

RESEARCH STATEMENT

George J. Schaeffer

After the completion of my PhD, I plan to improve and expand the *Hecke stability method* (HSM), a technique developed in my dissertation for the analysis and computation of weight 1 modular forms. Because the details of this method touch on several areas of number theory and because its core idea may be applicable to similar computational problems, I anticipate a highly productive postdoctoral research program.

Modular forms have found utility both in number theory (e.g. the proof of Fermat’s last theorem [Wil95]) and other areas of mathematics (e.g. the explicit construction of families of expander graphs [Sar90] [CGL07]). One of the major achievements of modern algebraic number theory is the following correspondence between Galois representations and modular forms:

$$\left\{ \begin{array}{l} \text{certain cuspidal modular forms} \\ \text{over } \overline{\mathbb{F}}_p \text{ of weight } k \text{ and level } N \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Galois representations } \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p) \\ \text{of “Serre type,” unramified outside } Np \end{array} \right\}$$

established by the work of many researchers and codified in the theorems of Eichler–Shimura [Shi71], Deligne [Del68], Deligne–Serre [DS74] (\rightarrow), and Khare–Wintenberger [KW09] (\leftarrow).

I originally designed the HSM with a view towards studying the above correspondence in the weight 1 case ($k = 1$), which is exceptional for the following reasons:

- There may exist *ethereal forms*, cuspidal modular forms of weight 1 over $\overline{\mathbb{F}}_p$ (elements of the left-hand side above) which do not “lift” to classical cusp forms of weight 1 over \mathbb{C} [Edi06].
- The projective versions of the Galois representations (elements of the right-hand side above) in this case are **unramified at p** [CV92] [Wie11], and the representations arising from ethereal forms may have “large image” [Edi06] [Kha07]. Ethereal forms might therefore be applied to construction of number fields which are exceptional in the sense of [Rob08].
- The methods typically used to compute cusp forms in weights $k > 1$ (e.g. modular symbols [Ste07]) do not extend directly to $k = 1$.

The main application of the HSM is the computation of spaces of weight 1 cusp forms. Section 1 explains the general principles behind the method and relates the correctness of the HSM to two topics of broader interest in number theory: isogeny graphs and zeros of Eisenstein series.

In Section 2, I explain how the HSM has allowed for a number of surprising discoveries concerning ethereal forms (see above). Previously, few examples of such forms were known [Kha07], but it now appears that ethereal forms are common even at relatively small levels N . The phenomenon of ethereality can be related to the size of the torsion subgroup of $H^1(X_1(N), \omega(-D))$ where ω^2 is the canonical line bundle on the modular curve $X_1(N)$ and D is the reduced cuspidal divisor. Because of the correspondence between ethereal forms and Galois representations, estimates for the growth of this group as $N \rightarrow \infty$ would have deep consequences for the statistics of algebraic number fields.

The basic idea behind the HSM is general enough that it ought to be possible to extend this method to related problems in number theory. In Section 3, I discuss how the HSM might be adapted to the computation of *Siegel modular forms*. In this particular setting, I am motivated by the open question of whether or not there exist “ethereal” Siegel modular forms [Ghi09].

Note: The proofs of Theorems 1, 2, 3, and 5 below will appear in my dissertation [Sch12].

Brief overview of notation and terminology

Let $N > 4$ and let R be a $\mathbb{Z}[1/N]$ -algebra. There is an affine curve $Y_1(N)$ whose R -points parametrize isomorphism classes of pairs (E, P) where E/R is an elliptic curve and $P \in E(R)$ is a point of order N . The *modular curve* $X_1(N)$ completes $Y_1(N)$ by adding finitely many points called *cusps*.

A *modular form* (in the sense of Katz [Kat72]) of weight k and level N over R is an element of $H^0(X_1(N)_R, \underline{\omega}_R^{\otimes k})$, where $\underline{\omega}$ is a square root of the canonical line bundle on $X_1(N)$. A *cuspidal form* is a modular form which vanishes on the divisor D consisting of the cusps. The space of all modular forms (resp. cuspidal forms) of weight k and level N over R is denoted $M_k(N; R)$ (resp. $S_k(N; R)$).

