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*. Specifically, for an "algebraic" automorphic representation π of a group $G(\mathbb{A}_{\mathbb{Q}})$, it is conjectured that there exists an associated Galois representation $\rho_\pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \check{G}(k)$, where k can be $\mathbb{C}$ or $\overline{\mathbb{Q}_\ell}$, such that the automorphic L-function $L(s, \pi)$ coincides with the Artin L-function $L(s, \rho_\pi)$. Here, $\check{G}$ denotes the Langlands dual group of G. The case where $G = \mathrm{GL}_1$ is well understood through class field theory, and for $G = \mathrm{GL}_2$, the conjecture is proven when π is associated with holomorphic modular forms, culminating in the celebrated modularity theorem by Wiles, Taylor, and others, which played a key role in the proof of Fermat's Last Theorem.

Recently, there has been growing interest in the *relative* Langlands program, which seeks to extend the classical Langlands program to spherical varieties [44, 45]. A major goal of this program is to systematically address the many instances of identities between automorphic periods and special values of L-functions (Ichino–Ikeda type formula [27]), as seen in the works of Hecke, Iwasawa–Tate, Rankin–Selberg, Godement–Jacquet, Ichino–Ikeda, and Lapid–Mao. Moreover, Ben-Zvi, Sakellaridis, and Venkatesh have put forward a conjectural *duality* within the relative Langlands program [4]. This duality suggests that for a Hamiltonian G-space $G \curvearrowright M$, one should expect a corresponding dual pair $\check{G} \curvearrowright \check{M}$, where a *dual identity* between automorphic periods and special values of L-functions arises by exchanging the roles of (G, M) and $(\check{G}, \check{M})$.

Mao–Rallis trace formula for dual pairs

I am working on a conjectural identity relating automorphic periods and L-values for the dual pairs introduced by Mao and Rallis [40]. For simple, split, and simply-laced groups G', excluding type A_n, Mao and Rallis construct a dual pair (SL_2, G) within G' by utilizing Heisenberg groups associated with G'. This includes cases such as $(\mathrm{SL}_2, \mathrm{SL}_6)$ within E_6. They proposed conjectural relative trace formulae for these dual pairs, suggesting that period integrals of automorphic forms on G (resp. SL_2) should correspond to special L-values associated with automorphic representations of SL_2 (resp. G). In their work, they established the fundamental lemma for unit elements in the Hecke algebras of both G and SL_2.

Recently, Mao, Wan, and Zhang [41] formulated a refined version of this conjecture, in the form of an Ichino–Ikeda type formula, within the framework of the relative Langlands program [4]. They also proved smooth transfer for local functions at non-Archimedean places. In collaboration with Yuchan Lee, we are working to complete the comparison of the relative trace formula for the case $(\mathrm{SL}_2, \mathrm{SL}_6)$, focusing on proving the fundamental lemma for the full Hecke algebras, establishing smooth transfer at Archimedean places, and analyzing the spectral decomposition of the relative traces. Together with the result of Lapid–Mao [31] on Whittaker–Fourier coefficients, this would confirm one direction of the non-refined conjecture: if Π is a cuspidal automorphic representation of SL_2 and π is its functorial lift to G via the L-group morphism $\mathrm{PGL}_2 \to {}^L G$, then the Mao–Rallis automorphic period is nonzero if the adjoint L-value $L(1, \Pi, \mathrm{Ad})$ is nonzero. Additionally, we aim to prove the refined formula by establishing local relative character identities and combining them with the refined identity of Lapid–Mao for SL_2. It is worth noting that this refined formula is "dual" to the conjectural formula for the Ginzburg–Rallis periods and the exterior cube L-values of PGL_6 [22].

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

Building upon the groundwork laid by Liu [39] on the special orthogonal groups ($\mathrm{SO}_2 \times \mathrm{SO}_5$ and $\mathrm{SO}_3 \times \mathrm{SO}_6$) and drawing insights from Emory's work [19] on *general spin groups* ($\mathrm{GSpin}_n \times \mathrm{GSpin}_{n+1}$ 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 $\mathrm{SO}_2 \times \mathrm{SO}_{2n+1}$ 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 $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$) are usually easy to compute explicitly with help of computer algebra systems like SageMath [48] or MATLAB [28].

Modular forms and optimal sphere packings

The *optimal sphere packing problem* seeks the densest arrangement of unit balls in d-dimensional space $\mathbb{R}^d$. While the problem is trivial for $d = 1$, the two-dimensional case was solved by Thue in 1890. The three-dimensional case, known as Kepler's conjecture, was settled by Thomas Hales in 2005 using extensive computer calculations [25], with the formal verification completed nearly a decade later through the use of proof assistants HOL Light and Isabelle [24].

