Research Statement

Seewoo Lee seewoo5@berkeley.edu

Last updated: August 31, 2025

My research focuses on number theory, where I solve problems in number theory using various computational tools including computer algebra systems (SageMath, MAGMA), proof assistants (Lean), and Machine Learning.

1 Number Theory with computer algebra systems

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.

1.1 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 [20], with the formal verification completed nearly a decade later through the use of proof assistants HOL Light and Isabelle [19].

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 [38], and similar methods soon resolved the case for dimension 24 [14].

To prove these two cases, the authors [38, 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 [34], I have found *algebraic* proofs for both the 8- and 24-dimensional cases that avoid reliance on numerical approximations [28]. 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* [24], 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 [18]. 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 [24], and currently working on the case of higher levels defined by Sakai and Tsutsumi [35]. I'm also working on improving *lower* bounds for the uncertainty principle, by constructing a new class of summation formulae from other types of automorphic forms, possibly generalizing the work of Cohn and Triantafillou [15].

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 $t \longrightarrow 0^+$ - both of which turned out to hold true (Propositions 5.1 and 5.2 of [28]).

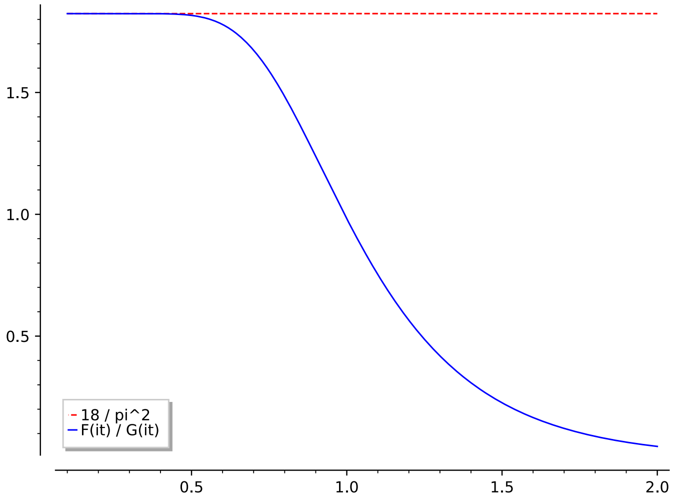

Figure 1: Graph of the quotient $F(it)/G(it)$ of two modular forms as a function in $t > 0$ for 8-dimensional sphere packing.

1.2 Function field arithmetic

During the summer of 2025, I mentored four students at the Berkeley mathematics REU in a project on function field arithmetic, specifically focusing on the function field analogue of Diophantine equations involving Fibonacci polynomials and prime races. The first two works below are joint with Bates, Jesubalan, Lu, and Shim, and all the results are motivated by SageMath experiments.

Diophantine equations involving Fibonacci numbers have been studied extensively, with many interesting results. For example, Bugeaud, Mignotte, and Siksek [6] used modular approach and linear forms to prove that the only perfect powers in the Fibonacci sequence are 0, 1, 8, and 144. In [4], we studied the function field analogue of these Diophantine equations, particularly focusing on the *Fibonacci polynomials* defined as $F_n(T) = TF_{n-1}(T) + F_{n-2}(T)$ with $F_0(T) = 0$ and $F_1(T) = 1$. For each $j > 1$, we give a complete characterization of the perfect j-th powers in the sequence of Fibonacci polynomials over finite fields. One noticeable difference from the classical case is that there are infinitely many perfect j-powers among Fibonacci polynomials for each j and a coefficient field $\mathbb{F}_q$.

The second project of our REU team is about *ties* in function field prime races [3]. For a given monic polynomial $m \in \mathbb{F}_q[T]$, "prime race" in function field considers the number of irreducible monic polynomials (primes) of degree N congruent to $a \in \mathbb{F}_q[T]$ modulo m, which we denote as $\pi(a, m, N)$. In [8], Cha studied limiting distributions of the error functions, and proved that primes are biased towards non-quadratic residues under certain hypothesis on Dirichlet L-functions whe q is odd. In our project, we instead focus on the cases when $\pi(a, m, N) = \pi(b, m, N)$ for distinct congruence classes $a, b \in (\mathbb{F}_q[T]/m)^{\times}$. We found that there are infinitely many triples (m, a, b) where $\pi(a, m, N) = \pi(b, m, N)$ holds for infinitely many N. We suggest two ways to prove such ties: (1) by writing an explicit formula for each $\pi(a, m, N)$ using L-functions and exploiting unexpected conjugate pairs of elements in cyclotomic fields, and (2) by constructing an explicit bijection using $\mathrm{GL}_2(\mathbb{F}_q)$-action. For example, we prove that $\pi(1, m, N) = \pi(T, m, N)$ holds for $m = T^3+T+1 \in \mathbb{F}_2[T]$ for all $N \equiv 1 \pmod 7$.

