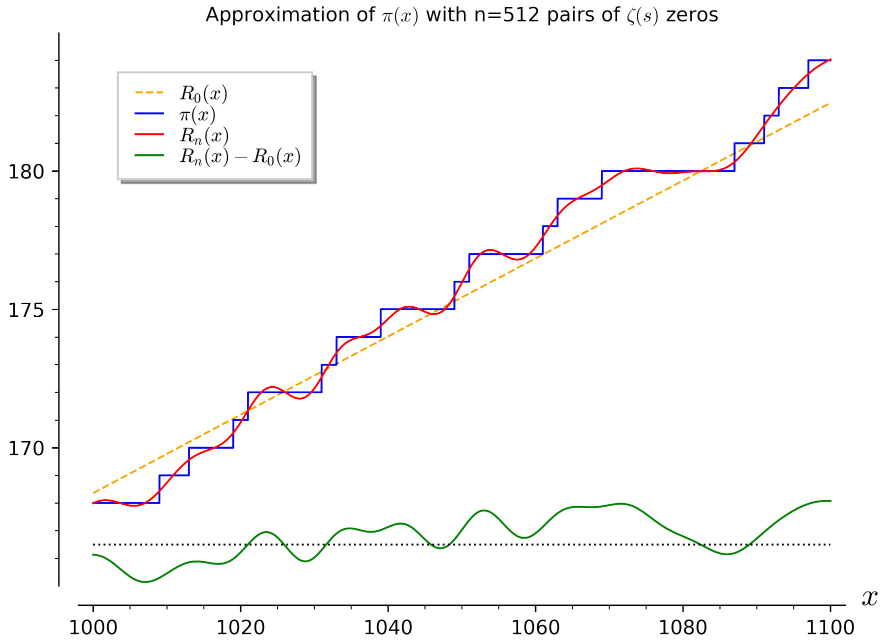
Approximation of $\pi(x)$ with n=16 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x


Approximation of $\pi(x)$ with n=32 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

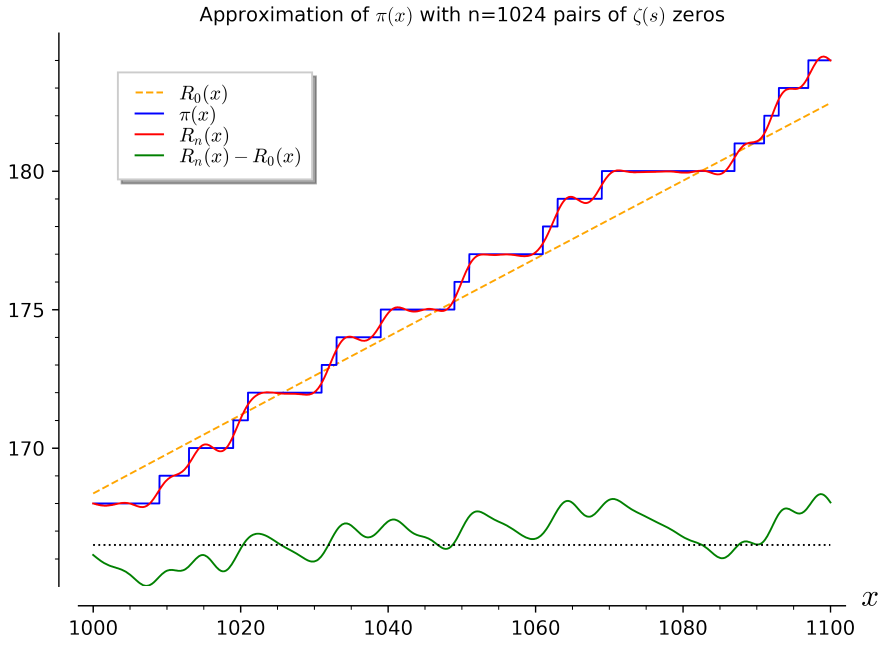

Approximation of $\pi(x)$ with n=64 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x


Approximation of $\pi(x)$ with n=128 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

