Seewoo Lee
Research Statement

My research centers on number theory, particularly delving into the realms of automorphic forms and the (relative) Langlands program, leveraging computational tools to enhance exploration and understanding.

Relative Langlands program

Introduced by Robert Langlands, the *Langlands Program* constitutes a comprehensive unification theory in number theory and beyond, seeking to establish connections between *automorphic forms / representations* and *Galois representations*. More precisely, for a given automorphic representation π of a group $G(\mathbb{A}_{\mathbb{Q}})$, one expect that there exists an associated Galois representation $\rho_{\pi} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \check{G}(k)$ for $k = \mathbb{C}$ or $\overline{\mathbb{Q}_{\ell}}$ such that the automorphic L-function $L(s, \pi)$ is equal to the Artin L-function $L(s, \rho_{\pi})$ (here $\check{G}$ is the Langlands dual group of G). The most well-understood case is when $G = \mathrm{GL}_1$, which is essentially the class field theory. When $G = \mathrm{GL}_2$, the conjecture is known when π is associated to the holomorphic modular forms, which is the celebrated modularity theorem by Wiles, Taylor, and others, and also the key step for the proof of Fermat's Last Theorem.

Recently, there's an emerging interest in the *relative* Langlands program, which aims to generalize the classical Langlands program to the case of spherical varieties [45, 46]. Especially, one of the main goal of the relative Langlands program is to give a systematic treatment of the abundant examples of the identities bewteen the automorphic periods and the special values of L-functions, including the works by Hecke, Iwasawa–Tate, Rankin–Selberg, Godement–Jacquet, Ichino–Ikeda, and Lapid–Mao. Also, Ben-Zvi, Sakellaridis, and Venkatesh proposed a conjectural *duality* in relative Langlands program [4], which suggests that one expect a dual pair $\check{G} \curvearrowright \check{M}$ to a given hamiltonian G-space $G \curvearrowright M$, where one expect a *dual identity* on the automorphic periods and the special values of L-functions associated to the dual pair, by simply exchanging the roles of (G, M) and $(\check{G}, \check{M})$.

Mao–Rallis trace formula for dual pairs

I'm also working on the conjectural Ichino–Ikeda type formula for the dual pairs introduced by Mao and Rallis [41]. For simple, split, and simply laced groups G' which is not of the type A_n, Mao and Rallis construct a dual pair (SL_2, G) in G', using Heisenberg groups of G', which includes the case of $(\mathrm{SL}_2, \mathrm{SL}_6)$ in E_6. They proposed conjectural relative trace formulae for the dual pairs, which should relate the period integrals of automorphic forms on G (resp. SL_2) and special L-values associated to the automorphic representations of SL_2 (resp. G). The authors proved fundamental lemma for the unit elements in the Hecke algebras of G and SL_2. Recently, Mao–Wan–Zhang [42] formulated the refined version of the conjecture (Ichino–Ikeda type formula) in context of the relative Langlands program

[4], and proved smooth transfer of the local functions for non-archimedean places. With Yuchan Lee, we are working completing the comparision of the relative trace formula for the (SL_2, SL_6) case, by proving the fundamental lemma for the full Hecke algebras, along with the smooth transfer at the archimedean places and spectral decomposition of the relative traces. Combined with the result of Lapid–Mao [32] on Whittaker–Fourier coefficients, this would prove one direction of the non-refined version of the conjecture: if Π is a cuspidal automorphic representation of SL_2 and π is a functorial lift of Π to G through the morphism between L-groups $PGL_2 \to {}^L G$, then the Mao–Rallis automorphic period is nonzero if the adjoint L-value $L(1, \Pi, \mathrm{Ad})$ of Π is nonzero. We also expect to prove the refined formula by proving the local relative character identities, and combine with refined identity of Lapid–Mao for SL_2. Note that the refined formula is "dual" to the conjectural formula for the Ginzburg–Rallis periods and exterior cube L-values of PGL_6 [23].

