Modular Forms: Arithmetic and Computation

John Cremona (University of Warwick), Henri Darmon (McGill University),
Kenneth Ribet (University of California at Berkeley), Romyar Sharifi (McMaster University),
William Stein (University of Washington)

June 3-8, 2007

1 Overview of the Field

Modular forms are functions on the extension $\mathbf{H}^* = \mathbf{H} \cup \mathbf{Q} \cup \{\infty\}$ of the complex upper half-plane $\mathbf{H}$ that are holomorphic on $\mathbf{H}$, transform well under the action of a subgroup of $\mathrm{SL}_2(\mathbf{Z})$, and satisfy certain growth conditions at the cusps $\mathbf{Q} \cup \{\infty\}$. In particular, for some level $N \geq 1$ and weight $k \geq 2$, a modular form should satisfy

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathbf{H}^*$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N),$$

where $\Gamma_1(N)$ is the congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ consisting of matrices as above with $a-1$, c, and $d-1$ divisible by N. Modular forms play a central role in number theory, one far larger than that which the scope of any week-long workshop might hope to cover. Our workshop focused on algebraic aspects of their study, especially those amenable to computation.

A modular form f comes endowed with a q-expansion, which is essentially its Taylor series about ∞. One often writes f as its q-expansion:

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = e^{2\pi i z}$. We say that f is a cusp form if it vanishes at all cusps, which in particular implies that $a_0 = 0$. The modular curve $X_1(N)$ is a Riemann surface that arises as the quotient of $\mathbf{H}^*$ with respect to the action of $\Gamma_1(N)$, with a certain topology. Modular forms of level N and weight k may be also viewed as sections of the line bundle $\Omega^{k-2}_{X_1(N)/\mathbf{C}}$ of higher differentials on the modular curve $X_1(N)$. Certain commuting Hecke operators T_n with $n \geq 1$ act on the space of modular forms of a given weight and level, and one says that f is a (normalized) eigenform if $T_n f = a_n f$ for all such n. Together, these form a commutative algebra known as the Hecke algebra.

One can attach a number of objects to a cuspidal eigenform. For instance, one constructs an L-function attached to f, which is defined for $s \in \mathbf{C}$ with large enough real part by

$$L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

that satisfies a functional equation and has an analytic continuation to all of $\mathbf{C}$. To any modular eigenform, constructions of Shimura [32] and Deligne [13] attach a Galois representation

$$\rho_f \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{Q}_\ell})$$

for some prime ℓ that satisfies $\mathrm{Tr}\, \rho_f(\varphi_p) = a_p$ for any Frobenius φ_p at p for every prime p.

Modular forms are intricately connected with elliptic curves, genus one curves that can be described by equations of the form

$$y^2 = x^3 + Ax + B$$

with $4A^2 + 27B^2 \neq 0$. As with $\Gamma_1(N)$, we have a congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbf{Z})$ consisting of those matrices with lower left-hand entry divisible by N, and we obtain a closed modular curve $X_0(N)$ as the quotient $\Gamma_0(N)\backslash\mathbf{H}^*$. The modular curve $X_0(N)$ may be viewed as a moduli space of (generalized) elliptic curves over $\mathbf{C}$ together with a distinguished subgroup of order N. Conversely, we may define the algebraic curve $X_0(N)$ over any number field F as the moduli space space of elliptic curves defined over F (i.e., with $A, B \in F$) together with such a subgroup of its complex points.

We say that elliptic curve over $\mathbf{Q}$ is modular if it arises as the quotient of a modular curve $X_0(N)$ for some $N \geq 1$. That every elliptic curve over $\mathbf{Q}$ is modular is the famous conjecture of Shimura-Taniyama-Weil proven in most cases in the work of Wiles [37] and Taylor-Wiles [34] and completed in the work of Breuil-Conrad-Diamond-Taylor [4].

