

Introduction

In modern Number Theory, the theory of automorphic forms is deeply related to the understanding of the structure of the absolute Galois group $G_{\mathbf{Q}} = \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, via its representations.

The Theorem of Kronecker-Weber, which states that all abelian extensions of \mathbf{Q} are contained in cyclotomic fields, can be viewed as the simplest example of this relationship. The modular function j and the Weierstrass \wp -function, via the theory of complex multiplication, gives a similar result about class fields of imaginary quadratic fields. This is one instance of the Hilbert 12th problem which aims to find class field of more general number fields by means of analytic methods.

The construction of class fields of quadratic fields using automorphic forms has been conjecturally extended to real quadratic fields and quadratic extensions of real quadratic fields with exactly one complex place by Darmon [9], and Darmon and Logan [10]. But ultimately what one would like to obtain is a non-abelian class field theory, and automorphic forms on \mathbf{GL}_2 is a first step in that direction.

Since the work of Wiles [39] on Fermat Last Theorem, there has been some tremendous progress in that direction, for the base field \mathbf{Q} , with the recent proof of the Serre conjecture by Khare and Wintenberger [28] and Kisin [29], and work of Kisin [30] on the Fontaine-Mazur conjecture.

Long before all the major contributions of the last decade that led to proving that every Abelian variety of \mathbf{GL}_2 -type defined over the field of rationals is modular, there was a great deal of numerical results available on classical modular forms and related conjectures, such as the Serre and Birch and Swinnerton-Dyer conjectures (cf. Antwerp Tables [2] and Cremona [7]). Cremona's database has been largely extended by Stein [38].

In fact, the value of numerical experimentation in Number Theory has grown increasingly important alongside our computational capabilities, especially in the last 50 years. Indeed, the Birch and Swinnerton-Dyer conjecture which has now become central to Number Theory and Arithmetic Geometry was discovered in 1965 with the help of one of the early computers EDSAC available at Cambridge. This shows that experimentation can open new avenues for theoreticians to explore, the same way it can help them refine some of their conjectures. So the symbiotic relationship between computational and theoretical aspects of Number Theory is as stronger as ever.

Outside the classical setting however, one must deplore that there is very little numerical results on automorphic forms in general. However, there is an increased need as suggested by all the recent progress.

1 Past research

1.1 The Hilbert Modular Forms Package

In [12, 13, 19], I developed a very efficient algorithm for computing Hilbert modular forms over totally real number fields. I also wrote a major component of the Hilbert Modular Forms Package which will be part of the January 2009 Magma release. Given a totally real number field F , an integral ideal $\mathfrak{n} \subseteq \mathcal{O}_F$, the ring of integers of F , and an arithmetic weight \underline{k} , the package computes the space of Hilbert cusp forms of level \mathfrak{n} and weight \underline{k} as a Hecke module. The computation relies on the Jacquet-Langlands correspondence [27, Chap. XVI] which relates such spaces to automorphic forms on certain totally definite quaternion algebras over F .

Given a rational prime p , and an irreducible $\overline{\mathbf{F}}_p$ -representation V of $\mathbf{GL}_2(\mathcal{O}_F/p)$, the package can also compute the space of \pmod{p} Hilbert modular forms of weight V . I have used this component to do computations related to the Serre conjecture for totally real number fields as well as the \pmod{p} Langlands Correspondence.

1.2 Algorithm for modular elliptic curves over real quadratic fields

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalized eigenform over the rationals. The Eichler-Shimura construction provides a systematic way to obtain the associated abelian variety A_f over \mathbf{Q} . In the case when the form f has rational Fourier coefficients, Cremona [7] made this construction explicit by using the theory of modular symbols. This gave an algorithm which he then used to create a database of (modular) elliptic curves over \mathbf{Q} that has proved extremely useful to number theorists. This database has been largely extended by Stein [38].

There is a conjectural extension of the Eichler-Shimura construction to Hilbert modular forms that can be formulated in several ways. We recall the following motivic generalization due to Oda [33] in the case of real quadratic fields.