As an aside, I studied a function field analogue of Shanks bias. In [36], Shanks studied higher-order effects of Chebyshev's bias and proposed several conjectures based on numerical experiments. In particular, he conjectured that there are more positive integers n such that $\lambda(n)\chi_{-4}(n) = +1$ than those with $\lambda(n)\chi_{-4}(n) = -1$, where λ is the Liouville function and χ_{-4} is the nontrivial quadratic character modulo 4. Computing the logarithmic density of such n's is also proposed as the 22nd problem in the Comparative Prime Number Theory Problem List [21]. In [29], I studied the function field analogue of this problem, comparing the number of monic polynomials $f \in \mathbb{F}_q[T]$ satisfying $\lambda(f)\chi(f) = 1$ or $\lambda(f)\chi(f) = -1$, where $\chi = \chi_m$ is a quadratic Dirichlet character modulo m. Specifically, assuming Grand Simplicity Hypothesis for the Dirichlet L-function, I proved that $\lambda \cdot \chi$ is biased towards $+1$, where the bias can be made arbitrarily small by taking m to have large enough degree. The proof is based on the Kronecker–Weyl equidistribution theorem and elementary trigonometric series computations.

1.3 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 [26, 27]. Additionally, one can associate *quantum modular forms* to the Maass wave form via period integrals, following the work of Lewis and Zagier [31, 40], and I demonstrated that this map is Hecke-equivariant. As a result, this leads to nontrivial identities between certain 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 [32].

2 Number theory with Lean

The formal verification of mathematical proofs is a rapidly growing field aimed at ensuring the correctness of mathematical results. I worked on several formalization projects using Lean, including

- Formalization of the Viazovska's proof of the optimal sphere packing in $\mathbb{R}^8$
- Formalization of the Mason–Stothers theorem and polynomial Fermat's Last Theorem
- Google DeepMind's *Formal Conjectures* project.

2.1 Formalization of 8-dimensional optimal sphere packing

I am working on a project to formalize Viazovska's proof of the optimal sphere packing in $\mathbb{R}^8$ [38] in Lean 4, alongside a team led by Sidharth Hariharan, which includes Chris Birkbeck, Gareth Ma, Bhavik Mehta, and Maryna Viazovska. This also involves formalizing my algebraic proof of the modular form inequalities introduced in Section 1.1, which would allow us to bypass the need for formalizing various aspects of numerical analysis and the Hardy–Ramanujan formula. We also found several mathematical tricks to reduce the identities for the Serre derivatives of level 2 modular forms to the case of level 1, which allow us to avoid formalization of the dimension formula for the higher levels, which requires formalizing valence 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. The project is open to public and available at:

https://github.com/thefundamentaltheor3m/Sphere-Packing-Lean

2.2 Formalization of polynomial FLT

One notable ongoing project in Lean community is the formalization of the (modern) proof of Fermat's Last Theorem, led by Kevin Buzzard [7]. Given the complexity of the proof and the advanced mathematics required, many of which are not yet in Lean's mathlib4 library, 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 [37, 33].

In collaboration with Jineon Baek, we give a complete formalization of the Mason–Stothers theorem in Lean 4 [2]. While the theorem has previously been formalized in HOL by Eberl [17] and in Lean 3 by Wagemaker [39], our work provides a detailed comparison with these prior formalizations [2, Section 7]. Now the whole proofs are fully integrated into the mathlib4 library (see PR #15706 and PR #18882), where the previous codes are available at:

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

2.3 Formal Conjectures project

Google DeepMind's *Formal Conjectures* project aims to formalize statements of mathematical conjectures and theorems (without proofs) in Lean 4. I contributed to the project by formalizing several conjectures and theorems in number theory, including Ramanujan–Petersson conjecture, Lehmer's conjecture, Hall's conjecture, congruent number problem, and some of the Erdös problems (#9, #307, #364).

3 Number theory with Machine Learning

3.1 Machine Learning Galois Groups

Recently, there has been a growing interest in applying machine learning techniques to number theory. One of the most notable example is the recent finding of *murmuration* pattern of elliptic curves [23] by He, Lee, Oliver, and Pozdnyakov, where the authors used machine learning to predict ranks of elliptic curves and found a surprising murmuration pattern of traces of Frobenius of certain families of elliptic curves while analyzing the models. Another example is the work of He, Lee, and Oliver [22] on classifying various invariants of number fields from Dedekind zeta coefficients and polynomial coefficients, where they found the classical machine learning algorithms such as logistic regression and random forest perform very well in classifying Galois groups of number fields.