There are several equivalent formulations of modularity, two of which can be seen by considering objects attached to elliptic curves analogous to those of modular forms. First, an elliptic curve E defined over the rational numbers also gives rise to an L-function $L(E, s)$. It is determined by the number of points in its reductions modulo all prime numbers p. When this L-function is equal to the L-function of some normalized cuspidal eigenform of weight 2, the elliptic curve is modular. In particular, the modularity theorem yields an analytic continuation of $L(E, s)$ to the entire complex plane and a function equation, a special case of a conjecture of Artin's. Secondly, one has a Galois representation

$$\rho_E \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_\ell)$$

arising from the action of Galois on the first étale cohomology group of E over $\overline{\mathbf{Q}}$ with coefficients in $\mathbf{Z}_\ell$, or essentially equivalently, on the ℓ-adic torsion points of E over $\overline{\mathbf{Q}}$. That the elliptic curve E is modular says that ρ_E is conjugate in $\mathrm{GL}_2(\overline{\mathbf{Q}_\ell})$ to ρ_f for some weight 2 cuspidal eigenform f.

2 Recent Developments and Open Problems

Today, the central problem in the field is undoubtedly the Birch and Swinnerton-Dyer conjecture, commonly known as BSD. Given an elliptic curve E over $\mathbf{Q}$, it states that the rank r of the Mordell-Weil group $E(\mathbf{Q})$ of rational points of E is equal to the order of vanishing r_{an} of the L-function $L(E, s)$ at $s = 1$. Moreover, its strong form gives a precise description of the leading coefficient of its Taylor expansion about 1:

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E^+ \cdot |\mathrm{Sha}(E)| \cdot |R_\infty(E)| \cdot \prod_{p \text{ prime}} c_p}{|E(\mathbf{Q})_{\mathrm{tors}}|^2},$$

where $\mathrm{Sha}(E)$ denotes the Tate-Shafarevich group of E, where $R_\infty(E)$ is a certain regulator attached to E, where the c_p are Tamagawa numbers, where Ω_E^+ is a real period attached to E, and where $E(\mathbf{Q})_{\mathrm{tors}}$ denotes the torsion subgroup of the Mordell-Weil group. The finiteness of $\mathrm{Sha}(E)$ is in and of itself a conjecture of great interest and difficulty: moreover, if $\mathrm{Sha}(E)$ is finite then a result of Cassels tells us that its order is a square.

A proof of BSD appears to be still distant, but some important partial results are known, of which we mention an incomplete sampling. Gross and Zagier [16] gave a formula for $L'(E, 1)$ in terms of Heegner points (when $r_{\mathrm{an}} \geq 1$) which allowed them to prove that $r \geq 1$ whenever $r_{\mathrm{an}} = 1$. Heegner points on elliptic curves are the images of points in an imaginary quadratic field K in the upper half plane that lie in $E(L)$ for an abelian extension L of K. Later work of Kolyvagin [23] on Euler systems of Heegner points then yielded that $r = r_{\mathrm{an}}$ if $r_{\mathrm{an}} \leq 1$.

Euler systems have also played a major role in Iwasawa theory. In Iwasawa theory, one studies modules over an Iwasawa algebra Λ, which is usually to say the completed $\mathbf{Z}_p$-group ring of the Galois group of the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$. One such Iwasawa module is the Selmer group over $\mathbf{Q}_\infty$ of the representation ρ_f attached to a cuspidal eigenform f, which is constructed as a subgroup of a Galois cohomology group attached to the representation, with certain local conditions. This Selmer group is finitely generated as a Λ-module, and it therefore has a characteristic ideal which determines much of its structure. The main conjecture of Iwasawa theory for modular forms states that the characteristic ideal of Selmer group is given by a certain p-adic L-function $L_p(f, s)$ attached to f. This p-adic L-function is a function of the p-adic numbers that interpolates values of the classical L-function $L(f, s)$ at integers s, up to certain prescribed factors. This conjecture is closely related to a p-adic version of BSD [26]. In groundbreaking work, Kato [18] used an Euler system to prove that the characteristic ideal of the Selmer group divides the ideal attached to the p-adic L-function. Since that time, Skinner and Urban have announced a much-anticipated proof of most of the reverse divisibility that uses Galois representations for higher-dimensional automorphic forms.