Ichino–Ikeda formula for general spin groups (Bessel case)

For example, the Gan–Gross–Prasad conjecture [22] proposes an answer to the restriction problem - restricting an automorphic representation on a group to a subgroup - in terms of non-vanishing of the special values of the associated L-functions. Ichino and Ikeda presented a refined version of the conjecture, an equation directly relates period integrals and L-values, and proved certain cases [28]. Building upon the groundwork laid by Liu [40] on the special orthogonal groups ($SO_2 \times SO_5$ and $SO_3 \times SO_6$) and drawing insights from Emory's work [19] on *general spin groups* ($GSpin_n \times GSpin_{n+1}$ for $n = 2, 3, 4$), I am working on the Ichino–Ikeda conjecture for general spin groups, particularly in cases involving general Bessel periods. Furthermore, I'm trying to generalize Furusawa and Morimoto's work on the $SO_2 \times SO_{2n+1}$ case and Böcher's conjecture [21] in this direction. My approach involves leveraging exceptional isomorphisms between low-rank general spin groups and other classical groups and reducing the conjecture to the already known cases.

Computational Approach in Number Theory

In the realm of the Langlands Program, dealing with abstract objects like Galois representations and automorphic forms often benefits from grounding these concepts in tangible, computable counterparts. Especially, these "classical" objects (e.g. modular forms and Maass wave forms, instead of automorphic representations of $GL_2(\mathbb{A}_\mathbb{Q})$) are usually easy to compute explicitly with help of computer algebra systems like SageMath [49] or MATLAB [29].

Modular forms and optimal sphere packings

Optimal sphere packing problem asks the densest packing of d-dimensional space $\mathbb{R}^d$ with unit balls. The problem is trivial for $d = 1$, and $d = 2$ case is solved by Thue in 1890. The three-dimensional case, known as Kepler's conjecture, was resolved by Thomas Hales based

on heavy computer calculations [26]. It took nearly a decade to be formally checked via computer proof assistants HOL Light and Isabelle [25].

A surprising bridge emerges between the 8 and 24-dimensional sphere packing problem and number theory. Cohn and Elikies introduced the *linear programming bound* [13], which suggests that identifying specific "magic functions" holds the key to optimal sphere packing in these dimensions. However, constructing these functions, requiring control over both the function and its Fourier transform, is challenging due to the uncertainty principle. Maryna Viazovska used modular forms from number theory to construct a magic function for dimension 8 [50], and the 24-dimensional case was soon resolved using similar methods [14].

To prove these two cases, the authors [50, 14] relied on numerical approximations and extensive computer assisted computations to establish desired inequalities between modular forms. However, it is natural to ask if there is a more general and conceptual proof for these inequalities. While a more straightforward proof exists for the case of dimension 8 by Dan Romik [44], I found *algebraic* proofs for both of the dimensions 8 and 24 cases that circumvents reliance on numerical calculations or approximations [36]. Notably, I develop a theory of *positive* and *completely positive* quasimodular forms, and use the theory to study the *magic modular forms* appear in the optimal sphere packing. I also found an interesting connection with Kaneko and Koike's *extremal quasimodular forms* [31], which are conjectured to have nonnegative Fourier coefficients. The main ingredients are the differential equations satisfied by the modular forms. This also opens a new possibility to generalize Viazovska's construction to the dimensions other than 8 and 24, based on the construction of Fourier eigenfunctions by Feigenbaum, Grabner, and Hardin [20]. Especially, it would imply a new upper bound for the uncertainty principle [5] in specific dimensions. Also, as a byproduct, I proved Kaneko–Koike's conjecture on the positivity of Fourier coefficients of extremal forms in the case of depth 1.

The above proofs are hinted a lot from extensive experiments with SageMath. Especially, when I saw the plot of the quotient of two modular forms (Figure 1), it becomes clear that what I should try to prove (monotonicity and limit as $t \to 0^+$), where both out to be true (Proposition 5.1 and 5.2 of [36]).