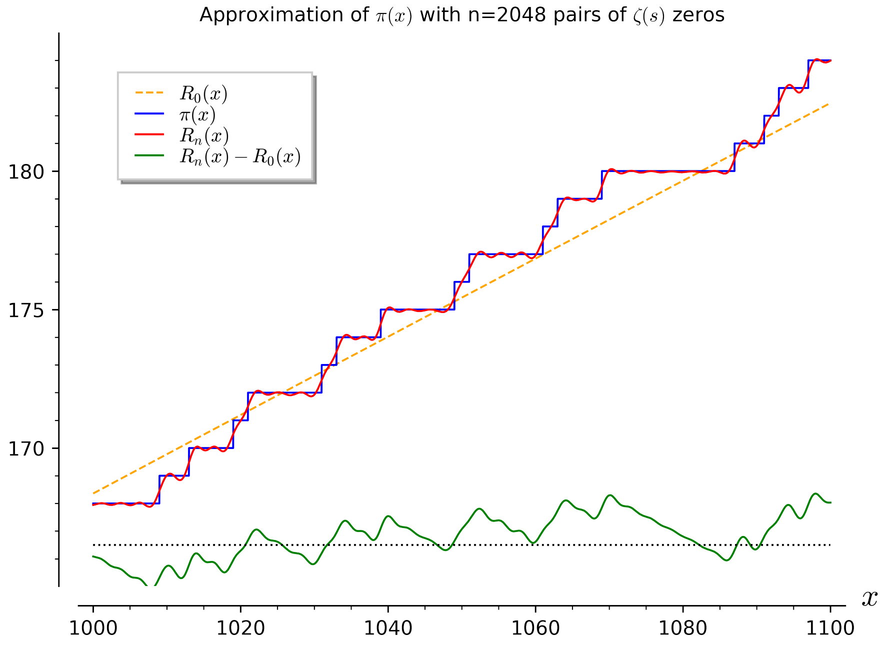

Approximation of $\pi(x)$ with n=256 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

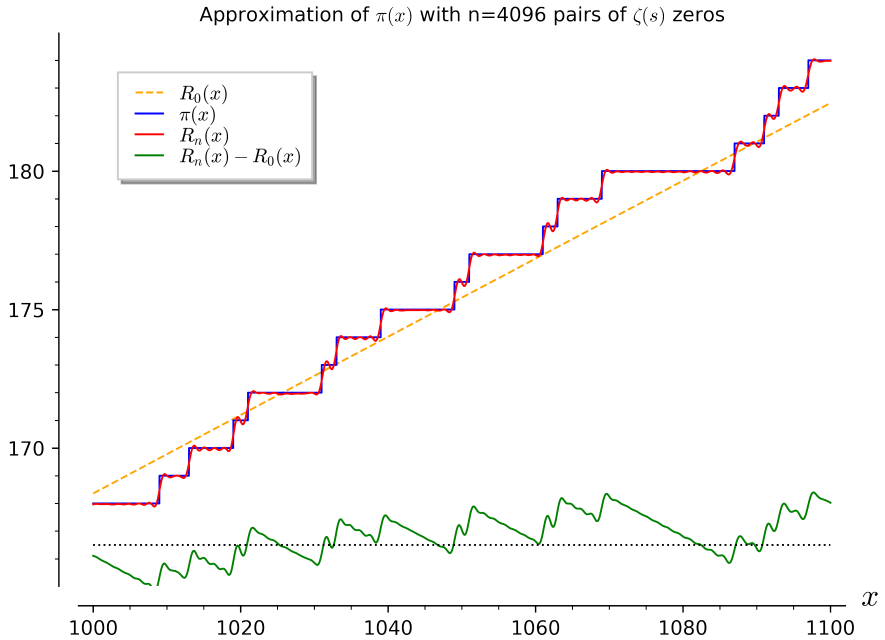


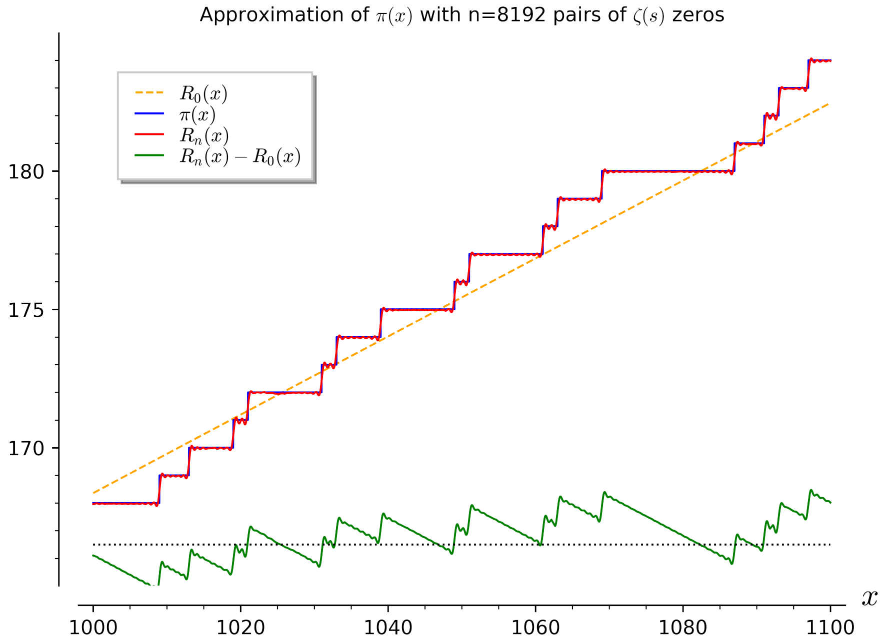
Approximation of $\pi(x)$ with n=512 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x



