Mathematics and Computation

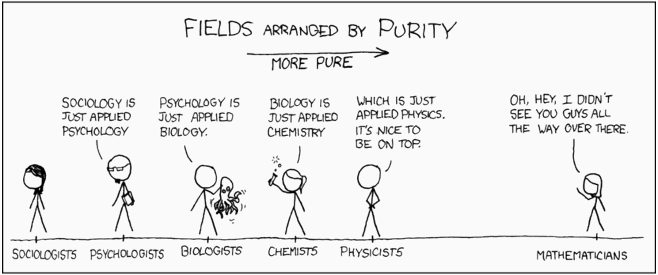
How computation and experimentation inform research

David Lowry-Duda

BYU Focus on Math, March 2022

ICERM
Brown University

The nature of math research



It's said that math is the purest of the sciences — that it is pure abstraction. Does this mean that math research is entirely different than other research in the sciences?

Actually doing math involves *lots* of experimentation, often in the form of examples and counterexamples. One of the most powerful tools for sharpening intuition is to curate a collection of particularly good examples.

The prototypical path in research is to

1. ask a question
2. generate data
3. formulate conjectures (and maybe other questions)
4. test these conjectures
5. try to prove the conjecture (likely prompting more questions)

This might feel familiar! This process is often the same when writing proofs for a class.

Notable examples

Question (Basel Problem)

$$\textit{What is } \sum_{n\geq 1} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \cdots \textit{?}$$

Question (Prime Number Count)

How many primes are there up to N?

Basel Problem: computation as justification

This was asked by Mengoli in 1650 and answered by Euler in 1734. Euler asked whether power series (infinite-degree polynomials) should factor uniquely as a product over their roots. If they did, then perhaps

$$\frac{\sin x}{x} = \left(1 - \frac{x}{\pi}\right)\left(1 + \frac{x}{\pi}\right)\left(1 - \frac{x}{2\pi}\right)\left(1 + \frac{x}{2\pi}\right)\cdots \tag{1}$$

On the one hand, $\frac{\sin x}{x} = 1 - \frac{x^2}{6} + \cdots$ by Taylor series. On the other hand, the collected coefficient of x^2 from the right of (1) is $\frac{1}{\pi^2}\sum\frac{1}{n^2}$. This suggests that

$$\sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Euler then computed the sum to several digits (using what we now call Euler-Maclaurin summation), and $\pi^2/6$ to several digits, and saw that they agreed. This was good enough for him!

(About 100 years later, Weierstrass proved that (1) is actually true).

Prime number theorem: computation as conjecture

It's not too hard to show that there are infinitely many primes, but how many primes are there up to a fixed number N? How would you begin to try to answer this question?

The resolution of this problem includes computational efforts by many, performed over more than 100 years.

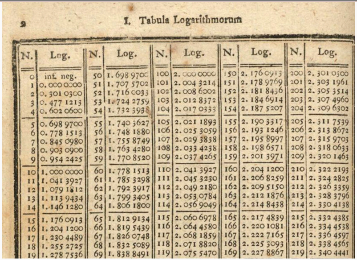
In 1777, Felkel published tables of factorizations of all numbers up to 408000 (and thus also a table of the primes). In 1783, Vega published tables of computed logarithms.

Tables

In 1797, Legendre examined these tables (*both*, as how does one compute logs?) and conjectured that the number of primes less than N (which we denote by $\pi(N)$) is approximately given by

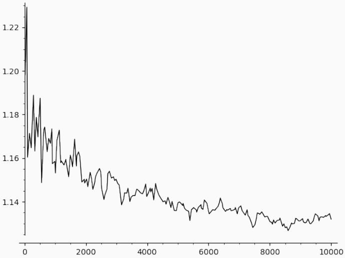
$$\pi(N) \approx \frac{N}{a \log N + b}$$

for some constants a and b. We can replicate some of his thinking when we look at the ratio of $\pi(n)/(n/\log n)$, plotted at right. (Visualization is itself an important tool in research).