Maass wave forms, Quantum modular forms, and Hecke operators

In [12], Cohen construct the first explicit example of maass wave form, based on one of the Ramanujan's q-series. Its coefficients are certain Hecke character of the real quadratic field $\mathbb{Q}(\sqrt{6})$, and Cohen conjectured that the Maass wave form is an eigenform for suitable Hecke operators. However, the usual Hecke operator is not the right candidate since the multiplier system (Nebentypus) of Cohn's Maass wave form does not come from Dirichlet characters. In my undergraduate and master's thesis, I propose the correct definition of Hecke operator that works for more general multiplier systems, including Cohn's Maass wave form, and prove that the Maass wave form is indeed eigenform under the operators [34, 35]. Also, one can associate *quantum modular forms* to the Maass wave form as a period integral (following [38, 52]), and I proved that this map is Hecke-equivariant. As a corollary, this gives a nontrivial identities on ceratin p-th root of unities and p-th coefficient of the Maass
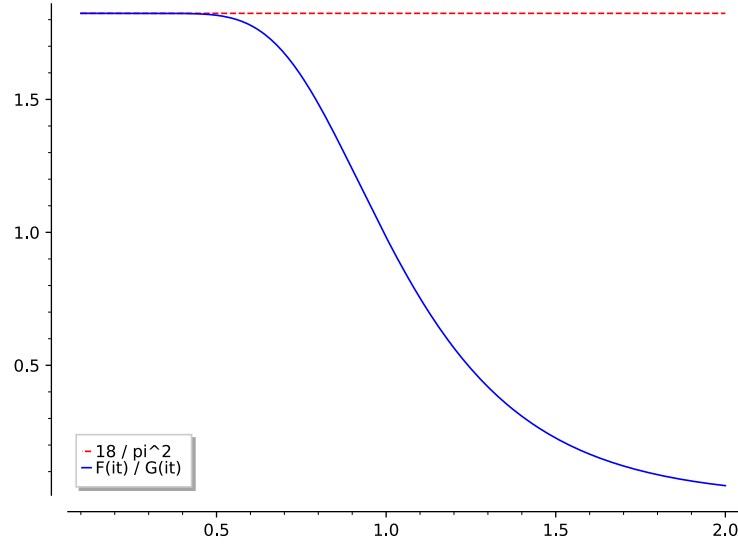
3

Figure 1: Graph of the quotient $F(it)/G(it)$ of two modular forms as a function in $t > 0$.

wave form for primes p. Same argument also worked for Li–Ngo–Rhoades' Maass wave form [39].

Other Projects

My interest is not restricted to number theory. I'm interested in various subjects, including

- formalization of mathematics,

- discrete geometry,

- homomorphic encryption.

Formalization of polynomial FLT and sphere packing in $\mathbb{R}^8$

Formal verification of mathematical proofs is a rapidly growing field, with the aim of ensuring the correctness of mathematical results. A lot of the mathematical objects and proofs are formalized, including the Hales' proof of Kepler's conjecture [25], Scheme [8], Perfectoid space [7], and Gowers–Green–Manners–Tao's proof of the polynomial Frieman–Rusza conjecture [24, 48].

There's also an ongoing project to formalize the proof of Fermat's Last theorem in Lean 4 [6], lead by Kevin Buzzard. Since the proof of Fermat's Last Theorem is very complicated and requires a lot of advanced mathematics that are not in Lean's `mathlib4` library [15], we expect that the complete formalization would take more than 10 years. However, the *polynomial* version of the Fermat's Last Theorem is much easier to prove, and in fact we

have a more general result called the Mason–Stothers theorem [47, 43], which is an analogue of ABC conjecture for polynomials.

With Jineon Baek, we give a complete formalization of the Mason–Stothers theorem in Lean 4 [3]. In fact, the theorem is already formalized in HOL by Eberl [18] and in Lean 3 by Wagemaker [51]. We gave extensive comparison between those previous formalizations and ours [3, Section 7], and we also in the process of integrating our formalization of the Mason–Stothers theorem to the `mathlib4` library. The code is available at

$$\text{https://github.com/seewoo5/lean-poly-abc}$$

Also, I'm working on a project formalizing the Viazovska's [50] proof of the optimal sphere packing in $\mathbb{R}^8$ in Lean 4, with several people including Sidharth Hariharan (project leader), Chris Birkbeck, Gareth Ma and Maryna Viazovska. This may includes the formalization of my algebraic proof of the modular form inequalities [36], which help us to completely avoid formalizing various numerical analysis and the Hardy–Ramanujan formula. Currently, we completed to formalize the E_8 lattice and its density, and now we are on the stage of formalzing Cohn–Elkies bound and the basic theory of (quasi)modular forms.