Classically, elliptic curves with complex multiplication can be used to give an explicit version of class field theory over imaginary quadratic fields. Here, so-called elliptic units play the role that cyclotomic units play in explicit class field theory over $\mathbf{Q}$. In fact, Rubin [29] used this and Kolyvagin's Euler system to prove the main conjecture of elliptic curves with complex multiplication. It was Kronecker's "Jugendtraum" that a similarly explicit theory could be provided for general number fields, and in particular, for real quadratic fields. Gross and Stark had conjectured the existence of special units in abelian extensions of a real quadratic field K that would fill the role of the elliptic units. Darmon gave a conjectural description of these units using a certain multiplicative integral on $\mathbf{P}^1(\mathbf{Q}_p)$ [9]. The major remaining obstacle is that the elements are constructed locally and as of yet only conjecturally arise as global units.

Second only to BSD as an open problem concerning modular forms was Serre's conjecture [30]. It has been proven in very recent work of Khare-Wintenberger [19, 20], together with a result of Kisin [21]. The representation ρ_f attached to a cuspidal eigenform f is given by the action of Galois on a lattice, which allows us to consider its reduction modulo a prime lying over a prime integer ℓ:

$$\rho_{f,\ell} \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell).$$

Serre [30] conjectured that every irreducible odd Galois representation into $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is modular in the sense that each is conjugate to $\rho_{f,\ell}$ for some cuspidal eigenform f. Moreover, the now-proven conjecture gives a precise description of an optimal weight and level of a modular form that yields such a representation.

3 Presentation Highlights

The workshop included reports on a wide variety of major current research on modular forms. By highlighting them in this section, we provide an overview of much of the field as it stands. By design, many of the talks were on computational aspects of the theory.

Several talks at the workshop were given on the structure of Shafarevich-Tate groups of elliptic curves, whose finiteness is predicted by BSD. Amod Agashe [1] spoke on a factor of $L'(E, 1)$ in the case that $r_{\mathrm{an}} = 1$ that is related to the order of $\mathrm{Sha}(E)$ and presented evidence of a conjecture of Stein's on the structure of Tate-Shafarevich in this case in terms of computations of Cremona and Watkins. Dimitar Jetchev spoke on an improvement of an upper bound of on the Tate-Shafarevich group of E that is the first substantial improvement on the upper bound of Kolyvagin. Jetchev's work [17] was motivated by a computational project that Stein reported on to verify the full Birch and Swinnerton-Dyer conjecture for all elliptic curves with rank at most 1 and conductor at most 1000. Christian Wuthrich [33] also spoke about a project motivated by Stein's work to give upper bounds on the rank and p-primary part of the order of $\mathrm{Sha}(E)$, employing known results coming from Iwasawa theory on the Mazur-Tate p-adic analogue of BSD. Additionally, Neil Dummigan [14] spoke on his investigation of the critical values of symmetric square L-functions of level one cusp forms and his construction of elements in the associated Shafarevich-Tate groups predicted by the Bloch-Kato conjecture.

Several talks involved the study of Galois representations attached to modular forms. Gabor Wiese [36] discussed his work on the multiplicities of Galois representations attached to modular forms of weight one, settling the final remaining case in the study of the question of multiplicity one for modular Galois representations. In particular, he showed that the multiplicity is always greater than one if Frobenius acts as a scalar. In closely related work, Lloyd Kilford [22] discussed the occurrence of the failure of localizations of Hecke algebras to be Gorenstein in prime weight. He described extensive calculations of the Gorenstein defect, asking whether the muliplicity of the attached Galois representation is always 2 in the case that the Hecke algebra is not Gorenstein. In particular, their work resulted in a major improvement of the algorithm for computing modular symbols over a finite field. In another direction, Aaron Greicius gave a talk on his Ph.D. thesis (with Bjorn Poonen), in which he gave explicit necessary and sufficient conditions for the surjectivity of the global Galois representation into $\mathrm{GL}_2(\hat{\mathbf{Z}})$ attached to an elliptic curve over a number field. In particular, he gave computational examples in which this surjectivity holds.