A modular form $f \in M_k(N; R)$ has *character* $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ if for every pair (E, P) representing a point of $Y_1(N)$ and every d relatively prime to N we have $f(E, dP) = \chi(d)f(E, P)$. The space of all modular forms (resp. cuspidal forms) with character χ is denoted $M_k(N, \chi; R)$ (resp. $S_k(N, \chi; R)$). When R is (for example) an algebraically closed field, we have decompositions $M_k(N; R) = \bigoplus_\chi M_k(N, \chi; R)$ and $M_k(N, \chi; R) = E_k(N, \chi; R) \oplus S_k(N, \chi; R)$ where $E_k(N, \chi; R)$ is the space of *Eisenstein series*. The spaces $E_k(N, \chi; R)$ and $S_k(N, \chi; R)$ are invariant under the action of the *Hecke operators*, certain distinguished elements of $\text{End}_R M_k(N; R)$. There is a Hecke operator T_ℓ for each prime $\ell \nmid N$; the value of $(T_\ell f)(E, P)$ averages f over the $\ell + 1$ pairs (E', P') which are ℓ -isogenous to (E, P) .

There is a map $f \mapsto f(q) : M_k(N; R) \rightarrow R[[q]]$ called *q-expansion*; it will always be injective in what follows. *q-expansion* is analogous to Fourier expansion of modular forms over \mathbb{C} (with $q = e^{2\pi iz}$). To compute a space of modular forms over R is to compute its image in $R[[q]]$ to sufficient precision. The action of T_ℓ on *q-expansions* from $M_k(N, \chi; R)$ can be made explicit.

1. The Hecke stability method and computing weight 1 cusp forms

1.1 The HSM over \mathbb{C} . Weight 1 cusp forms are mysterious even in the classical setting over \mathbb{C} . For example, there is no known general formula for the dimension of $S_1(N; \mathbb{C})$ though such formulas are available in higher weights (see [Ste05], pg. 75).

The Hecke stability method provides us with an algorithm for computing $S_1(N; \mathbb{C})$. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ be an odd Dirichlet character and assume for simplicity that there is $\lambda_\chi \in E_1(N, \chi^{-1}; \mathbb{C})$ which is nonzero at every cusp. We compute a basis for $S_2(N, \mathbf{1}; \mathbb{C})$ (using modular symbols algorithms included in SAGE, for example) and let

$$V(N, \chi; \mathbb{C}) = \{ g/\lambda_\chi : g \in S_2(N, \mathbf{1}; \mathbb{C}) \}.$$

We have $S_1(N, \chi; \mathbb{C}) \subset V(N, \chi; \mathbb{C}) \subset S_1^*(N, \chi; \mathbb{C})$ where $S_1^*(N, \chi; \mathbb{C})$ is a space of objects which have the same modularity properties as elements of $S_1(N, \chi; \mathbb{C})$ but which may have poles away from the cusps. $S_1^*(N, \chi; \mathbb{C})$ inherits the action of the Hecke operators but its subspace $V(N, \chi; \mathbb{C})$ is **not** invariant under this action. We choose a prime $\ell \nmid N$ and consider the inclusion

$$S_1(N, \chi; \mathbb{C}) \subset V(N, \chi; \mathbb{C})^{(T_\ell)} = \{ f \in V(N, \chi; \mathbb{C}) : \forall r \ T_\ell^r f \in V(N, \chi; \mathbb{C}) \}.$$

Note that the space on the right can be computed in finitely many steps (in terms of *q-expansions*).

Theorem 1. For any $\ell \nmid N$ the above inclusion is an equality, so the HSM computes $S_1(N, \chi; \mathbb{C})$.

The proof exploits two facts:

- (1) By construction, elements of $V(N, \chi; \mathbb{C})$ may only have poles where the Eisenstein series λ_χ has zeros; this is a finite subset of $X_1(N)_\mathbb{C}$ which does not include any cusps.
- (2) The Hecke operator T_ℓ is the adjacency operator for the directed graph $G_\ell(N; \mathbb{C})$ whose vertices are points of $Y_1(N)_\mathbb{C}$ and whose edges are ℓ -isogenies between them. Every connected component of this graph is infinite and contains at most one cycle.