Conway–Soifer conjecture - homothetic case

Consider an equilateral triangle of side length $n + \varepsilon$ for an integer $n \geq 1$ and a sufficiently small $\varepsilon > 0$. What is the minimum number of unit equilateral triangles needed to cover the whole triangle? It is easy to see that at least $n^2 + 1$ triangles are required, by considering area. Conway and Soifer give two different ways to cover the large triangle with $n^2 + 2$ unit triangles [16], and conjectured that this is the minimum number of triangles required.

With Jineon Baek, we proved that the conjecture is true *if we restrict our attention to homothetic triangles*, i.e. assuming all the sides of the unit equilateral triangles are parallel to the large triangle ($\triangle$ or $\triangledown$) [2]. In fact, we proved the following general statement.

Theorem (Baek–L.). *Call a triangle a horizontal triangle of base b and height h, if it has a side of length b parallel to the x-axis, and the height h measured in the direction of y-axis. Then $n^2 + 1$ horizontal triangles of base b and height h cannot cover a horizontal triangle of base nb and height $> nh$.*

The proof is elementary, and we also determined the largest possible ε such that an equilateral triangle of side length $n + \varepsilon$ can be covered by $n^2 + 2$ or $n^2 + 3$ homothetic unit equilateral triangles ($\varepsilon = 1/(n+1)$ and $\varepsilon = 1/n$, respectively). We expect that our method can be generalized to higher dimensions, or to find the largest side length of an equilateral triangle that can be covered by $n^2 + k$ homothetic unit equilateral triangles for $1 \leq k \leq 2n$.

Encrypted transfer learning with homomorphic encryption

While I was working at CryptoLab as a Research Engineer during my alternative military service, I developed privacy-preserving machine learning library called `HEaaN.SDK` [1] based

on Cheon–Kim–Kim–Song (CKKS) homomorphic encryption (HE) scheme [9]. In theory, one can compute arbitrary arithmetic circuit over encrypted real and complex numbers (with small errors) using CKKS scheme, and one might think implementing machine learning algorithms with HE is not hard. However, encrypted computations over ciphertexts are much slower than over plaintexts, and naive implementations could be highly impractical. Hence we need to re-design the algorithm in *HE-friendly* way, which is usually a nontrivial research problem. In particular, I found that there were no HE-based training algorithms for *multiclass* classification tasks at the moment, and most of the previous works are only applicable for binary classifications with small number of features.

To implement such an HE-based multiclass classification algorithm, we need 1) efficient encrypted softmax computation with large input, and 2) efficient large encrypted matrix multiplication. Both problems were resolved in HETAL (efficient **H**omomorphic **E**ncryption based **Tra**nsfer **L**earning) [37]. For the softmax computation, we found that homomorphic comparison [10] can be used to normalize inputs (subtract maximum value), then homomorphic domain extension [11] let us to cover wider range of inputs with much smaller errors, compared to the previous works [30, 33, 27]. To perform efficient encrypted matrix multiplications, we implement two types of multiplications $AB^\intercal$ and $A^\intercal B$ separately, which allow us to avoid transpose operation. Tiling and complex packing techniques are used to reduce the number of rotations required substantially, which result matrix multiplication algorithms that are 1.8 to 323 times faster than the previous algorithms [17, 30]. As a result, we were able to fine-tune commonly used vision and language models within an hour with a single A40 GPU on five benchmark datasets, which shows HE-based encrypted fine-tuning is indeed practical.

References

[1] HEaaN.SDK. `https://www.heaan.it/docs/stat/python/`.

[2] Jineon Baek and Seewoo Lee. $n^2 + 1$ unit equilateral triangles cannot cover an equilateral triangle of side $> n$ if all triangles have parallel sides. *to appear in American Mathematical Monthly.*

[3] Jineon Baek and Seewoo Lee. Formalizing Mason-Stothers Theorem and its Corollaries in Lean 4. *arXiv preprint arXiv:2408.15180*, 2024.