An unexpected link between the 8- and 24-dimensional sphere packing problems and number theory emerged through the work of Cohn and Elkies, who introduced the *linear programming bound* [13]. This approach hinted that finding specific "magic functions" could unlock optimal sphere packings in these dimensions. However, constructing such functions, which must satisfy constraints on both the function and its Fourier transform, is challenging due to the uncertainty principle. Maryna Viazovska made a breakthrough by using modular forms to construct the magic function for dimension 8 [49], and similar methods soon resolved the case for dimension 24 [14].

To prove these two cases, the authors [49, 14] relied on numerical approximations and extensive computer assisted computations to establish desired inequalities between modular forms, and it is natural to ask if there is a more general and conceptual proof for these inequalities. While a more direct proof exists for the dimension 8 case by Dan Romik [43], I have found *algebraic* proofs for both the 8- and 24-dimensional cases that avoid reliance on numerical approximations [35]. In my work, I developed a theory of *positive* and *completely positive* quasimodular forms, which I used to study the *magic modular forms* appearing in the optimal sphere packing problem. Additionally, I discovered connections to Kaneko and Koike's *extremal quasimodular forms* [30], which are conjectured to have non-negative Fourier coefficients. A key aspect of my approach involves leveraging the differential equations satisfied by these modular forms. My work opens new possibilities for generalizing Viazovska's construction to dimensions beyond 8 and 24, based on Fourier eigenfunctions constructed by Feigenbaum, Grabner, and Hardin [20]. In particular, this could lead to a new upper bound for the uncertainty principle in specific dimensions [5]. Furthermore, as a byproduct of my research, I proved Kaneko and Koike's conjecture regarding the positivity of Fourier coefficients for extremal forms in the case of depth 1 [30].

These proofs were inspired by extensive experiments using SageMath. Notably, after observing the plot of the quotient of two modular forms (Figure 1), I realized the key properties to prove - monotonicity and the limit as $t \to 0^+$ - both of which turned out to hold true (Propositions 5.1 and 5.2 of [35]).

Maass wave forms, Quantum modular forms, and Hecke operators

In [12], Cohen constructed the first explicit example of a Maass wave form, based on one of Ramanujan's q-series. The coefficients of this form are related to a Hecke character of the real quadratic field $\mathbb{Q}(\sqrt{6})$, and Cohen conjectured that this Maass wave form is an eigenform for suitable Hecke operators. However, the usual Hecke operators are not appropriate in this case, as the multiplier system (Nebentypus) of Cohen's Maass wave form does not arise from Dirichlet characters.

In my undergraduate and master's thesis, I proposed a correct definition of Hecke operators that applies to more general multiplier systems, including Cohen's Maass wave form. I further proved that this Maass wave form is indeed an eigenform under these operators [33, 34]. Additionally, one can associate *quantum modular forms* to the Maass wave form via period integrals, following the work of Lewis and Zagier [37, 51], and I demonstrated that this map is Hecke-equivariant. As a result, this leads to nontrivial identities between certain

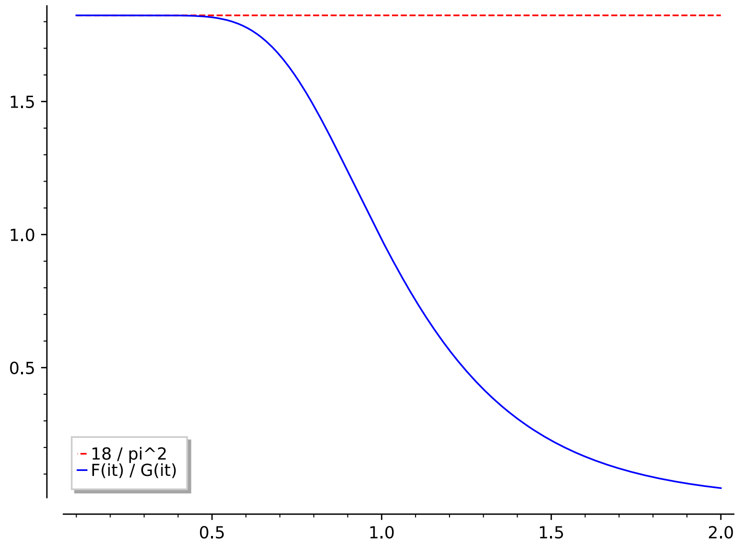

Figure 1: Graph of the quotient $F(it)/G(it)$ of two modular forms as a function in $t > 0$.

p-th roots of unity and the p-th coefficients of the Maass wave form for primes p. The same argument applies to the Maass wave form of Li, Ngo, and Rhoades [38].

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 $\mathbb{R}^8$

The formal verification of mathematical proofs is a rapidly growing field aimed at ensuring the correctness of mathematical results. A number of significant mathematical objects and proofs have been formalized, including Hales' proof of Kepler's conjecture [24], schemes [8], perfectoid spaces [7], and Gowers, Green, Manners, and Tao's proof of the polynomial Freiman–Ruzsa conjecture [23, 47].