These facts allow us to show that if some $f \in V(N, \chi; \mathbb{C})$ has a pole, then there is an r such that $T_\ell^r f$ has a pole outside the zero set of λ_χ , so $T_\ell^r f \notin V(N, \chi; \mathbb{C})$ and $f \notin V(N, \chi; \mathbb{C})^{(T_\ell)}$.

1.2 The HSM over $\bar{\mathbb{F}}_p$. It is possible to replace \mathbb{C} in the above discussion everywhere with $\bar{\mathbb{F}}_p$ (for p outside some finite set of bad primes, including those which divide N). However, in contrast to the characteristic zero case, $G_\ell(N; \bar{\mathbb{F}}_p)$ has a **finite** component whose vertices are the supersingular points of $X_1(N)_{\bar{\mathbb{F}}_p}$. This means that $S_1(N, \chi; \bar{\mathbb{F}}_p) \subset V(N, \chi; \bar{\mathbb{F}}_p)^{(T_\ell)}$ (with $\ell \nmid Np$) can be a **proper** inclusion when λ_χ has supersingular zeros.

Project. Characterize those cases where $S_1(N, \chi; \bar{\mathbb{F}}_p) \subsetneq V(N, \chi; \bar{\mathbb{F}}_p)^{(T_\ell)}$.

Though I have found a few examples where the inclusion is proper, there are ways to determine the truth of the desired equality $S_1(N, \chi; \bar{\mathbb{F}}_p) = V(N, \chi; \bar{\mathbb{F}}_p)^{(T_\ell)}$ once a basis for $V^{(T_\ell)}$ has been computed. For example, if $f \in V(N, \chi; \bar{\mathbb{F}}_p)$, then for any positive integer k ,

$$f \in S_1(N, \chi; \bar{\mathbb{F}}_p) \iff f^k \in S_k(N, \chi^k, \bar{\mathbb{F}}_p).$$

Because the condition on the right is nonlinear, such a criterion is truly only useful for certification.

The desired equality is known to hold in a number of special cases, and in general we have:

Theorem 2. *The equality $S_1(N, \chi; \bar{\mathbb{F}}_p) = V(N, \chi; \bar{\mathbb{F}}_p)^{(T_\ell)}$ holds provided that (a.) λ_χ has few supersingular zeros, or (b.) $p \geq B(\chi, \ell)$ where $B(\chi, \ell)$ depends on the conductor of χ and on ℓ .*

The Lang–Trotter conjecture for elliptic curves (Conjecture 4.8 in [Sil09]) would imply that condition (a.) in Theorem 2 holds “most of the time,” assuming that most of the zeros of λ_χ on $X_1(N)_\mathbb{C}$ do not lie over curves with complex multiplication.

Condition (b.) can be made effective using a very handy lemma of Goren and Lauter on quaternion arithmetic (Lemma 2.1.1 in [GL04]); the explicit bounds I have obtained in this way are fairly complicated and certainly not sharp.

Project. Improve the explicit bound of condition (b.) in Theorem 2 by studying the zeros of the Eisenstein series λ_χ and the structure of isogeny graphs.

Eisenstein series and isogeny graphs are both topics of broader interest, and I look forward to collaborating with other number theorists on these investigations. I have made some progress on locating the zeros of various λ_χ using the moduli interpretation of Eisenstein series provided in [Khu09]. Isogeny graphs are used in computational number theory to compute endomorphism rings of elliptic curves [Koh96] [Bis11a] and modular polynomials [BLS10]; they also have found applications in cryptography [CGL07] [Bis11b] [JD11].

2. Ethereal forms and their associated Galois representations

2.1 Ethereal characteristics and cohomology. Another reason weight 1 cusp forms are challenging from a computational perspective is that there may be primes p (not dividing N) such that $\dim S_1(N; \overline{\mathbb{F}}_p) > \dim S_1(N; \mathbb{C})$. Such p are the *ethereal characteristics* of level N . Elements of $S_1(N; \overline{\mathbb{F}}_p)$ which do not lift (in a suitable sense) to elements of $S_1(N; \mathbb{C})$ are *ethereal forms*.