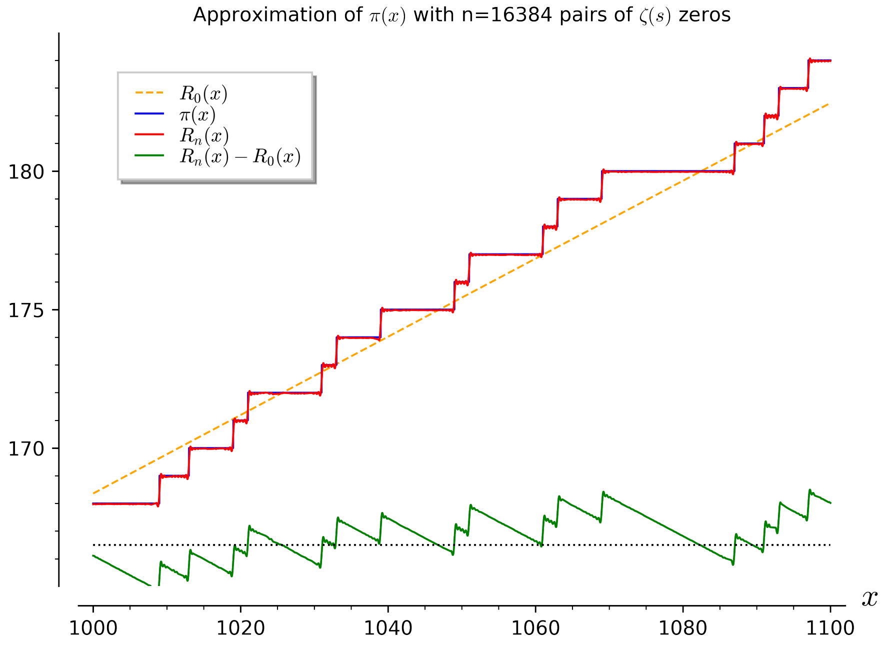
Approximation of $\pi(x)$ with n=1024 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x


Approximation of $\pi(x)$ with n=2048 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

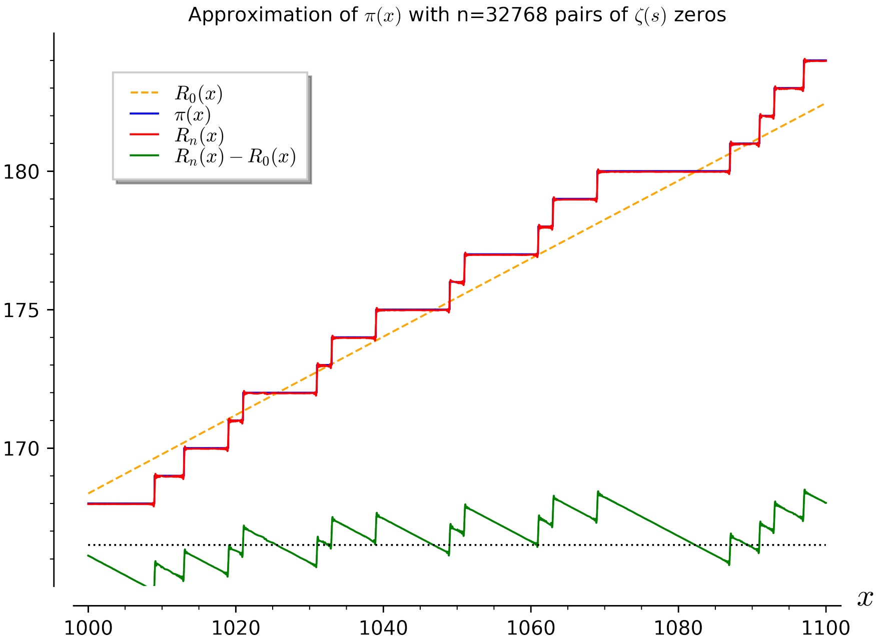

Approximation of $\pi(x)$ with n=4096 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x