One notable ongoing project is the formalization of the proof of Fermat's Last Theorem in Lean 4, led by Kevin Buzzard [6]. Given the complexity of the proof and the advanced mathematics required, many of which are not yet in Lean's `mathlib4` library [15], it is estimated that the complete formalization could take over 10 years. In contrast, the *polynomial* version of Fermat's Last Theorem is much simpler to prove, and a more general result, known as the Mason–Stothers theorem, provides an analogue of the ABC conjecture for polynomials [46, 42].

In collaboration with Jineon Baek, we give a complete formalization of the Mason–Stothers theorem in Lean 4 [3]. While the theorem has previously been formalized in HOL by Eberl [18] and in Lean 3 by Wagemaker [50], our work provides a detailed comparison with these prior formalizations [3, Section 7]. We are also in the process of integrating our formalization into the `mathlib4` library, with the code available at:

https://github.com/seewoo5/lean-poly-abc

Additionally, I am working on a project to formalize Viazovska's proof of the optimal sphere packing in $\mathbb{R}^8$ [49] in Lean 4, alongside a team led by Sidharth Hariharan, which includes Chris Birkbeck, Gareth Ma, and Maryna Viazovska. This effort may also involve formalizing my algebraic proof of the modular form inequalities [35], which would allow us to bypass the need for formalizing various aspects of numerical analysis and the Hardy–Ramanujan formula. So far, we have completed the formalization of the E_8 lattice and its density, and are now working on formalizing the Cohn–Elkies bound and the foundational theory of (quasi)modular forms.

Conway–Soifer conjecture - homothetic case

Consider an equilateral triangle with side length $n+\varepsilon$, where $n \geq 1$ is an integer and $\varepsilon > 0$ is sufficiently small. What is the minimum number of unit equilateral triangles required to cover this larger triangle? By considering the area, it is straightforward to show that at least n^2+1 unit triangles are necessary. Conway and Soifer provided two different ways to cover the large triangle using n^2+2 unit triangles [16] and conjectured that this is the minimum number needed.

In collaboration with Jineon Baek, we proved that this conjecture holds if we restrict the covering to *homothetic* triangles, i.e., when the sides of the unit triangles are parallel to those of the large triangle (aligned either as $\triangle$ or $\bigtriangledown$) [2]. Specifically, we established the following general result:

Theorem (Baek–L.). *A triangle is called a horizontal triangle of base b and height h if one of its sides of length b is parallel to the x-axis, and its height h is measured along the y-axis. Then n^2+1 horizontal triangles of base b and height h cannot cover a horizontal triangle of base nb and height greater than nh.*

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

Encrypted transfer learning with homomorphic encryption

During my alternative military service as a Research Engineer at CryptoLab, I developed a privacy-preserving machine learning library called `HEaaN.SDK` [1], based on the Cheon–Kim–Kim–Song (CKKS) homomorphic encryption (HE) scheme [9]. The CKKS scheme theoretically allows arbitrary arithmetic computations on encrypted real and complex numbers (with small errors), which might lead one to believe that implementing machine learning algorithms using HE is straightforward. However, encrypted computations are significantly slower than plaintext computations, and naive implementations can be highly impractical due to performance bottlenecks. To address this, algorithms need to be redesigned in an *HE-friendly* way, which is often a complex research problem.

One key challenge I encountered was the lack of HE-based algorithms for *multiclass* classification tasks; most prior work focused on binary classifications with a limited number of features. Implementing a multiclass classification algorithm using HE required overcoming two major obstacles: (1) efficiently performing encrypted softmax computations with large inputs and (2) executing large-scale encrypted matrix multiplications.

These challenges were addressed in HETAL (**H**omomorphic **E**ncryption-based **T**ransfer **L**earning) [36]. For softmax computation, we used homomorphic comparison techniques [10] to normalize inputs by subtracting the maximum value, followed by homomorphic domain extension [11], which significantly reduced errors and expanded the input range compared to previous approaches [29, 32, 26]. To optimize matrix multiplications, we implemented two distinct multiplication methods: $AB^\intercal$ and $A^\intercal B$ which allowed us to bypass the costly transpose operation. We further employed tiling and complex packing techniques to minimize the number of required rotations, resulting in matrix multiplication algorithms that were 1.8 to 323 times faster than previous methods [17, 29]. As a result, we successfully fine-tuned commonly used vision and language models within an hour on five benchmark datasets, using a single A40 GPU. This demonstrated that HE-based encrypted fine-tuning is not only feasible but also practical for real-world applications.

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

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

[24] 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.

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

[26] 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.

[27] 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.

[28] The MathWorks Inc. MATLAB, 2022.

[29] 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.

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

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

[32] 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.

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

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

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

[36] 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.

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

[38] 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.

[39] 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.

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

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

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

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

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

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

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

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

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

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

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

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