Research Statement

Seewoo Lee seewoo5@berkeley.edu

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

Modular forms and optimal sphere packings The *optimal sphere packing problem* asks the densest arrangement of unit balls in $\mathbb{R}^d$. The problem is solved in dimensions $d = 1, 2, 3, 8$ and 24, where the last two cases are recently resolved by Maryna Viazovska and her collaborators. Their method constructs so-called *magic functions* for the Cohn–Elkies linear programming bound, using (quasi)modular forms.

One of the main steps of the proofs is the verification of certain inequalities involving (quasi)modular forms, corresponds to the linear constraints of the magic functions. The original arguments relied on numerical approximations and extensive computer assisted computations, and it is natural to ask if there is a more general and conceptual proof for these inequalities. A more direct proof is recently given by Dan Romik for the dimension 8 case.

In [8], I have found *algebraic* proofs for both the 8- and 24-dimensional cases that avoid reliance on numerical approximations, by developing a simple yet effective theory of *positive* and *completely positive* quasimodular forms. Additionally, I uncovered connections to Kaneko and Koike's *extremal quasimodular forms*, which are the quasimodular forms with largest possible orders at cusp of given weight and depth. They are conjectured to have non-negative Fourier coefficients, where I proved the conjecture for the case of depth 1 in *loc. cit*. A key ingredient in my approach is the use of modular differential equations satisfied by these 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. In particular, this lead to new upper bounds for the sign uncertainty principle à la Bourgain–Clozel–Kahane in certain dimensions.

Theorem (L., In progress)**.** The optimal constant $\mathrm{A}_+(d)$ for the $(+1)$-sign uncertainty principle of Bourgain–Clozel–Kahane satisfies $\mathrm{A}_+(d) \le \sqrt{2\left\lfloor \frac{d}{16} \right\rfloor + 2}$ when $d \equiv 0 \pmod 4$ and $d \le 14000$.

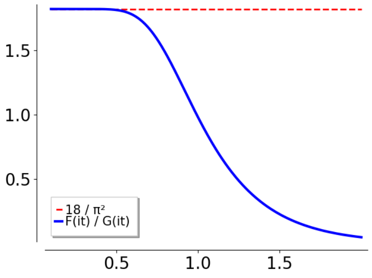

Figure 1: Plot of $F(it)/G(it)$.

These proofs were inspired by experiments using SageMath. For instance, the plot of a quotient of modular forms (Figure 1) suggested key properties - monotonicity and the limiting behavior as $t \to 0^+$ - to prove the inequality $F(it) < \frac{18}{\pi^2} G(it)$ for dimension 8. Likewise, the quasimodular identities in [8] can be verified both computationally and by hand.

Currently, I am extending this theory to higher-level quasimodular forms, aiming to prove analogous conjectures for extremal forms of level ≥ 2, as studied by Sakai and Tsutsumi, as well as to give algebraic proofs of other modular form inequalities that appear in the proof of the universal optimality of the E_8 and Leech lattice. I am also working on improving *lower* bounds for the uncertainty principle, by constructing new summation formulae from other types of automorphic forms, potentially generalizing the work of Cohn and Triantafillou on dual LP bounds.

Function field arithmetic In the summer of 2025, I mentored four students at the Berkeley Mathematics REU on projects in the arithmetic of function fields. We explored analogues of classical Diophantine problems and prime number races. For example, we completely characterized all perfect powers in the sequence of Fibonacci polynomials over finite fields, showing that infinitely many occur - in sharp contrast to the classical integer case, where only finitely many exist [3]. We also discovered infinite families of *ties* in function field prime races, proving that for certain moduli m and residue classes a, b, the counts $\pi(a, m, N)$ and $\pi(b, m, N)$ of monic irreducible polynomials of degree N are equal for infinitely many N. These results were established both via explicit formulas involving L-functions and by constructing bijections using $\mathrm{GL}_2(\mathbb{F}_q)$-actions.

Separately, I studied a function field analogue of Shanks' higher order Chebyshev's bias [9]. Shanks conjectured biases in the sign of $\lambda(n)\chi_{-4}(n)$, where λ is the Liouville function and χ_{-4} is the quadratic character mod 4. I studied the analogous problem for polynomials over $\mathbb{F}_q$, comparing the number of monic polynomials f satisfying $\lambda(f)\chi(f) = 1$ or $\lambda(f)\chi(f) = -1$, where $\chi = \chi_m$ is a quadratic Dirichlet character modulo square-free polynomial m. Especially, I proved the following theorem:

Theorem (L. [9])**.** Let $A^{\lambda}_{\pm}(n; m)$ be the number of non-constant monic polynomials $f \in \mathbb{F}_q[T]$ of degree at most n with $\lambda(f)\chi_m(f) = \pm 1$. Assume that Grand Simplicity Hypothesis holds for the Dirichlet L-function $L(s, \chi_m)$. Then we have

$$\lim_{n\to\infty} \frac{\#\{1 \le k \le n : A^{\lambda}_{+}(k; m) > A^{\lambda}_{-}(k; m)\}}{n} > \frac{1}{2}$$

where a closed formula for the density is obtained. When $q \equiv 1 \pmod{4}$, the density can be made arbitrarily close to $\frac{1}{2}$ by choosing m appropriately with large enough degree.

This answers a function field analogue of the 22nd problem in the *Comparative Prime Number Theory Problem List* by Hamieh et al. I am also working on other problems including the average degree of least degree k-th power nonresidue modulo irreducible primes and the average number of divisors of polynomials over function fields, questions whose integer analogues are either classical or still open.