Conjecture 1 (Oda). *Let F be a real quadratic field, \mathfrak{n} an integral ideal of \mathcal{O}_F , the ring of integers of F , and $X_0(\mathfrak{n})/\mathbf{Q}$ the Hilbert-Blumenthal modular surface of level \mathfrak{n} . Let f be a normalized eigenform of level \mathfrak{n} and parallel weight 2, and $H^2(X_0(\mathfrak{n}), \mathbf{Q})_f$ the isotypic component of f in the cuspidal cohomology. Then, there exists an abelian variety A_f defined over F , with good reduction outside \mathfrak{n} and real multiplication by the number field K_f generated by the Fourier coefficients of f , together with an isomorphism of Hodge structures*

$$H^2(X_0(\mathfrak{n}), \mathbf{Q})_f \cong H^1(A_f, \mathbf{Q}) \otimes H^1(A_f^\sigma, \mathbf{Q}),$$

where A_f^σ is the Galois conjugate of A_f .

Many cases of Conjecture 1 have been proved by using the arithmetic theory of Shimura curves. Unfortunately, when the abelian variety A_f has everywhere good reduction, the Shimura curves approach does not work.

In [14], I recently developed an algorithm that computes modular elliptic curves over real quadratic fields based on Conjecture 1. I hope to combine the Hilbert modular forms algorithm and the elliptic curves algorithm in order to create a database such as the ones by Cremona [7] and Stein [38] in the case of real quadratic fields. This will provide additional numerical evidence for Conjecture 1. One important application of my algorithm is to give a way to systematically compute modular elliptic curves with everywhere good reduction over real quadratic fields.

1.3 Computing Hilbert-Siegel modular forms

The algorithm described in Subsection 1.1 for the computation of Hilbert modular forms relies on the Jacquet-Langlands correspondence. There is a conjectural generalization of this correspondence to the genus 2 case due to Ihara [26] and Ibukiyama [25]. By making use of this, C. Cunningham and I were able to extend my algorithm to this case, thus providing a conjectural algorithm for the computation of Hilbert-Siegel modular forms of genus 2. We have tabulated examples of systems of eigenvalues of weight 3 and genus 2 of such forms for small primes levels over the quadratic fields $\mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}(\sqrt{2})$ in [8] and [17], and I hope to expand this data in the near future.

In fact, the algorithm presented in [8, 17] gives a more systematic approach to the computation of algebraic modular forms. And so, it can be used for other algebraic groups such as the unitary groups $\mathbf{U}(3)$. I have illustrated this fact by computing eigenforms on the unitary groups in three variables $\mathbf{U}(3)/\mathbf{Q}$ attached to the quadratic fields $F = \mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-3})$, and the unitary group $\mathbf{U}(3)/\mathbf{Q}(\sqrt{5})$ attached to the cyclotomic field $\mathbf{Q}(\zeta_5)$.

2 Current projects

2.1 Nonsolvable Galois extensions ramified only at one small prime

The following conjecture is proposed in Gross [23].

Conjecture 2. *For any prime number p , there is a finite non-solvable Galois extension K of \mathbf{Q} ramified at p only.*

For primes $p \geq 11$, one knows how to construct extensions satisfying Conjecture 2. Indeed, Serre [35] shows that for such a prime p , there is $k = 12, 16, 18, 20, 22$ or 26 such that the residual Galois representation $\bar{\rho}_{k,p} \bmod p$ associated to the unique cuspidal form of level 1 and weight k , with integral coefficients, is absolutely irreducible. Hence the fixed field of $\ker \bar{\rho}_{k,p}$ is a non solvable extension of \mathbf{Q} unramified away from p .

As for primes ≤ 7 , the first case of the Serre conjecture [34] was proved and later published by Tate [37], for $p = 2$, by simply ruling out the existence of mod

2 irreducible representations of the absolute Galois group $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, unramified away from 2. His results were later extended to the primes 3 and 5 by [36] and [4] respectively, assuming GRH in the latter case. By Khare and Wintenberger [28], this is now true unconditionally for $p = 5, 7$.

Recently, following a suggestion of Dick Gross, I showed [15] that Conjecture 2 is true for $p = 2$ by using Galois representations attached to mod p Hilbert modular forms over the maximal totally real subfield of the cyclotomic $\mathbf{Q}(\zeta_{32})$. The extension K I constructed is totally complex, has degree $2251731094732800 = 2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2$ and has root discriminant $\delta_K < 2^{\frac{47}{8}} = 58.68\dots$, which is rather small.