2 I. Tabula Logarithmorum

N.	Log.	N.	Log.	N.	Log.	N.	Log.	N.	Log.
0	inf. neg.	50	1. 698 9700	100	2. 000 0000	150	2. 176 0913	200	2. 301 0300
1	0. 000 0000	51	1. 707 5702	101	2. 004 3214	151	2. 178 9769	201	2. 303 1961
2	0. 301 0300	52	1. 716 0033	102	2. 008 6002	152	2. 181 8436	202	2. 305 3514
3	0. 477 1213	53	1. 724 2759	103	2. 012 8372	153	2. 184 6914	203	2. 307 4960
4	0. 602 0600	54	1. 732 3938	104	2. 017 0333	154	2. 187 5207	204	2. 309 6302
5	0. 698 9700	55	1. 740 3627	105	2. 021 1893	155	2. 190 3317	205	2. 311 7539
6	0. 778 1513	56	1. 748 1880	106	2. 025 3059	156	2. 193 1246	206	2. 313 8672
7	0. 845 0980	57	1. 755 8749	107	2. 029 3838	157	2. 195 8997	207	2. 315 9703
8	0. 903 0900	58	1. 763 4280	108	2. 033 4238	158	2. 198 6571	208	2. 318 0633
9	0. 954 2425	59	1. 770 8520	109	2. 037 4265	159	2. 201 3971	209	2. 320 1463
10	1. 000 0000	60	1. 778 1513	110	2. 041 3927	160	2. 204 1200	210	2. 322 2193
11	1. 041 3927	61	1. 785 3298	111	2. 045 3230	161	2. 206 8259	211	2. 324 2825
12	1. 079 1812	62	1. 792 3917	112	2. 049 2180	162	2. 209 5150	212	2. 326 3359
13	1. 113 9434	63	1. 799 3405	113	2. 053 0784	163	2. 212 1876	213	2. 328 3796
14	1. 146 1280	64	1. 806 1800	114	2. 056 9049	164	2. 214 8438	214	2. 330 4138
15	1. 176 0913	65	1. 812 9134	115	2. 060 6978	165	2. 217 4839	215	2. 332 4385
16	1. 204 1200	66	1. 819 5439	116	2. 064 4580	166	2. 220 1081	216	2. 334 4538
17	1. 230 4489	67	1. 826 0748	117	2. 068 1859	167	2. 222 7165	217	2. 336 4597
18	1. 255 2725	68	1. 832 5089	118	2. 071 8820	168	2. 225 3093	218	2. 338 4565
19	1. 278 7536	69	1. 838 8491	119	2. 075 5470	169	2. 227 8867	219	2. 340 4441



Legendre later made the explicit conjecture that

$$\pi(N) \approx \frac{N}{\log N - 1.08366}.$$

Dirichlet and Gauss made related conjectures in the early 1800s. Around 1850, Chebyshev considered the limit

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log n}. \tag{2}$$

He showed that if this limit exists, then it is equal to 1, and he gave unconditional upper and lower bounds for the ratio.[1]

In 1859, Riemann presented his memoir (introducing the Riemann zeta function $\zeta(s)$), describing how to apply complex analysis and $\zeta(s)$ to study $\pi(N)$. Finally, in 1896, Hadamard and de la Vallée Poussin completed (independent) proofs that (2) exists and equals 1.

[1] His proof is itself very computational! He had to find particular weights that minimized a family of approximations.

As we can see, research has been guided by computational experimentation for hundreds of years.

But the nature of computation has recently changed. (For example, we no longer need to consult tables of logarithms).

Role of computers

Computers can generate *a lot* of data and can often be used to *rapidly* test conjectures and ideas. Computer driven research began with the dawn of computing, and entirely new areas of math have formed around computer automation.

SOME CALCULATIONS OF THE RIEMANN ZETA-FUNCTION

By A. M. TURING

[Received 29 February 1952.—Read 20 March 1952]

Introduction

IN June 1950 the Manchester University Mark 1 Electronic Computer was used to do some calculations concerned with the distribution of the zeros of the Riemann zeta-function. It was intended in fact to determine whether there are any zeros not on the critical line in certain particular intervals.

Sometimes, it is now possible to set up problems for *exhaustive* search (and to make computers do the exhausting part).

Data and proof

Here is a pair of examples (which we'll explain more in a moment).

Theorem

For all integer $n \in \mathbb{Z}_{\geq 0}$*, we have that* $\displaystyle\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Proof: We verify this explicitly for $n = 0, 1, 2, 3, 4$. These cases prove the theorem.