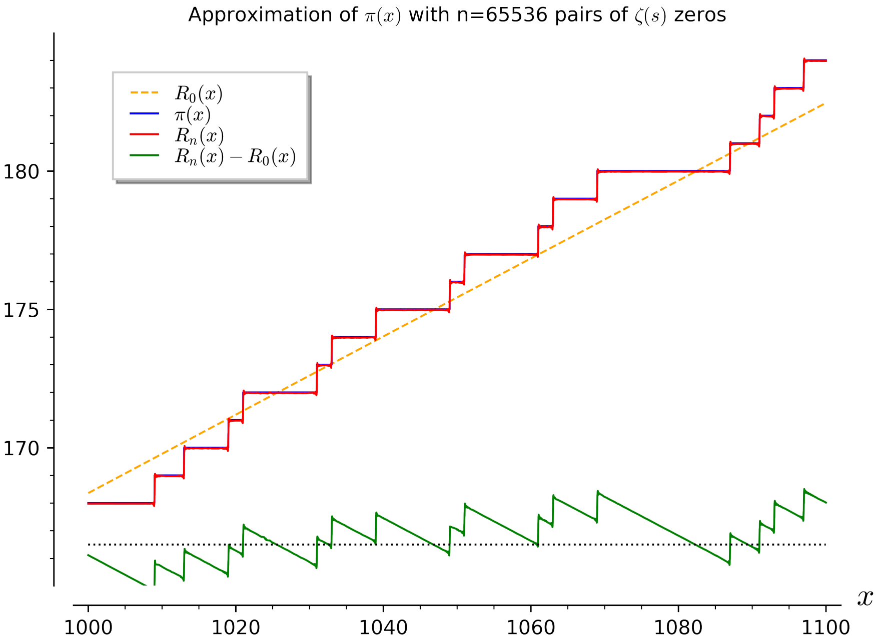
Approximation of $\pi(x)$ with n=8192 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x



Approximation of $\pi(x)$ with n=16384 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
x
1000
1020
1040
1060
1080
1100



Approximation of $\pi(x)$ with n=32768 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x


Approximation of $\pi(x)$ with n=65536 pairs of $\zeta(s)$ zeros
$R_0(x)$
$\pi(x)$
$R_n(x)$
$R_n(x) - R_0(x)$
180
175
170
1000
1020
1040
1060
1080
1100
x

Riemann zeta function is an arithmetic L-function

Arithmetic L-functions have certain properties

- Euler products $L(s) = \prod_p F_p(p^{-s})^{-1}$ with $F_p(t) \in 1 + t\mathbb{C}[t]$ and $\deg F_p(t) \leq d$
  $\Rightarrow L(s) = \sum_{n \geq 1} a_n n^{-s}$, and $a_{nm} = a_n a_m$ if $gcd(n, m) = 1$

Riemann zeta function is an arithmetic L-function

Arithmetic L-functions have certain properties

- Euler products $L(s) = \prod_p F_p(p^{-s})^{-1}$ with $F_p(t) \in 1 + t\mathbb{C}[t]$ and $\deg F_p(t) \leq d$
  $\Rightarrow L(s) = \sum_{n \geq 1} a_n n^{-s}$, and $a_{nm} = a_n a_m$ if $gcd(n, m) = 1$
- By adding some factors
  - $N^{s/2}$ and
  - $\Gamma_L(s) := \prod_j \Gamma_{\mathbb{R}}(s + \mu_j) \prod_k \Gamma_{\mathbb{C}}(s + \nu_k)$,
    where $\Gamma_{\mathbb{R}}$ and $\Gamma_{\mathbb{C}}$ are defined in terms of Γ-function.

  we obtain
  $$\Lambda(s) := N^{s/2}\Gamma_L(s) \cdot L(s) = \varepsilon\overline{\Lambda}((1 + w) - s).$$
  for some $w \in \mathbb{N}$ and $\varepsilon \in \mathbb{C}$ of norm one.

We say

- d is the degree of $L(s)$
- N is the conductor of $L(s)$, and
- w is the (motivic) weight of $L(s)$.

What other L-functions are out there?