A number of talks at the workshop were related to the conjectural construction of units of Gross-Stark type units and the Stark-Heegner points used in their construction. Pierre Charollois spoke on his joint work with Henri Darmon on the construction of Stark-type units in abelian extensions of almost totally real extensions of a totally real field F in terms of certain invariants attached to Eisenstein series on GL_2 over F and tori in this group. Samit Dasgupta presented his computations of Gross-Stark units via Shintani zeta functions, discussing work with his student Kaloyan Slavov in implementing algorithms suggested by Dasgupta's work. A paper by Dasgupta [11] on the calculation of Gross-Stark units in the p-adic setting has subsequently appeared. Matt Greenberg presented a more conceptual, cohomological approach to the theory of Stark-Heegner points which has enabled him to vastly extend various definitions, due to Darmon, Dasgupta, Trifkovic, and others, of Stark-Heegner points given previously in the literature (see for instance [15]). In a related direction, Darmon gave a report on work in progress with Bertolini and Prasanna concerned with constructing points on CM elliptic curves using higher dimensional cycles on Kuga-Sato varieties. This work [2, 3] is now almost completed, and will appear in a series of two articles. The first of these, which treats a new a p-adic variant of the Gross-Zagier formula, is about to be submitted for publication.

Frank Calegari and Matthew Emerton gave coordinated talks on their joint work on automorphic forms of cohomological type. Calegari described a bound on the dimension of the space of automorphic forms for a semisimple group over a number field that does not admit a discrete series [7]. Emerton spoke on the cohomology of arithmetic groups and the construction and study of objects such as p-adic representations. They have two joint papers in preparation related to the subject.

Victor Rotger discussed the structure of endomorphism algebras of the modular abelian variety attached to a newform of weight 2. He reported on progress towards a conjecture that there exist only finitely many isomorphism classes of such endomorphism algebras of a given degree over $\mathbf{Q}$. Some of the techniques and results, both theoretical and computational, can be found in [28] and [5]. Noam Elkies discussed a method for determining explicit formulas for genus 2 curves C over $\mathbf{Q}$ for which the endomorphism algebra contains an order in a real quadratic field. Such curves arise, for instance, as the degree two factors of the Jacobian of a modular curve. Armand Brumer reported on joint work with Ken Kramer on the existence of semistable abelian varieties over $\mathbf{Q}$.

Bjorn Poonen spoke on joint work with Ed Schaefer and Michael Stoll [27] on the equation $x^2+y^3=z^7$, one of the most difficult to solve equations of Fermat type. The determination of its solutions required a wide variety of sophisticated techniques involving modular curves and their Jacobians, including a sophisticated descent argument and very intensive computational work. Ken Ribet spoke on recent work of his then Ph.D. student, Soroosh Yazdani (also a workshop participant), on elliptic curves of odd modular degree. In particular, he described a relationship between the modular degree and congruences of modular forms that hold with the modular form attached to the elliptic curve.

John Cremona gave an excellent foundational talk on the construction of modular forms over general number fields: discussing the analogues of classical objects such as cusps, Hecke operators, and modular symbols, with an eye towards computing with the latter, as he and his students have already done for many imaginary quadratic fields. Cecelia Busuioc [6] described a construction of a very special modular symbol with values in Milnor K_2 of the ring of p-integers of the pth cyclotomic field, for an odd prime p. She used it to give evidence for a conjecture of Sharifi's [31] relating values of a cohomological pairing on p-units to L-values of cusp forms satisfying congruences with Eisenstein series.