Theorem

For every triangle ABC*, the angle bisectors intersect at one point.*

Proof: We verify this explicitly for the 64 triangles for which $\angle A = 10^\circ, \ldots, 80^\circ$ and $\angle B = 10^\circ, \ldots, 80^\circ$. These cases prove the theorem.

What's going on here? The idea is that with a bit of extra insight, we can reduce proving a general result to a finite number of explicit computations.

In the first example, the key insight is that $\sum_{j=1}^{n} j^k$ is a degree $k+1$ polynomial[2] in n. The first proof then relies on the fact that a degree 4 polynomial is uniquely determined by 5 points.

In the second example, the key insight is the computation that coordinates of pairs of angle bisectors are rational functions of degree ≤ 7 in $\tan(\angle A/2)$ and $\tan(\angle B/2)$, which are uniquely determined by 64 values.

[2] I encourage you to prove this if you haven't seen it!

How exhausting can it be?

- **Bounded gaps between primes**: There is a number $d \leq 246$ such that there are infinitely many primes of the form $p, p+d$.
  Initially Yitang Zhang showed this with $d \leq 7 \cdot 10^7$. The Polymath8 project designed algorithms to find "weights" to reduce d; the weights are easily verified.
- **Ternary Goldbach**: Every odd integer $n \geq 5$ can be written as the sum of three primes.
  Helfgott (with *lots* of computer power) showed that this is true for all $n \geq 10^{27}$. Explicit verification for all numbers up to 10^{27} completes the proof; any individual decomposition can be verified.
- **Four color theorem**: No planar map requires more than 4 colors. The proof involved reducing the problem to consider maps from a finite set of types, from a finite set of configurations. Computers verified each of these; it is impractical to human verify these computations.

My work as an experimental and computational mathematician

During grad school, I began to use computers as an *experimental* tool to help guide my research. I was studying problems related to the *Gauss circle problem*:

Question (Gauss circle problem)

How many integer points $(n, m) \in \mathbb{Z}^2$ are contained inside a circle of radius R centered at the origin? Call this $N(R)$.

In the 1790s, Gauss showed that $N(R) = \pi R^2 + O(R)$. And maybe he thought that was as good as one could do? In the 1900s, Sierpiński showed that actually the error term is at most $O(R^{2/3})$ and (computationally) suggested that it might be $O(R^{1/2})$.

I was studying these problems from the perspective of modular forms, which are highly self-symmetric holomorphic complex functions with many special properties.

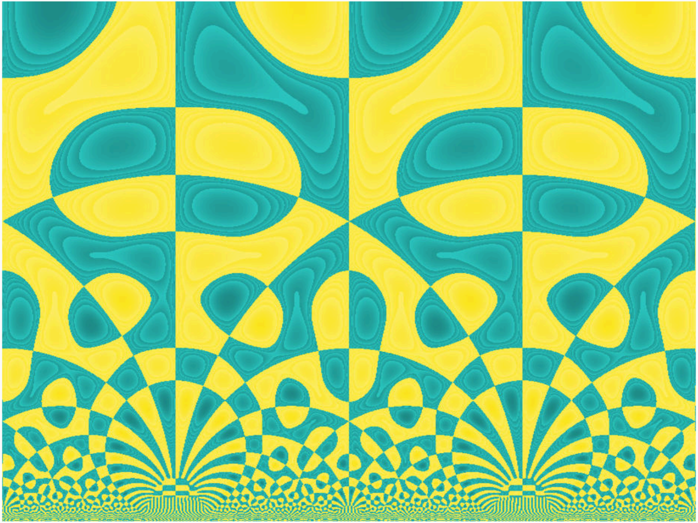
Briefly but concretely, a modular form f is a complex-valued, differentiable function on $\mathcal{H} = \{x + iy : y > 0\}$ that satisfies an infinite family of symmetries of the shape