[4] David Ben-Zvi, YIANNIS Sakellaridis, and AKSHAY Venkatesh. Relative langlands duality. *Preprint available at https://www. math. ias. edu/akshay/research/BZSVpaperV1. pdf*, 2023.

[5] Jean Bourgain, Laurent Clozel, and Jean-Pierre Kahane. Principe d'heisenberg et fonctions positives. In *Annales de l'institut Fourier*, volume 60, pages 1215–1232, 2010.

[6] Kevin Buzzard. Formalization of Fermat's Last theorem. `https://github.com/ImperialCollegeLondon/FLT`. Accessed: 2024-10-02.

[7] Kevin Buzzard, Johan Commelin, and Patrick Massot. Formalising perfectoid spaces. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, pages 299–312, 2020.

[8] Kevin Buzzard, Chris Hughes, Kenny Lau, Amelia Livingston, Ramon Fernández Mir, and Scott Morrison. Schemes in lean. *Experimental Mathematics*, 31(2):355–363, 2022.

[9] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23*, pages 409–437. Springer, 2017.

[10] Jung Hee Cheon, Dongwoo Kim, and Duhyeong Kim. Efficient homomorphic comparison methods with optimal complexity. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*, pages 221–256. Springer, 2020.

[11] Jung Hee Cheon, Wootae Kim, and Jai Hyun Park. Efficient homomorphic evaluation on large intervals. *IEEE Transactions on Information Forensics and Security*, 17:2553–2568, 2022.

[12] Henri Cohen. q-identities for maass waveforms. *Inventiones mathematicae*, 91(3):409–422, 1988.

[13] Henry Cohn and Noam Elkies. New upper bounds on sphere packings i. *Annals of mathematics*, pages 689–714, 2003.

[14] Henry Cohn, Abhinav Kumar, Stephen Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017.

[15] Lean Community. mathlib4. `https://github.com/leanprover-community/mathlib4`. Accessed: 2024-10-02.

[16] JH Conway and Alexander Soifer. Covering a triangle with triangles, 2005.

[17] Eric Crockett. A low-depth homomorphic circuit for logistic regression model training. *Cryptology ePrint Archive*, 2020.

[18] Manuel Eberl. The mason–stothers theorem. *Archive of Formal Proofs*, December 2017. `https://isa-afp.org/entries/Mason_Stothers.html`, Formal proof development.

[19] Melissa Emory. On the global Gan–Gross–Prasad conjecture for general spin groups. *Pacific Journal of Mathematics*, 306(1):115–151, 2020.

[20] Ahram S Feigenbaum, Peter J Grabner, and Douglas P Hardin. Eigenfunctions of the fourier transform with specified zeros. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 171, pages 329–367. Cambridge University Press, 2021.

[21] Masaaki Furusawa and Kazuki Morimoto. Refined global gross–prasad conjecture on special bessel periods and böcherer's conjecture. *Journal of the European Mathematical Society*, 23(4):1295–1331, 2020.

[22] Wee Teck Gan, Benedict H Gross, and Dipendra Prasad. Symplectic local root numbers, central critical L-values, and restriction problems in the representation theory of classical groups. *Astérisque*, pages No–pp, 2011.

[23] David Ginzburg and Stephen Rallis. The exterior cube l-function for gl (6). *Compositio Mathematica*, 123(3):243–272, 2000.

[24] WT Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of marton. *arXiv preprint arXiv:2311.05762*, 2023.

[25] Thomas Hales, Mark Adams, Gertrud Bauer, Tat Dat Dang, John Harrison, Hoang Le Truong, Cezary Kaliszyk, Victor Magron, Sean McLaughlin, Tat Thang Nguyen, et al. A formal proof of the kepler conjecture. In *Forum of mathematics, Pi*, volume 5, page e2. Cambridge University Press, 2017.

[26] Thomas C Hales. A proof of the kepler conjecture. *Annals of mathematics*, pages 1065–1185, 2005.