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

What happens if we swap some signs? Not every combination works, but some do:

$$L\left(s, \left(\frac{-4}{\bullet}\right)\right) = \prod_{p \equiv 1 \bmod 4} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3 \bmod 4} \frac{1}{1 + p^{-s}} = \prod_p \left(1 - \left(\frac{-4}{p}\right) p^{-s}\right)^{-1}$$

$$L\left(s, \left(\frac{5}{\bullet}\right)\right) = \prod_{p \equiv \pm 1 \bmod 5} \frac{1}{1 - p^{-s}} \prod_{p \bmod 5 \in \{2,3\}} \frac{1}{1 + p^{-s}} \equiv \prod_p \left(1 - \left(\frac{5}{p}\right) p^{-s}\right)^{-1}$$

What other L-functions are out there?

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

What happens if we swap some signs? Not every combination works, but some do:

$$L\left(s, \left(\frac{-4}{\bullet}\right)\right) = \prod_{p \equiv 1 \bmod 4} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3 \bmod 4} \frac{1}{1 + p^{-s}} = \prod_p \left(1 - \left(\frac{-4}{p}\right) p^{-s}\right)^{-1}$$

$$L\left(s, \left(\frac{5}{\bullet}\right)\right) = \prod_{p \equiv \pm 1 \bmod 5} \frac{1}{1 - p^{-s}} \prod_{p \bmod 5 \in \{2,3\}} \frac{1}{1 + p^{-s}} \equiv \prod_p \left(1 - \left(\frac{5}{p}\right) p^{-s}\right)^{-1}$$

If $\zeta(s)$ is associated with $\mathbb{Q}$, then $\zeta(s)L\left(s, \left(\frac{d}{\bullet}\right)\right)$ are associated with $\mathbb{Q}(\sqrt{d})$.

Dedekind zeta function

For $d \equiv 0, 1 \bmod 4$, consider the zero dimensional variety

$$X : x^2 - dx + d(d-1)/4$$

We have $X(\mathbb{C}) = X(\mathbb{Q}(\sqrt{d})) = \{(1 \pm \sqrt{d})/2\}$. Modulo p we have

$$\#X(\mathbb{F}_p) = \begin{cases} 2, & d \in (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = 1 \\ 0, & d \notin (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = -1 \\ 1, & d \equiv 0 \bmod p \Leftrightarrow \left(\frac{d}{p}\right) = 0 \end{cases}$$

$$L_p(t) := \exp\left(\sum_{n \geq 1} \frac{\#X(\mathbb{F}_{p^n}) t^n}{n}\right) = \begin{cases} (1-t)^{-2}, & d \in (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = 1; \\ (1-t^2)^{-1}, & d \notin (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = -1; \\ (1-t)^{-1}, & d \equiv 0 \bmod p \Leftrightarrow \left(\frac{d}{p}\right) = 0. \end{cases}$$

Dedekind zeta function

For $d \equiv 0, 1 \bmod 4$, consider the zero dimensional variety

$$X : x^2 - dx + d(d-1)/4$$

$$L_{d,p}(t) := \exp\left(\sum_{n\geq 1} \frac{\#X(\mathbb{F}_{p^n})t^n}{n}\right) = \begin{cases} (1-t)^{-2}, & d \in (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = 1; \\ (1-t^2)^{-1}, & d \notin (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = -1; \\ (1-t)^{-1}, & d \equiv 0 \bmod p \Leftrightarrow \left(\frac{d}{p}\right) = 0. \end{cases}$$

$$\prod_p L_{d,p}(p^{-s}) = \zeta(s) \prod_p \left(1 - \left(\frac{d}{p}\right) p^{-s}\right) = \zeta(s) L\left(s, \left(\frac{d}{\bullet}\right)\right) =: \zeta_{\mathbb{Q}(\sqrt{d})}(s)$$

Analogously one can defined ζ_K for any number field K.

The residue of $\zeta_K(s)$ at $s = 1$ constains arithmetic information about K.

This is known as the class number formula.