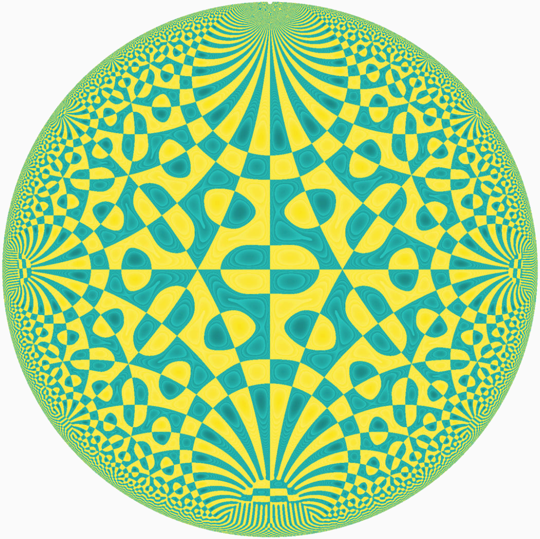
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for a fixed k, and *any* choice of integers a, b, c, d such that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant 1. Each modular form has a Fourier expansion of the form

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z},$$

and “doesn’t grow too big” anywhere.





There is a modular form (typically called θ^2) whose properties include data related to the Gauss circle problem. In particular,

$$\theta^2(z) = 1 + \sum_{n \geq 1} r_2(n) e^{2\pi i n z}$$

where $r_2(n)$ is the number of ways of writing n as a sum of two squares. We can show that

$$N_2(R) = \sum_{n \leq R^2} r_2(n).$$

In order to recover estimates for $N_2(R)$ from θ^2, one uses the associated *L*-function

$$L(s, \theta^2) = \sum_{n \geq 1} \frac{r_2(n)}{n^s}.$$

(This L-function behaves in many ways like $\zeta(s)$).

I was working on relating modular properties of θ^2 to estimates for the Gauss circle problem (and related topics). Modular forms have beautiful properties, but they can be challenging to reason about. To understand which directions to investigate further, I began to perform numerical experiments.

I used sage (also called sagemath), a free math computer algebra system written largely by researchers and building on decades of established research software.

For more sophisticated data associated to modular forms, I turned to the L-function and Modular Form Database (LMFDB).

In my field of analytic number theory, it is often possible to work *really hard with lots of technical effort* to improve a result, but it's also possible to work really hard and prove nothing more. Initially I experimented to determine areas which might yield to more scrutiny.

This led to my thesis, as well as [HKLDW18, HKLDW21] (and other related papers included in the bibliography).

Experiments suggested that many of our results (particularly in the Laplace transform aspect) were best possible — which led to [LD20a]. But it was also very clear that much of what we could prove was far from the truth.[3]

It felt like the only place with information on these gaps was the LMFDB, and I joined its development team.

[3]In these projects, this is related to understanding the distribution and behavior of Maass forms, which I'm talking about tomorrow!

Background on the LMFDB and its purpose

That modular forms hold arithmetic data (in this case, about counting lattice points in the Gauss circle problem) is not a coincidence. This is a piece of a large family of ideas called the Langlands program.

Broadly speaking, the Langlands program suggests that arithmetic or algebrogeometric objects are deeply connected to modular forms. For example, the $\mathbb{Q}$-Modularity Theorem asserts that every elliptic curve defined over $\mathbb{Q}$ is related to a modular form, and was the final ingredient in the proof of Fermat's Last Theorem.

Langlands suggests that the Modularity Theorem should be true more generally, for example with $\mathbb{Q}$ replaced by any number field. Most of these generalizations remain unknown.

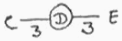
In many cases, we don't even have explicit conjectures formed yet on what to expect.

Background on the LMFDB and its purpose

The heart of the Langlands program is the concept of the *L*-function. The LMFDB seeks to describe relationships between *L*-functions, modular forms, and algebrogeometric objects. This continues the tradition of making tables to inspire others, and makes it available electronically (LMFDB.org).[4]

For example, it includes information such as this portion of elliptic curve data from the 1976 Antwerp IV tables.[5]

		38 = 2.19										
A	1	1	1	0	1	-	5, 1	I5,	I1	5, 1	5	0
B	1	1	1	-70	-279	-	1, 5	I1,	I5	1, 5	1	0
C	1	0	1	-16	22	-	3, 1	I3,	I1	3, 1	3	0
D	1	0	1	9	90	-	9, 3	I9,	I3	9, 3	3	0
E	1	0	1	-86	-2456	-	27, 1	I27,	I1	27, 1	1	0
		39 = 3.13										
A	1	1	0	1	0	-	1, 1	I1,	I1	1, 1	2	0
B	1	1	0	-4	-5	+	2, 2	I2,	I2	2, 2	4	0
C	1	1	0	-69	-252	+	4, 1	I4,	I1	4, 1	2	0
D	1	1	0	-19	22	+	1, 4	I1,	I4	1, 4	4	0



---

[4] If you want to see what's up and coming, see beta.lmfdb.org for portions in trial.
[5] This part of the tables corresponds to the five elliptic curves at `https://www.lmfdb.org/EllipticCurve/Q/38/` and the four elliptic curves at `https://www.lmfdb.org/EllipticCurve/Q/39/`.