I am currently working on extending this strategy to the primes $p = 3$ and 5. Preliminary computations suggested however that this will not work for $p = 7$, as the dimension of the spaces of Hilbert modular forms involved become rather large.

2.2 The Serre conjecture for totally real number fields

The following conjecture due to Serre [34], which has been proved recently by Khare and Wintenberger [28] and Kisin [29], has been very influential in Number Theory. (For definitions, we refer to [34]).

Conjecture 3 (Serre). *Let \mathbf{F} be a finite field, and $\rho : G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{F})$ an irreducible continuous representation such that $\det \rho(c) = -1$ for the complex conjugation c . Then ρ is modular.*

In [34], Serre gives a precise recipe to find the minimal weight $k(\rho)$ and level $N(\rho)$ of the corresponding modular form. Buzzard, Diamond and Jarvis [5] have formulated a generalization of this conjecture to the context of totally real number fields, where predicting the weights of the modular forms is more subtle. Gee [21] proved that their weight recipe is correct in lots of cases. I am working on a joint project with F. Diamond and D. Roberts [18] which aims to provide numerical evidence for the conjecture and further insight into the remaining cases of the weight recipe. My algorithm for computing mod p Hilbert modular forms is an important component of this project.

2.3 Motives attached to Hilbert-Siegel modular forms

Thanks to the works of Wiles [39] and of Breuil, Conrad, Diamond and Taylor [3] on the Shimura–Taniyama conjecture and of Khare and Wintenberger [28] and Kisin [29] on the Serre conjecture, there has been some tremendous progress toward the Langlands correspondence for \mathbf{GL}_2/\mathbf{Q} . Indeed, we now know that every abelian variety A/\mathbf{Q} of \mathbf{GL}_2 -type is modular.

The symplectic group \mathbf{GSp}_4 is the natural next step in trying to understand the Langlands correspondence for groups of higher ranks. In the spirit of Fontaine-Mazur, one expects the following conjecture.

Conjecture 4. *Let X/\mathbf{Q} be a threefold over the rationals, with the Hodge numbers $h^3 = 4$, $h^{3,0} = h^{2,1} = h^{1,2} = h^{0,3} = 1$. Let $\ell \geq 3$ be a prime number, and let*

$$\rho_{X,\ell} : \mathbf{G}_{\mathbf{Q}} \longrightarrow \mathbf{GL}(\mathbf{H}^3(X_{\text{ét}}, \bar{\mathbf{Q}}_{\ell}))$$

be the ℓ -adic Galois representation in the degree 3 étale cohomology of X . Then $\rho_{X,\ell}$ is automorphic in the sense that it is isomorphic to the Galois representation attached to some Siegel modular form of genus 2 and weight 3.

In the literature, there are several examples that provide both theoretical and numerical evidences towards Conjecture 4. For example, Consani and Scholten [6] investigate a quintic threefold that satisfies the assumptions in Conjecture 4 and give strong evidence that it is indeed automorphic.

Unfortunately, in most of the known examples related to Conjecture 4, the corresponding automorphic forms are lifted from \mathbf{GL}_2 . In part, this is due to the difficulty of computing automorphic forms in higher rank. We would like to produce examples that support Conjecture 4 and that do not come from lifts by using our algorithm on Hilbert-Siegel modular forms. More specifically, by exploiting the ideas in [6], we hope to determine some of the motives associated to the eigensystems of Hilbert-Siegel modular forms we computed in [8, 17]. This will provide some numerical evidence for both the Jacquet-Langlands correspondence and the Langlands correspondence in the genus 2 case.

2.4 Modular abelian surfaces over real quadratic fields

As explained earlier, by making the Eichler-Shimura construction for modular elliptic curves over the rationals explicit, Cremona [7] was able to generate tables of such curves that proved extremely useful to number theorists. Recently, Guàrdia [24] developed the theory of Jacobian nullwerte which is analogue to Cremona's approach for modular abelian surfaces over the rationals. González and González-Jiménez [22] then used this construction to produce tables of modular abelian surfaces over \mathbf{Q} . We hope to extend their results to real quadratic fields, and combine this with Oda's conjecture in order to find explicit examples of modular abelian surfaces with real multiplication over real quadratic fields. An important application of this project would be to find (simple) modular abelian surfaces with everywhere good reduction.