Several talks presented algorithms for computation with objects related to modular forms. Lassina Dembélé presented an algorithm for the computation of Hilbert-Siegel modular forms over real quadratic fields and related it to the modularity of certain threefolds. Gonzalo Tornaría presented his spectacularly fast algorithms for computing Brandt matrices attached to ternary quadratic forms and showed how to use them to compute explicit Shimura correspondences. Ulf Kühn reported on an algorithm developed by his student, Anna Posingies, for computing the first non-vanishing coefficient of L-series that contribute to the constant term of non-holomorphic Eisenstein series, studied in [25].

Beyond the daytime lecture series, there were some evening sessions specifically devoted to discussing mathematical packages devoted to and useful for computing with modular forms and related objects. In particular, Stein gave a tutorial on Sage (`http://sagemath.org`), which is a free open source mathematical software program with substantial new functionality for computing with elliptic curves and modular forms. In addition, Cremona gave another evening session discussing tools for computing with elliptic curves.

4 Progress Made and Outcomes

The workshop provided an excellent opportunity for the exchange of ideas between researchers and the development of productive collaboration. We report on a small sampling of work that grew out of the conference, collaborations that were formed at the conference or by its participants, and one follow-up meeting that was organized by some of the speakers at the workshop.

In the course of the meeting, Charollois and Darmon found a more elegant interpretation of the invariants discussed by Charollois in his talk as the images of certain (non-algebraic) cycles on a Hilbert modular variety under a map which is formally analogous to the Griffiths Abel-Jacobi map on higher dimensional complex algebraic cycles, which will soon appear.

Also during the meeting, Tornaría pursued his collaboration with Darmon on the connections between the Shimura correspondence and the theory of Stark-Heegner points. The joint work of Darmon and Tornaría that was essentially completed at the BIRS meeting has now appeared [10].

Moreover, Stein and Weise had productive discussions on the details of an article [24] they wrote with Tak-Lun Koo, in which they studied the set of primes for which the pth coefficient of a given CM newform generates its field of coefficients.

The meeting also led to some fruitful exchanges between Dembélé and Greenberg which later led to Dembélé proving the existence of a finite (non-solvable) extension of $\mathbf{Q}$ unramified outside 2, answering a question of Gross and Serre. This work of Dembélé [12], which grew out of exchanges at the BIRS meeting, was solicited by Serre and is to appear.

During the meeting, Dembélé and Weise began to discuss collaboration on a work in progress, and Dembélé has held a position at Universität Duisberg-Essen to work with Weise since that time. In May 2009, he will move to the University of Warwick to work with Cremona. Similarly, Yazdani has held an NSERC postdoctoral fellowship at McMaster University under the supervision of Sharifi since shortly after the meeting.

In August 2008, Kilford, Wiese, and Dembélé organized a follow-up meeting to the BIRS workshop at the Heilbronn Institute in Bristol on Computations with Modular Forms. This meeting was announced at the BIRS workshop, where some of the planning was done by its organizers. The conference emphasized the actual coding of algorithms for computing with modular forms. Links to the code presented can be found at the conference's web page: `http://maths.pratum.net/CMF`.

5 Conclusion

We are happy to report that the meeting achieved its stated goal of bringing together researchers working with modular forms who employ a wide range of styles in their approaches to computation. Some of the researchers are at the forefront of developing algorithms for modular forms and useful software packages employing these algorithms, others are at the forefront of modern theoretical developments in the field, and quite a few are at both. As conjecture frequently demands computation, the interaction between the researchers in attendance had tremendous potential benefit for the participants, and thereby the field, benefit that has been and will continue to be realized.

References

[1] A. Agashe, Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank one, to appear in *Int. Math. Res. Not.*

[2] M. Bertolini, H. Darmon, and K. Prasanna, Generalized Heegner cycles and Rankin L-series, preprint.

[3] M. Bertolini, H. Darmon, and K. Prasanna, Exotic Heegner points on CM elliptic curves, preprint.