Dedekind zeta function

For $d \equiv 0, 1 \bmod 4$, consider the zero dimensional variety

$$X : x^2 - dx + d(d-1)/4$$

$$L_{d,p}(t) := \exp\left(\sum_{n\geq 1} \frac{\#X(\mathbb{F}_{p^n})t^n}{n}\right) = \begin{cases} (1-t)^{-2}, & d \in (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = 1; \\ (1-t^2)^{-1}, & d \notin (\mathbb{F}_p^2)^\times \Leftrightarrow \left(\frac{d}{p}\right) = -1; \\ (1-t)^{-1}, & d \equiv 0 \bmod p \Leftrightarrow \left(\frac{d}{p}\right) = 0. \end{cases}$$

$$\prod_p L_{d,p}(p^{-s}) = \zeta(s) \prod_p \left(1 - \left(\frac{d}{p}\right) p^{-s}\right) = \zeta(s) L\left(s, \left(\frac{d}{\bullet}\right)\right) =: \zeta_{\mathbb{Q}(\sqrt{d})}(s)$$

Analogously one can defined ζ_K for any number field K.

The residue of $\zeta_K(s)$ at $s = 1$ constains arithmetic information about K.

This is known as the class number formula.

https://www.lmfdb.org/NumberField/

Dirichlet L-functions

Given a Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$ we can associate to it an L-function

$$L(s, \chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$$

https://www.lmfdb.org/Character/Dirichlet/

Dirichlet L-functions

Given a Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$ we can associate to it an L-function

$$L(s, \chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$$

$L(s, \chi)$ were introduced by Dirichlet (1837) to prove Dirichlet's theorem

> There are infinitely many primes of the shape $a + kd$ with $gcd(a, d) = 1$.

Dirichlet L-functions

Given a Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$ we can associate to it an L-function

$$L(s, \chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$$

$L(s, \chi)$ were introduced by Dirichlet (1837) to prove Dirichlet's theorem

> There are infinitely many primes of the shape $a + kd$ with $gcd(a, d) = 1$.

$L(s, \chi)$ also played a crucial role in the proof of Goldbach's weak conjecture

> Every odd integer (> 7) can be written as the sum of three odd primes.

Dirichlet L-functions

Given a Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$ we can associate to it an L-function

$$L(s, \chi) = \prod_p \left(1 - \chi(p) p^{-s}\right)^{-1}$$

$L(s, \chi)$ were introduced by Dirichlet (1837) to prove Dirichlet's theorem

$L(s, \chi)$ also played a crucial role in the proof of Goldbach's weak conjecture

Every odd integer (> 7) can be written as the sum of three odd primes.

Proved recently by Helfgott (2015) where he combined:

- Verification of the Riemann hypothesis $L(s, \chi)$ for a large range of χ (Platt)
- Verification of Goldbach's weak conjecture up to $8.8 \cdot 10^{30}$ (Helfgott-Platt)
- Advancements on understanding zero free regions on the critical strip
- Improvement of Hardy–Littlewood circle method.

Ramanujan τ function

Ramanujan in 1916 also introduced another look alike L-function

$$\sum_{n\geq 1} \tau(n)q^n = q\prod_{n\geq 1}(1-q^n)^{24}$$

He conjectured

1. $\tau(mn) = \tau(m)\tau(n)$, if $gcd(m,n) = 1$
2. $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ for p prime and $n > 0$

In other words, we have $L(s) = \sum_{n\geq 1} \tau(n)n^{-s} = \prod_p (1 - \tau(p)t + p^{11}t^2)^{-1}$.

In the LMFDB this L-function is known by the label 2-1-1.1-c11-0-0.

Ramanujan τ function

Ramanujan τ function also defines a modular form

$$\Delta(z) := \sum_{n\geq 1} \tau(n) q^n = q \prod_{n\geq 1} (1-q^n)^{24}, \quad q = e^{2\pi i z}$$

Then Δ is a modular form of weight 12 on $\mathrm{SL}(2,\mathbb{Z})$.

A (classical) modular form f of weight k on $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$, is a holomorphic function defined on the the upper half plane $\mathcal{H} := \{z : \mathrm{Im}(z) > 0\}$ which satisfies the transformation property

$$f(\gamma z) := f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathcal{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and at all the cusps of Γ (= points at infinity).

One can think of $f(z)(\mathrm{d}z)^k$ as a differential form on the curve $\mathcal{H}/\Gamma$.

Modular forms

A (classical) modular form f of weight k on $\Gamma \subset \mathrm{SL}(2, \mathbb{Z})$, is a holomorphic function defined on the the upper half plane $\mathcal{H} := \{z : \mathrm{Im}(z) > 0\}$ which satisfies the transformation property

$$f(\gamma z) := f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathcal{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and at all the cusps of Γ (= points at infinity).