Background on the LMFDB and its purpose

The LMFDB isn't so different from the log and prime tables of Felkel and Vega. It is a huge collection of number theoretic and algebraic data that can be used to formulate and test conjectures.

Systematic computation of elliptic curves and their L-functions led to the formulation of the Sato–Tate conjecture, modularity conjecture, and the Birch and Swinnerton-Dyer conjecture.

The frontiers of research are advancing: to more complicated curves of higher genus, more general geometric surfaces, and modular forms of higher degree. The LMFDB aims to provide data for new conjectures, ideas, and theorem.

The LMFDB has been cited in nearly 500 papers, and we are continuing to add and connect data.

I went from doing *experimental* number theory to doing *computational* number theory: I designed and implemented algorithms for rigorous computation. A strong grasp of a subject is required to implement efficient computation.

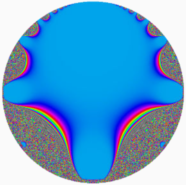
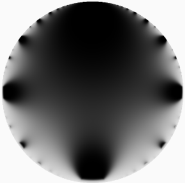
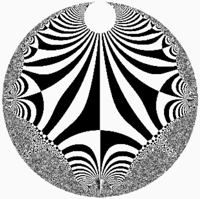
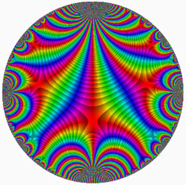
Deliberate computation leads to more understanding.

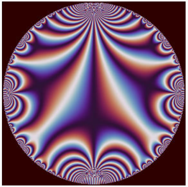
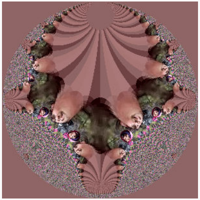
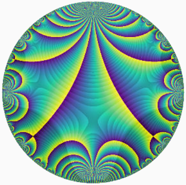
One of the first major projects I worked on with the LMFDB was to explicitly compute and verify classical modular forms — and to identify related algebraic objects.[6]

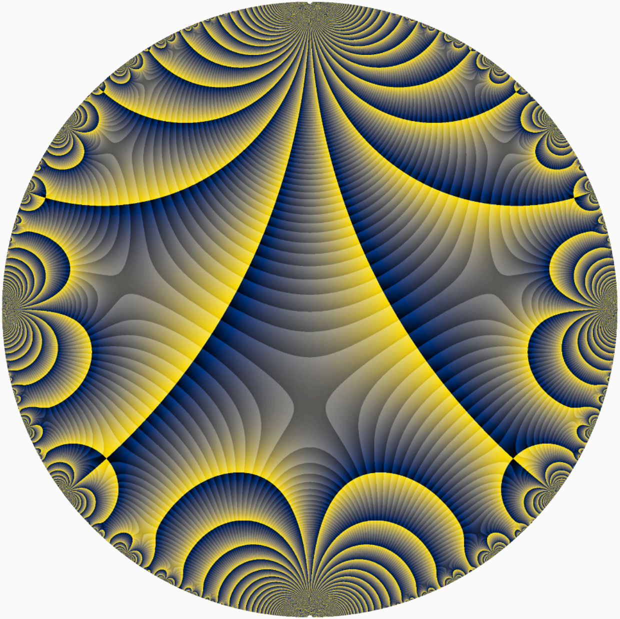
[6] This was a large effort by many people, described more in [BBB$^+$22].