Theorem 3. *There is an algorithm which, on input N , outputs a finite list L of rational primes containing all the ethereal characteristics of level N .*

The proof combines ideas of K. Buzzard and the correctness of the HSM over \mathbb{C} (Theorem 1).

By cohomology and base change, p is an ethereal characteristic for level N if and only if the group $H^1(X_1(N), \underline{\omega}(-D))$ has nontrivial p -torsion [Kat72] [Kha07].

Project. Adapt the HSM to compute the full torsion subgroup of $H^1(X_1(N), \underline{\omega}(-D))$.

In [Kha07], Khare asks whether the ethereal characteristics of level N can be bounded in terms of the Faltings height of the modular curve $X_1(N)$. My work suggests that this may be difficult: The ethereal characteristics grow quickly in N , even when we consider the contribution from a single character χ . For example, consider the following table:

N	$7 \cdot 29$	$7 \cdot 71$	$7 \cdot 139$	$7 \cdot 241$	$7 \cdot 251$
p	5	23 89	3577593541	1357729 1422097 5194030189	2939535258278478698811649

Here, the p are ethereal characteristics in level N contributed by ethereal forms with character χ being that induced by the mod 7 quadratic character. This means for example, that the torsion subgroup of $H^1(X_1(973), \underline{\omega}(-D))$ has order divisible by 3577593541. These and other data computed using the HSM support an ambitious conjecture of the following form:

Conjecture 4. *The limit $\lim_{N \rightarrow \infty} \frac{\log |H^1(X_1(N), \underline{\omega}(-D))_{\text{tors}}|}{[\text{SL}_2(\mathbb{Z}) : \Gamma_1(N)]}$ exists and is positive.*

(Where $[\text{SL}_2(\mathbb{Z}) : \Gamma_1(N)]$ is roughly on the order of N^2 .)

Though this conjecture currently seems intractable, and likely requires additional hypotheses, I plan to continue devising ways to attack it after completing my PhD. Bergeron and Venkatesh have made similar conjectures concerning the torsion homology of hyperbolic 3-manifolds [BV10].

2.2 Galois representations. *Newforms* $f \in S_k(N; \overline{\mathbb{F}}_p)$ correspond to irreducible 2-dimensional mod p Galois representations ρ_f with some prescribed properties. When $k = 1$, the corresponding projective representation $\tilde{\rho}_f : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \rightarrow \text{PGL}_2(\overline{\mathbb{F}}_p)$ is **unramified** at p [CV92] [Wie11].

Question (F. Calegari). *If f is an ethereal newform in characteristic p^2 is $\tilde{\rho}_f$ ramified at p ?*

If f is **not** ethereal, then it follows from a theorem of Deligne and Serre [DS74] that the image of $\tilde{\rho}_f$ embeds in $\text{PGL}_2(\mathbb{C})$, which has few finite subgroups. Heuristics suggest that projective representations $\tilde{\rho}_f$ coming from nonethereal f are typically dihedral [BG09]. Wiese has shown that when p is odd, the converse is true: dihedral mod p newforms lift to forms (of the same level N) in characteristic zero [Wie04].

The image of $\tilde{\rho}_f$ is not limited in this way when the newform f is ethereal. In this case we typically expect that the image is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ for some prime power p^r . For example, in the table above, we see that 5 is an ethereal characteristic for level $203 = 7 \cdot 29$. The Galois representation attached to the newform here cuts out the splitting field of $x^5 - 29x^2 + 58x - 29$, a quintic with discriminant $-7 \cdot 29^4$ and Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$. For specific newforms, one can verify quickly if $\tilde{\rho}_f$ has “large image” using a criterion of Serre [Ser72].

Project. Prove an effective “large image theorem” for ethereal forms. Reconcile the consequences of such a theorem and versions of Conjecture 4 with the nonabelian Cohen–Lenstra heuristics of Bhargava et al [Bha10] [VE10].