3 Research plans

In addition to continuing my work on the above projects, I plan to work on the following over the next two years.

3.1 The generalized Fermat equation

By making use of the techniques of Wiles [39], Bennett and Skinner [1] studied cases of the generalized Fermat equation $ax^p + by^p = cz^2$. The Frey representation attached to a non-trivial solution to such an equation is realized in the p -division points of some elliptic curve defined over \mathbf{Q} and some prime p . They then use the database of Stein [38] to draw conclusions on the non-existence of such solutions. I want to combine their methods with the strategy outlined in [11] to study equations of the form $ax^p + by^p = cz^5$. The Frey representations attached to non-trivial solutions to this equation are realized in the p -division points of hypergeometric abelian surfaces defined over $\mathbf{Q}(\sqrt{5})$ (cf. Darmon [11]). So with my database, I will be able to solve some cases of this equation.

3.2 Parallel weight one Hilbert modular forms

I would like to develop efficient algorithms to compute Hilbert modular forms of parallel weight one, for which quaternion algebra methods are not directly applicable. There is little numerical data on such forms, which correspond via Artin's conjecture to complex 2-dimensional Galois representations. I plan to consider the case of partial weight one as well, for which there may be no known explicit examples.

3.3 Revisiting the method of graphs for large genus

One of the fastest algorithms that can be used to compute classical modular forms is the so-called method of graphs developed by Mestre [32]. To briefly describe the method, let $p \geq 2$ be a prime and $M \geq 1$ an integer prime to p . One wishes to compute modular forms of level $N = pM$ and weight 2. The method of graphs consider the modular curve $X_0(M)/\mathbf{F}_p$. For a prime $\ell \neq p$, one uses explicit equations for the Hecke correspondence on this curve in order to compute the action of the operator T_ℓ . This method is extremely efficient when the genus of $X_0(M)$ is at most 1, but is impractical otherwise. As an alternative, one can use the classical Brandt matrices approach due to Pizer or the Quaternionic Hecke module approach due to Kohel [31]. However, both these methods can be extremely slow. In a joint project with D. Kohel and W. Stein [20], we want to show that the algorithm develop in [12, 13] is a much better alternative. We already have some partial results in that direction with the prime $p = 389$ for which the method of graphs would be totally unapplicable since the genus of the curve $X_0(389)$ is 33. Our algorithm has proved to be faster than the above mentioned ones.

References

- [1] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.* **56** (2004), no. 1, 23–54.
- [2] Modular functions of one variable. IV. Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, Edited by B. J. Birch and W. Kuyk. *Lecture Notes in Mathematics*, Vol. **476**. Springer-Verlag, Berlin-New York, 1975.
- [3] 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), no. 4, 843–939.
- [4] S. Brueggeman, The nonexistence of certain Galois extensions unramified outside 5, *J. Number Theory* **75** (1999), 4752.
- [5] K. Buzzard, F. Diamond and F. Jarvis, On Serre’s conjecture for mod l Galois representations over totally real fields, preprint. Available at: http://uk.arxiv.org/PS_cache/arxiv/pdf/0810/0810.2106v1.pdf
- [6] C. Consani and J. Scholten, Arithmetic on a quintic threefold. *International Journal of Mathematics* **12**, No. 8 (2001), pp. 943-972.
- [7] Cremona, J. E. *Algorithms for modular elliptic curves*. Second edition. Cambridge University Press, Cambridge, 1997. vi+376 pp.
- [8] C. Cunningham and L. Dembélé, Computing genus 2 Hilbert-Siegel modular forms over $\mathbf{Q}(\sqrt{5})$ via the Jacquet-Langlands correspondence. To appear in *Exp. Math.*
- [9] H. Darmon, Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Annals of Mathematics*, **154** (2001) 589-639.
- [10] H. Darmon and A. Logan, Periods of Hilbert modular forms and rational points on elliptic curves, *International Mathematics Research Notices*, **40** (2003), 2153-2180.
- [11] H. Darmon, Rigid local systems, Hilbert modular forms, and Fermat’s last theorem. *Duke Math. J.* **102** (2000), no. 3, 413–449.
- [12] L. Dembélé, Explicit computations of Hilbert modular forms on $\mathbf{Q}(\sqrt{5})$. *Experimental Mathematics*, Vol. **14**, No 4 (2005), pp. 457-466.
- [13] L. Dembélé, Quaternionic M -symbols, Brandt matrices and Hilbert modular forms. *Math. Comp.* Vol. **76**, no 258 (2007), 1039-1057.