Visualization

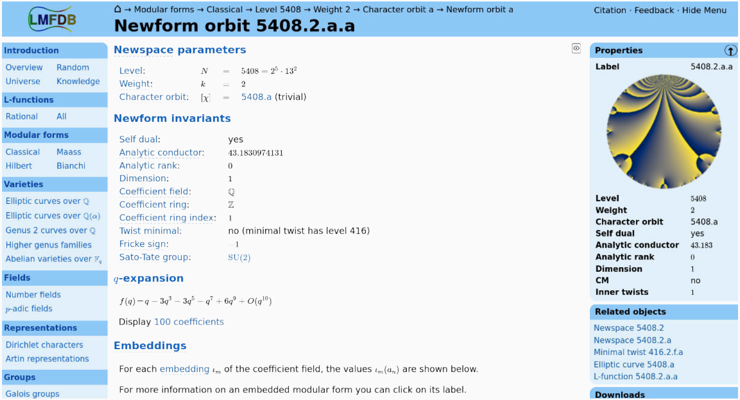
When viewing the database from the website, we want most objects to have a "portrait", ideally giving a meaningful mathematical description. While computing modular forms, I began to think about how they should be visualized.



https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/5408/2/a/a/



There are over 14 million other modular forms on the LMFDB.

Aside on visualizing modular forms

For more on visualizing modular forms and complex function visualization in general, see *Visualizing Modular Forms*, [LD22].

Much of the code I wrote to make the visualizations in the LMFDB is available at [LD20b].

This complex visualization software will be included in the next release of sage (sage9.6), available through `complex_plot`.

I'm now working on developing methods of computing fundamental objects related to modular forms called Maass forms, among other things.

My colleagues and collaborators are working on topics such as

- incorporating modular curves into the LMFDB,
- writing efficient p-adic software,
- computing half-integral weight modular forms,
- studying abelian surfaces,

and many more.

> Science is what we understand well enough to explain to a computer. Art is everything else we do. And over the last several years, an important part of mathematics has been transformed from an Art to a Science.
>
> Science advances whenever an art becomes a science. And the state of the Art advances too, because people always leap into new territory once they have understood more about the old.

- Donald Knuth

Conclusion

Computation and experimentation have been at the heart of research for hundreds of years.

Those with interest and facility in both computation and fundamental mathematics have an enhanced opportunity to prove theorems, develop algorithms, explore and create guiding examples, collect data, and to produce scholarly resources like the LMFDB that help the efforts of others.

Thank you very much.

Please note that these slides (and references for the cited works) are (or will soon be) available on my website (davidlowryduda.com).

References i

Alex J Best, Jonathan Bober, Andrew R Booker, Edgar Costa, John Cremona, Maarten Derickx, David Lowry-Duda, Min Lee, David Roe, Andrew V Sutherland, and John Voight.
Computing classical modular forms.
Simons Symposia on Arithmetic Geometry, Number Theory, and Computation, 2022.
`https://arxiv.org/abs/2002.04717`.

Thomas A. Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
Short-interval averages of sums of Fourier coefficients of cusp forms.
J. Number Theory, 173:394–415, 2017.
https://dx.doi.org//10.1016/j.jnt.2016.09.004.

Thomas A. Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
Sign changes of coefficients and sums of coefficients of L-functions.
J. Number Theory, 177:112–135, 2017.
https://dx.doi.org//10.1016/j.jnt.2017.01.007.

Thomas Andrew Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
The second moment of sums of coefficients of cusp forms.
J. Number Theory, 173:304–331, 2017.
https://arxiv.org/abs/1512.01299.

Thomas A. Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
Second moments in the generalized Gauss circle problem.
Forum Math. Sigma, 6:Paper No. e24, 49, 2018.
https://arxiv.org/abs/1703.10347.

Thomas A. Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
The Laplace transform of the second moment in the Gauss circle problem.
Algebra Number Theory, 15(1):1–27, 2021.
https://arxiv.org/abs/1705.04771.

David Lowry-Duda.
Non-real poles and irregularity of distribution.
J. Number Theory, 217:23–35, 2020.
https://arxiv.org/abs/1910.09969.

David Lowry-Duda.
phase_mag_plot.
https://github.com/davidlowryduda/phase_mag_plot/,
September 2020.
[Online; Reference version at
https://doi.org/10.5281/zenodo.4035117].

David Lowry-Duda.
Visualizing modular forms.
Simons Symposia on Arithmetic Geometry, Number Theory, and Computation, 2022.
https://arxiv.org/abs/2002.05234.