If $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, then $f(z) = f(z+1)$ and f has a fourier expansion

$$f(z) = \sum_{n \geq 0} a_n q^n, \quad q = e^{2\pi i z}.$$

If $a_0 = 0$ and $a_1 = 1$ these are known as cusps forms.

https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/

L-functions associated with modular forms

Let n be a positive integer, then Hecke defined a linear operator T_n acting on the vector space of modular forms $M_k(\Gamma \supset \Gamma(N) := \{\gamma : \gamma \equiv \mathrm{id} \bmod N\})$

$$T(n)\left(\sum_{m\geq 0} a_m q^m\right) := \sum_m \left(\sum_{d|gcd(m,n)} d^{k-1} a_{mn/d^2}\right) q^m \quad \gcd(n,N) = 1$$

and he showed that

1. $T(mn) = T(m)T(n)$ if $\gcd(m,n) = 1$
2. $T(p^{n+1}) = T(p)T(p^n) - p^{k-1}T(p^{n-1})\chi(p)$ for p prime and $n > 0$ where $\chi(p) = 0$ if $p|N$, and 1 otherwise.

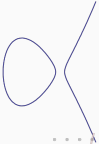
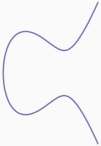
Moreover, if f is an eigenform for all $T(n)$, i.e., $T(n) = \lambda_n f$, then $\lambda_n = a_1 a_n$. If one normalizes $a_1 = 1$ an L-function can be constructed:

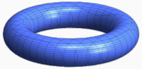
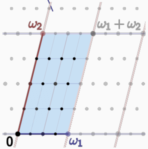
$$L_f(s) := \prod_p \left(1 - a_p p^{-s} + \chi(p) p^{k-1} p^{-2s}\right)^{-1}$$

Elliptic curves

An *elliptic curve* E is a smooth curve defined by

$$E : y^2 = x^3 + ax + b$$

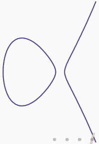
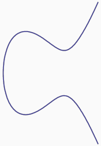
Over $\mathbb{R}$ it might look like  or 

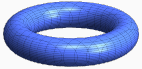
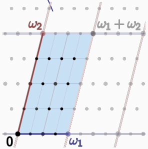
Over $\mathbb{C}$ is a torus  $\simeq$ 

Elliptic curves

An *elliptic curve* E is a smooth curve defined by

$$E : y^2 = x^3 + ax + b$$

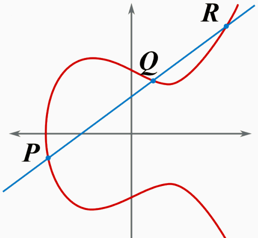
Over $\mathbb{R}$ it might look like  or 

Over $\mathbb{C}$ is a torus  $\simeq$ 

There is a natural *group structure*!

If P, Q, and R are colinear, then

$$P + Q + R = 0$$



Elliptic curves

For p such that $4a^3 + 27b^2 \neq 0 \bmod p$ one might consider

$$\exp\left(\sum_{n\geq 1} \#E(\mathbb{F}_{p^n})\frac{t^n}{n}\right) = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)}, \quad t_p := p + 1 - \#E(\mathbb{F}_p)$$

Thus if one considers $L_E(s) := \prod_p L_{E,p}(p^{-s})^{-1}$ where

$$L_{E,p}(t) := \begin{cases} 1 - a_p t + pt^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p); \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction.} \end{cases}$$

we obtain another look alike L-function.

Modular forms and elliptic curves

Comparing the local factors

$$L_{E,p}(t) := \begin{cases} 1 - a_p t + pt^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p); \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction.} \end{cases}$$

$$L_{f,p}(t) := 1 - a_p t + \chi(p) p^{k-1} t^2$$

There is a striking similarity when $k = 2$.

Given a cusp eigenform f of weight 2 can one construct an elliptic curve E such that

$$L_E(s) = L_f(s)?$$

Modular forms and elliptic curves

Comparing the local factors

$$L_{E,p}(t) := \begin{cases} 1 - a_p t + p t^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p); \\ 1 \pm t, & \text{non-split/split multiplicative reduction}; \\ 1 & \text{additive reduction}. \end{cases}$$

$$L_{f,p}(t) := 1 - a_p t + \chi(p) p^{k-1} t^2$$

There is a striking similarity when $k = 2$.

Given a cusp eigenform f of weight 2 can one construct an elliptic curve E such that

$$L_E(s) = L_f(s)?$$

Yes! This is known as the Eichler–Shimura construction.

Elliptic curves arising this way are called modular.