[27] Seungwan Hong, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe, and Jung Hee Cheon. Secure tumor classification by shallow neural network using homomorphic encryption. *BMC genomics*, 23(1):284, 2022.

[28] Atsushi Ichino and Tamutsu Ikeda. On the periods of automorphic forms on special orthogonal groups and the gross–prasad conjecture. *Geometric and Functional Analysis*, 19:1378–1425, 2010.

[29] The MathWorks Inc. MATLAB, 2022.

[30] Chao Jin, Mohamed Ragab, and Khin Mi Mi Aung. Secure transfer learning for machine fault diagnosis under different operating conditions. In *International Conference on Provable Security*, pages 278–297. Springer, 2020.

[31] Masanobu Kaneko and Masao Koike. On extremal quasimodular forms. *Kyushu Journal of Mathematics*, 60(2):457–470, 2006.

[32] Erez Lapid and Zhengyu Mao. A conjecture on Whittaker–Fourier coefficients of cusp forms. *Journal of Number Theory*, 146:448–505, 2015.

[33] Joon-Woo Lee, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee, Junghyun Lee, Donghoon Yoo, Young-Sik Kim, et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *iEEE Access*, 10:30039–30054, 2022.

[34] Seewoo Lee. Quantum modular forms and hecke operators. *Research in Number Theory*, 4(2):18, 2018.

[35] Seewoo Lee. Maass wave forms, quantum modular forms and hecke operators. *Research in the Mathematical Sciences*, 6(1):7, 2019.

[36] Seewoo Lee. Algebraic proof of modular form inequalities for optimal sphere packings. *arXiv preprint arXiv:2406.14659*, 2024.

[37] Seewoo Lee, Garam Lee, Jung Woo Kim, Junbum Shin, and Mun-Kyu Lee. HETAL: Efficient privacy-preserving transfer learning with homomorphic encryption. In *International Conference on Machine Learning*, pages 19010–19035. PMLR, 2023.

[38] John Lewis and Don Zagier. Period functions for maass wave forms. i. *Annals of Mathematics*, 153(1):191–258, 2001.

[39] Yingkun Li, Hieu T Ngo, and Robert C Rhoades. Renormalization and quantum modular forms, part i: Maass wave forms. *arXiv preprint arXiv:1311.3043*, 2013.

[40] Yifeng Liu. Refined global gan–gross–prasad conjecture for bessel periods. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2016(717):133–194, 2016.

[41] Zhengyu Mao and Stephen Rallis. A trace formula for dual pairs. *Duke Mathematical Journal*, 87(2):321–341, 1997.

[42] Zhengyu Mao, Chen Wan, and Lei Zhang. BZSV Duality for Some Strongly Tempered Spherical Varieties. *arXiv preprint arXiv:2310.17837*, 2023.

[43] R. C. Mason. *Diophantine equations over function fields*, volume 96 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1984.

[44] Dan Romik. On Viazovska's modular form inequalities. *Proceedings of the National Academy of Sciences*, 120(43):e2304891120, 2023.

[45] Yiannis Sakellaridis. Spherical varieties and integral representations of l-functions. *Algebra & Number Theory*, 6(4):611–667, 2012.

[46] Yiannis Sakellaridis and Akshay Venkatesh. Periods and harmonic analysis on spherical varieties. *Asterisque*, 2017(396):1–370, 2017.

[47] W. W. Stothers. Polynomial identities and Hauptmoduln. *Quart. J. Math. Oxford Ser. (2)*, 32(127):349–370, 1981.

[48] Terence Tao. The Polynomial Freiman-Ruzsa Conjecture. `https://teorth.github.io/pfr/`. Accessed: 2024-10-02.

[49] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8)*, 2023. `https://www.sagemath.org`.

[50] Maryna Viazovska. The sphere packing problem in dimension 8. *Annals of mathematics*, pages 991–1015, 2017.

[51] Jens Wagemaker. A formally verified proof of the mason-stothers theorem in lean, 2018. `https://matryoshka-project.github.io/pubs/wagemaker_bsc_thesis.pdf`.

[52] Don Zagier. Quantum modular forms. *Quanta of maths*, 11:659–675, 2010.