2.3 Even-dimensionality. There is a twisting action on the set of newforms in $S_1(N, \chi; \overline{\mathbb{F}}_p)$, and the fixed points of this action are exactly the dihedral forms. In light of [Wie04],

Theorem 5. *The subspace of $S_1(N, \chi; \overline{\mathbb{F}}_p)$ generated by ethereal newforms is even-dimensional.*

It is possible that Theorem 5 has some deeper meaning. For example, it might indicate the presence of an alternating pairing on $H^1(X_1(N), \omega(-D))$. Venkatesh has also suggested to me that this phenomenon may have a connection to spin structures, objects which are more commonly associated with mathematical physics.

3. Extending the Hecke stability method

3.1 Siegel modular forms. *Siegel modular forms* generalize modular forms to moduli spaces of abelian varieties of genus g with level structure [And09]—these specialize to the modular forms of before in the case $g = 1$. In brief, we work over the *Siegel modular variety* $\mathcal{A}_g(N)$, the moduli space of principally polarized abelian varieties of dimension g with level N structure; this is a scheme over any $\mathbb{Z}[1/N]$ -algebra R . The *scalar-valued Siegel modular forms* of weight k and level N are global sections of (some line bundle) $\underline{\omega}^{\otimes k}$ on $\mathcal{A}_g(N)$. We will denote this space by $M_k^g(N; R)$. Scalar-valued Siegel modular forms can be further generalized to *vector-valued Siegel modular forms*.

As before, we have reduction maps $M_k^g(N; \mathbb{Z}[1/N]) \rightarrow M_k^g(N; \mathbb{F}_p)$ ($p \nmid N$) which are surjective so long as $H^1(\mathcal{A}_g(N), \underline{\omega}^{\otimes k})[p]$ vanishes. Unsurprisingly, our knowledge here is much more limited than in the elliptic ($g = 1$) setting. Ghitza has shown [Ghi09] that the reduction is surjective when $k \geq g + 2$, but there are no known examples where $H^1(\mathcal{A}_g(N), \underline{\omega}^{\otimes k})[p]$ is nontrivial.

In my postdoctoral research I plan to adapt the Hecke stability method to the study of Siegel modular forms. This should be possible in principle, since analogs of the necessary players—Hecke operators and Eisenstein series—are present. The computational equipment for Siegel modular forms in genera $g > 1$ is less developed, and on the theoretical side, isogeny graphs on $\mathcal{A}_g(N)$ may exhibit more complicated structure when $g > 1$ [Rob11]. Despite these challenges, I am confident that the HSM can find utility in this setting. Such a program would be further motivated by the correspondence between mod p Siegel modular forms of genus 2 and representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GSp}_4(\overline{\mathbb{F}}_p)$ [Sor10].

Project. Adapt the HSM to compute $H^1(\mathcal{A}_g(N), \underline{\omega}^{\otimes k})$ and find examples of ethereal Siegel modular forms with $g > 1$. If these exist, study their associated mod p representations.

3.2 Other extensions. In addition to Siegel modular forms, there are many other contexts which generalize elliptic modular forms. The Hecke stability method might be adapted in many of these settings as well: modular forms of half-integral weight, overconvergent p -adic modular forms, and Hilbert modular forms.

Question (B. Mazur). Do ethereal forms arise from specializations to weight 1 of Hida families of p -adic modular forms?