In a joint work with Kyu-Hwan Lee, we give an answer for *why* machine learning models perform very well in classifying Galois groups of Galois number fields, by reverse engineering the

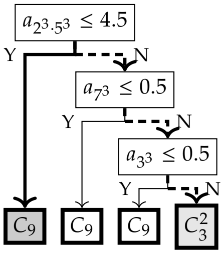

Figure 2: A decision tree predicts the Galois groups of nonic fields from zeta coefficients up to $a_{1000}(K)$.

classification logic of the models [25]. In particular, we studied the classification logic of decision tree models where the zeta coefficients are used as features, and we found that the models only use a small number of the coefficients whose indices are mostly certain powers. For example, Figure 2 shows the decision tree predicting the Galois groups of nonic Galois extensions (which obtained 100% accuracy on a test set) from zeta coefficients up to $a_{1000}(K)$, where the model only uses three coefficients: a_{1000}, a_{343}, and a_{27}, which are all cubic indices. Inspired from this, we conjectured and proved the following theorem, which has not been showed up in the literature before.

Theorem (Lee–L.)**.** Let ℓ be a prime and $K/\mathbb{Q}$ be a Galois extension of degree ℓ^2, hence $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_{\ell^2}$ or C_ℓ^2. Then $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_{\ell^2}$ if and only if there exists a prime p such that $a_{p^\ell}(K) = 0$.

We also studied degree $4, 6, 8, 9, 10$ number fields and established similar results. Our work demonstrates how machine learning can be used as a tool for generating conjectures and aiding in the discovery of rigorous mathematical theorems.

4 Other Projects

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

- discrete geometry
- homomorphic encryption

4.1 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 $\triangledown$) [1]. 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 $1 \leq k \leq 2n$.

4.2 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`, 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) [30]. 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. 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. 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] Jineon Baek and Seewoo Lee. An Equilateral Triangle of Side n Cannot be Covered by $n^2 + 1$ Unit Equilateral Triangles Homothetic to it. *The American Mathematical Monthly*, 132(2):113–121, 2024.

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

[3] Graeme Bates, Ryan Jesubalan, Seewoo Lee, Jane Lu, and Hyewon Shim. On Ties in Function Field Prime Races. *in preparation*.

[4] Graeme Bates, Ryan Jesubalan, Seewoo Lee, Jane Lu, and Hyewon Shim. Powerful Fibonacci Polynomials over Finite Fields. *in preparation*.

[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] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. *Annals of mathematics*, pages 969–1018, 2006.

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

[8] Byungchul Cha. Chebyshev's bias in function fields. *Compositio Mathematica*, 144(6):1351–1374, 2008.

[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] Henry Cohn and Nicholas Triantafillou. Dual linear programming bounds for sphere packing via modular forms. *Mathematics of Computation*, 91(333):491–508, 2022.

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

[17] Manuel Eberl. The Mason–Stothers Theorem. *Archive of Formal Proofs*, December 2017. https://isa-afp.org/entries/Mason_Stothers.html, Formal proof development.

[18] 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.

[19] 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.

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

[21] Alia Hamieh, Habiba Kadiri, Greg Martin, and Nathan Ng. Comparative Prime Number Theory Problem List. *arXiv preprint arXiv:2407.03530*, 2024.

[22] Yang-Hui He, Kyu-Hwan Lee, and Thomas Oliver. Machine-learning number fields. *arXiv preprint arXiv:2011.08958*, 2020.

[23] Yang-Hui He, Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov. Murmurations of elliptic curves. *Experimental Mathematics*, pages 1–13, 2024.

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

[25] Kyu-Hwan Lee and Seewoo Lee. Machines Learn Number Fields, But How? The Case of Galois Groups. *arXiv preprint arXiv:2508.06670*, 2025.

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

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

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

[29] Seewoo Lee. Shanks bias in function fields. *in preparation*, 2025.

[30] 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.

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

[32] 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.

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

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

[35] Yuichi Sakai and Hiroyuki Tsutsumi. Extremal quasimodular forms for low-level congruence subgroups. *Journal of Number Theory*, 132(9):1896–1909, 2012.

[36] Daniel Shanks. Quadratic residues and the distribution of primes. *Mathematics of Computation*, 13(68):272–284, 1959.

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

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

[39] Jens Wagemaker. A Formally Verified Proof of the Mason-Stothers Theorem in Lean, 2018. `https://matryoshka-project.github.io/pubs/wagemaker_bsc_thesis.pdf`.

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