[4] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[5] N. Bruin, E. Flynn, J. González, and V. Rotger, On finiteness conjectures for endomorphism algebras of abelian surfaces, *Math. Proc. Cambridge Philos. Soc.* **141** (2006), 383–408.

[6] C. Busuioc, The Steinberg symbols and special values of L-functions, *Trans. Amer. Math. Soc.* **360** (2008), 5999–6015.

[7] F. Calegari and M. Emerton, Bounds for multiplicities of unitary representations of cohomological type in spaces of cusp forms, arXiv:0704.0662, to appear in *Ann. of Math.*

[8] P. Charollois and H. Darmon, Arguments des units de Stark et priodes de sries d'Eisenstein, to appear in *Algebra Number Theory*.

[9] H. Darmon, Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications, *Ann. of Math.* **154** (2001), 589–639.

[10] H. Darmon and G. Tornaría, Stark-Heegner points and the Shimura correspondence, *Compos. Math.* **144** (2008), 1155–1175

[11] S. Dasgupta, Computations of Elliptic Units for Real Quadratic Fields, *Canad. J. Math.* **59** (2007), 553–574.

[12] L. Dembélé, A non-solvable Galois extension of Q ramified at 2 only, with a supplement by Jean-Pierre Serre, to appear in *C. R. Math. Acad. Sci. Paris*.

[13] P. Deligne, Formes modulaires et représentations ℓ-adiques, *Séminaire Bourbaki*, Exp. 355, 1968/9.

[14] N. Dummigan, Symmetric square L-functions and Shafarevich-Tate groups, II, preprint.

[15] M. Greenberg, Stark-Heegner points and the cohomology of quaternionic Shimura varieties, preprint.

[16] B. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225-320.

[17] D. Jetchev and W. Stein, Visibility of Shafarevich-Tate Groups at Higher Level, *Doc. Math.* **12** (2007).

[18] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. In *Cohomologies p-adiques et applications arithmtiques. III.* Asterisque **295**, 117–290, Soc. Math. France, 2004.

[19] C. Khare and J-P. Wintenberger, Serre's Modularity Conjecture (I), preprint.

[20] C. Khare and J-P. Wintenberger, Serre's Modularity Conjecture (II), preprint.

[21] M. Kisin, Modularity of 2-adic Barsotti-Tate representations, preprint.

[22] L. Kilford and G. Wiese, On the failure for the Gorenstein property for Hecke algebras of prime weight, *Exper. Math.* **17** (2008), 37–52.

[23] V. Kolyvagin, Euler systems. In *The Grothendieck Festschrift, Vol. II.* Progr. Math. **87**, Birkhäuser, 1990.

[24] T. Koo, W. Stein, and G. Wiese, On the generation of the coefficient field of a newform by a single Hecke eigenvalue, *J. Théorie Nombres Bordeaux* **20** (2008), 373-384.

[25] U. Kühn, Nron-Tate heights on algebraic curves and subgroups of the modular group, *Manuscripta Math.* **116** (2005), 401–419.

[26] B. Mazur, J. Tate, and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.

[27] B. Poonen, E. Schaefer, and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, *Duke Math. J.* **137** (2007), 103–158.

[28] V. Rotger, A. Skorobogatov, and A. Yafaev, Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$, *Mosc. Math. J.* **5** (2005), 463–476.

[29] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[30] J-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** (1987), 179–230.

[31] R. Sharifi, Cup products and L-values of cusp forms, *Pure Appl. Math. Quart.* **5** (2009), 339–348.

[32] G. Shimura, Correspondances modulaire et les functions ζ de courbes algébriques, *J. Math Soc. Japan*, **10** (1958), 1–28.

[33] W. Stein and C. Wuthrich, Computations on the Tate-Shafarevich group using Iwasawa theory, in preparation.

[34] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.

[35] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* **168** (1967), 149–156.

[36] G. Wiese, Multiplicities of Galois representations of weight one, with an appendix by Niko Naumann, *Algebra Number Theory* **1** (2007) 67–85.

[37] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* **141** (1995), 443–551.