References

- [And09] A. Andrianov. *Introduction to Siegel Modular Forms and Dirichlet Series*. Springer–Verlag, 2009.
- [BV10] N. Bergeron, A. Venkatesh. “The asymptotic growth of torsion homology for arithmetic groups.” Preprint, 2010.
- [Bha10] M. Bhargava. “The density of discriminants of quintic rings and fields.” *Ann. Math.*, **172** (2010) 1559–1591.
- [BG09] M. Bhargava, E. Ghate. “On the average number of octahedral forms of prime level” *Mathematische Ann.*, **344** (2009) 749–768.
- [Bis11a] G. Bisson. “Computing endomorphism rings of elliptic curves under the GRH.” *J. of Math. Crypto.*, (2011).
- [Bis11b] G. Bisson. *Endomorphism Rings in Cryptography*. PhD Thesis, Eindhoven University of Technology, 2011.
- [BLS10] R. Bröker, K. Lauter, A. V. Sutherland. “Modular polynomials via isogeny volcanoes.” arXiv 1001.0402, 2010.
- [BS11] G. Bisson, A. V. Sutherland. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field.” *J. Number Th.*, **131** (2011) 815–831.
- [CV11] F. Calegari, A. Venkatesh. *Towards a Torsion Jacquet–Langlands correspondence*. In preparation.
- [CGL07] D. X. Charles, E. Z. Goren, K. E. Lauter. “Cryptographic hash functions from expander graphs.” Technical report, Microsoft R., 2007.
- [CV92] R. Coleman, J.-F. Voloch. “Companion forms and Kodaira–Spencer theory.” *Inv. Math.*, **110** (1992) 263–28.
- [Del68] P. Deligne. “Formes modulaires et représentations ℓ -adiques.” *Sem. Bourbaki*, **355** (1968–69). *Lecture Notes in Math.*, **179** (1971) 136–172.
- [DS74] P. Deligne, J.-P. Serre. “Formes modulaires de poids 1.” *Annales scientifiques de l’É. N. S., 4^e série*, **7** (1974) 507–530.
- [Edi06] B. Edixhoven. “Comparison on integral structures of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. With appendices by Jean-François Mestre and Gabor Wiese.” *J. Inst. Math. Jussieu*, **5** (2006) 1–34.
- [Ghi09] A. Ghitza. “Some aspects of Siegel modular forms (mod p).” Talk, Universität Siegen, 2009.
- [GL04] E. Z. Goren, K. E. Lauter. “Class invariants for quartic CM fields.” Technical report, Microsoft R., 2004.
- [JD11] D. Jao, L. De Feo. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.” 2011.

- [Kat72] N. M. Katz. *p-adic Properties of Modular Schemes and Modular Forms*. International Summer School on Modular Forms. Antwerp, 1972.
- [Kha07] C. Khare. “Modularity of Galois representations and motives with good reduction properties.” *J. Ramanujan Math. Soc.*, **22** (2007) 1–26.
- [KW09] C. Khare, J.-P. Wintenberger. “Serre’s modularity conjecture.” *Inv. Math.*, **178** (2009) 485–586.
- [Khu09] K. Khuri-Makdisi. *Moduli interpretation of Eisenstein series*. Preprint, 2009.
- [Koh96] D. Kohel. *Endomorphism Rings of Elliptic Curves over Finite Fields*. PhD Thesis, University of California, Berkeley, 1996.
- [MV02] P. Michel, A. Venkatesh. “On the dimension of the space of cusp forms associated to 2-dimensional complex Galois representations.” *Int. Math. Res. Not.*, **38** (2002) 2021–2027.
- [Rob11] D. Robert. “Abelian varieties, theta functions and cryptography.” Talk, Luminy 2011.
- [Rob08] D. Roberts. “Chebyshev covers and exceptional number fields.” Preprint, 2008.
- [Sar90] P. Sarnak. *Some applications of modular forms*. Cambridge U. Press (1990).
- [Sch12] G. J. Schaeffer. *The Hecke Stability Method and Ethereal Forms*. PhD Thesis, in preparation, University of California, Berkeley, 2012.
- [Ser72] J.-P. Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques.” *Invent. Math.*, **15** (1972) 259–331.
- [Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publ. of Math. Soc. of Japan, **11** (1971).
- [Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer–Verlag, 2009.
- [Sor10] C. M. Sorensen. “Galois representations attached to Hilbert–Siegel modular forms.” *Doc. Math.*, **15** (2010) 623–670.
- [Ste05] W. Stein. “Computing with modular forms.” Course notes, Harvard University, 2004.
- [Ste07] W. Stein. *Modular Forms: A Computational Approach*. AMS Grad. Studies in Math., 2007.
- [VE10] A. Venkatesh, J. S. Ellenberg. “Statistics of number fields and function fields.” *Proceedings of the International Congress of Mathematicians*, Hyderabad, India, 2010.
- [Wie04] G. Wiese. “Dihedral Galois representations and Katz modular forms.” *Doc. Math.*, **9** (2004) 123–133.
- [Wie11] G. Wiese. “On Galois representations of weight one.” arXiv 1102.2302, 2011.
- [Wil95] A. Wiles. “Modular elliptic curves and Fermat’s last theorem.” *Ann. Math.*, **141** (1995) 443–551.