Maass wave forms, Quantum modular forms, and Hecke operators In 1988, Henri 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 [6, 7]. Additionally, one can associate *quantum modular forms* to the Maass wave form via period integrals, following the work of Lewis and Zagier, 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.

2 Number Theory with Proof Assistant (Lean)

Formalization of 8-dimensional optimal sphere packing I am one of the maintainers of the project to formalize Viazovska's proof of the optimal sphere packing in $\mathbb{R}^8$ in Lean 4, led by Sidharth Hariharan and including Chris Birkbeck, Bhavik Mehta, and Maryna Viazovska. This also involves formalizing my algebraic proof of the modular form inequalities introduced above, which allow us to bypass the need for formalizing interval arithmetic 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, thereby circumventing the need to formalize the dimension formula at higher levels, which relies on the 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 and related inequalities. The project is publicly available at Sphere-Packing-Lean.

Formalization of polynomial FLT In collaboration with Jineon Baek, we give a complete formalization of the Mason–Stothers theorem in Lean 4 [2], which implies Fermat's Last Theorem for polynomials. While earlier formalizations existed in HOL (Eberl) and Lean 3 (Wagemaker), our work provides a complete Lean 4 proof and a careful comparison with previous approaches [2, Section 7]. The entire proof is now integrated into the `mathlib` library.

Formal Conjectures project I also occasionally contribute to Google DeepMind's Formal Conjectures project, which aims to formalize the statements of mathematical conjectures and theorems (without proofs) in Lean 4. My contributions include conjectures in number theory such as the Ramanujan–Petersson conjecture, Lehmer's conjecture, Hall's conjecture, congruent number problem, and several of Erdös problems (#9, #307, #364, #946).

3 Number Theory with Machine Learning

Machine Learning Galois Groups Recent work by Yang-Hui He, Kyu-Hwan Lee, and Thomas Oliver applied machine learning to study invariants of number fields, including Galois groups. While simple algorithms achieved high prediction accuracy, the underlying classification mechanisms were not well understood.

In a joint work with Kyu-Hwan Lee, we addressed this gap by reverse-engineering the decision logic of ML models used to classify Galois groups of Galois number fields [5]. In particular, we studied the classification logic of decision trees where the Dedekind zeta coefficients are used as features, and we found that the models only use a small number of the coefficients, typically at indices that are perfect 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. This empirical observation inspired the following theorem, previously absent from the literature:

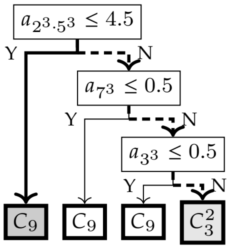

Figure 2: Decision tree classifying Galois group of nonic Galois extensions.

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, obtaining analogous results and showing that parts of the learned classification logic are, in fact, *provably correct*. Our work demonstrates how machine learning can be used as a tool for generating conjectures and aiding in the discovery of rigorous mathematical theorems. My future goal is to scale-up the research and to discover more new results, possibly discover more efficient algorithms to compute various invariants of number fields or other number theoretic objects (such as automorphic forms and abelian varieties), inspired from machine learning.

4 Additional Projects - Automorphic Representations and Discrete Geometry

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

- Automorphic representations and Poisson summation formula
- Discrete geometry

Modulation groups and Poisson summation formula In a joint work with Jayce R. Getz, Armando Gutiérrez Terradillos, Farid Hosseinijafari, Bryan Hu, Aaron Slipper, Marie-Hélène Tomé, HaoYun Yao, and Alan Zhao, we defined and studied *modulation groups* [4]. They can be viewed as generalizations of metaplectic groups acting on suitable Schwartz spaces of spherical varieties. More precisely, for an affine algebraic group H over a local field F, a "nice" affine H-scheme X, an H-representation V, and a H-equivariant map $\omega : X \longrightarrow V$, the *modulation group* $\Psi_\omega(F)$ is defined as a subgroup of the automorphism group of the Schwartz space $\mathcal{S}(X(F))$, generated by the action of $V^\vee(F)$, $H(F)$, and *Fourier transforms*. We compute this group in several cases and show that it consists of the F-points of an algebraic group or a metaplectic group. In particular, we compute the group when ω is the identity map or the symmetric square map on $\mathbb{G}_a^n$, or when $\omega : X \hookrightarrow \mathbb{G}_a^{2n}$ is a quadratic cone.

One can also globalize the definition to obtain an adelic version of the modulation group, and we prove that the Poisson summation formula holds if and only if a theta series associated with ω gives an "automorphic representation of $\Psi_\omega(\mathbb{A}_F)$," although the precise definition of this notion is not yet settled. This suggests that modulation groups will play an important role in the Braverman–Kazhdan program, whose goal is to study automorphic L-functions and Langlands functoriality via the Poisson summation formula.

This work was initiated through the 2024 Duke Research Scholars program and supported by the Duke Number Theory RTG grant.

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 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. [1])**.** 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 $1 \le k \le 2n$.

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. Powerful fibonacci polynomials over finite fields. *arXiv preprint arXiv:2601.02664*, 2026.

[4] Jayce R. Getz, Armando Gutiérrez Terradillos, Farid Hosseinijafari, Bryan Hu, Seewoo Lee, Aaron Slipper, Marie-Hélène Tomé, Haoyun Yao, and Alan Zhao. Modulation groups. *arXiv preprint arXiv:2510.23932*, 2025.

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

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

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

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

[9] Seewoo Lee. Shanks bias in function fields. *arXiv preprint arXiv:2509.16142*, 2025.