Modular elliptic curves

Given a cusp eigenform f of weight 2 can one construct an elliptic curve E such that

$$L_E(s) = L_f(s)?$$

Yes! This is known as the Eichler–Shimura construction.

Elliptic curves arising this way are called modular.

Modularity Theorem, formerly the Shimura–Taniyama–Weil conjecture (Wiles)

Every elliptic curve E over $\mathbb{Q}$ is modular.

Fermat's last theorem (Wiles)

$a^n + b^n = c^n$ has no solutins for $a, b, c \in \mathbb{N}$ and $n > 2$

If there was such a solution the elliptic curve

$$y^2 = x(x - a^n)(x - b^n)$$

known as Frey curve could not be modular.

Birch and Swinnerton-Dyer conjecture

Another Millennium Prize Problem listed by the Clay Mathematics Institute.

It shows us how can recover arithmetic information about E from $L_E(s)$.

Recall that $E(\mathbb{Q})$ is an abelian group. In particular,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{torsion}}$$

BSD predicts that the order of vanishing of $L_E(s)$ at the central point $s = 1$ is r.

Birch and Swinnerton-Dyer conjecture

Another Millennium Prize Problem listed by the Clay Mathematics Institute.

It shows us how can recover arithmetic information about E from $L_E(s)$.

Recall that $E(\mathbb{Q})$ is an abelian group. In particular,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{torsion}}$$

BSD predicts that the order of vanishing of $L_E(s)$ at the central point $s = 1$ is r. Furthermore,

$$\frac{1}{r!} L_E^{(r)}(1) = \frac{\mathsf{Sha}(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{\# E(\mathbb{Q})^2_{\mathrm{torsion}}}$$

Birch and Swinnerton-Dyer conjecture

Another Millennium Prize Problem listed by the Clay Mathematics Institute.

It shows us how can recover arithmetic information about E from $L_E(s)$.

Recall that $E(\mathbb{Q})$ is an abelian group. In particular,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{torsion}}$$

BSD predicts that the order of vanishing of $L_E(s)$ at the central point $s = 1$ is r. Furthermore,

$$\frac{1}{r!} L_E^{(r)}(1) = \frac{\mathsf{Sha}(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{\# E(\mathbb{Q})^2_{\mathrm{torsion}}}$$

This formula also allows one to speed up the Eichler–Shimura construction.

Birch and Swinnerton-Dyer conjecture

Another Millennium Prize Problem listed by the Clay Mathematics Institute.

It shows us how can recover arithmetic information about E from $L_E(s)$.

Recall that $E(\mathbb{Q})$ is an abelian group. In particular,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{torsion}}$$

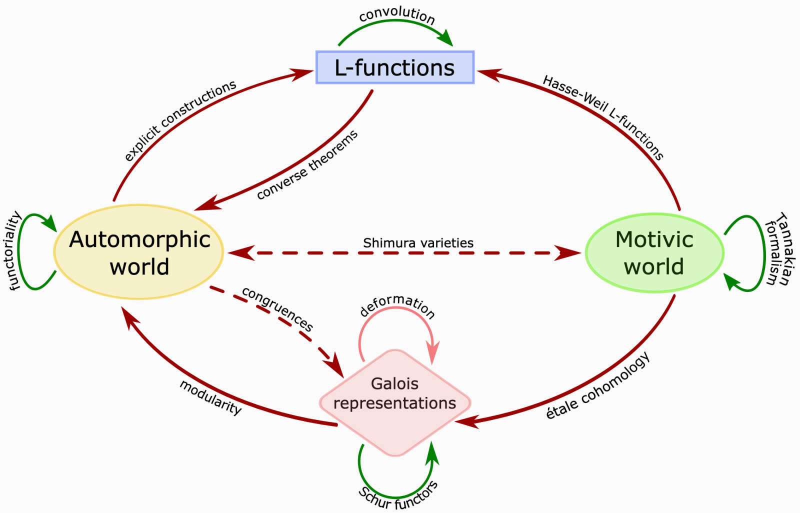
BSD predicts that the order of vanishing of $L_E(s)$ at the central point $s = 1$ is r. Furthermore,

$$\frac{1}{r!} L_E^{(r)}(1) = \frac{\mathrm{Sha}(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{\# E(\mathbb{Q})^2_{\mathrm{torsion}}}$$

This formula also allows one to speed up the Eichler–Shimura construction.

BSD has generalized to other settings.
Bloch–Kato conjectures try to unify these generalizations.

There is much more



https://www.lmfdb.org/ or https://beta.lmfdb.org/