- [14] L. Dembélé, An algorithm for modular elliptic curves over real quadratic fields. To appear in *Exp. Math.*
- [15] L. Dembélé, A non-solvable Galois extension of \mathbf{Q} ramified at 2 only, with a supplement by Serre (submitted).
- [16] L. Dembélé, An algorithm for modular abelian surfaces over real quadratic fields (in preparation).
- [17] L. Dembélé, On the computation of algebraic modular forms (submitted), 14 pages.
- [18] L. Dembélé, F. Diamond, D. Roberts, Numerical evidences and examples of Serre's conjecture over totally real fields (in preparation).
- [19] L. Dembélé and S. Donnelly, Computing Hilbert modular forms for fields with non-trivial class group. ANTS VIII Proceedings, *Lect. Notes in Comp. Sci.* Vol. **5011** (2008), 371–386.
- [20] L. Dembélé, D. Kohel and W. Stein, Efficient Computation of Modular Forms Using Quaternion algebras (in preparation).
- [21] T. Gee, On the weights of mod p Hilbert modular forms, preprint. Available at: http://uk.arxiv.org/PS_cache/math/pdf/0601/0601516v2.pdf
- [22] González-Jiménez, Enrique; González, Josep Modular curves of genus 2. *Math. Comp.* **72** (2003), no. 241, 397–418.
- [23] B. Gross, Modular forms (mod p) and Galois representations. *Inter. Math. Res. Notices* **16** (1998), 865–875.
- [24] Guàrdia, Jordi Jacobian nullwerte and algebraic equations. *J. Algebra* **253** (2002), no. 1, 112–132.
- [25] Ibukiyama, Tomoyoshi. On symplectic Euler factors of genus two. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **30** (1984), no. 3, 587–614.
- [26] Y. Ihara, On certain arithmetical Dirichlet series. *J. Math. Soc. Japan* Vol. **16** no 3 (1964), 214–225.
- [27] H. Jacquet and R. P. Langlands, Automorphic forms on $GL(2)$. *Lecture Notes in Mathematics*, Vol. **114**. Springer-Verlag, Berlin-New York, 1970. vii+548 pp.
- [28] C. Khare and J.-P. Wintenberger, On Serre's conjecture for 2-dimensional mod p representations of $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. To appear in *Annals of Math.*

- [29] M. Kisin, Moduli of finite flat group schemes, and modularity. To appear in *Annals of Math.*
- [30] M. Kisin, The Fontaine-Mazur conjecture for GL_2 . To appear in *J. Amer. Math. Soc.*
- [31] D. Kohel, The Hecke module structure of quaternions. *Class field theory—its centenary and prospect*. Math. Soc. Japan, Tokyo 1998, 177-195.
- [32] J.-F. Mestre, La méthode des graphes. Exemples et applications, *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, Katata (1986), 217-242.
- [33] T. Oda, Periods of Hilbert modular surfaces. *Progress in Math.*, **19**. Birkhauser, Boston, Mass., 1982.
- [34] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.* **54** (1987), no. 1, 179–230.
- [35] J.-P. Serre, Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]. Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, pp. 319–338. *Lecture Notes in Math.*, Vol. **317**, Springer, Berlin, 1973.
- [36] J.-P. Serre, Note 229.2 on p. 710, *Oeuvres III*, Springer-Verlag, 1986.
- [37] J. Tate, The non-existence of certain Galois extensions of \mathbf{Q} unramified outside 2, *Contemp. Math.* **174** (1994), 153–156.
- [38] W. Stein, Modular forms database, <http://modular.fas.harvard.edu/>
- [39] A. Wiles, Modular elliptic curves and Fermat Last Theorem. *Annals of Math.* **141** (1995), pp. 443–551.