THE PARAMODULAR CONJECTURE

ARMAND BRUMER

(Joint work with Ken Kramer and Magma)

Modular Forms and Curves of Low Genus:

Computational Aspects @ ICERM Sept. 30, 2015

- B&Kramer: Certain abelian varieties bad at one prime, ArXiv.
- BPVY: Work in Progress verifying the Paramodular conjecture for $N = 277$.
- BK1: Paramodular abelian varieties of odd conductor, Trans. Amer. Math. Soc. **366(5)** (2014), 2463–2516.
- BK2 A. Brumer and K. Kramer, Arithmetic of division fields, Proc. Amer. Math. Soc. **140** (2012) 2981-2995.
- Cris Poor and David Yuen: Paramodular Cusp Forms, Math. Comp. 84 (2015), 1401–1438.

THE PARAMODULAR CONJECTURE

The L-series of abelian surfaces of GL_2-type are products of L-series of weight 2 elliptic modular eigenforms. For all other abelian surfaces, we propose:

Conjecture. *Let $K(N)$ be the paramodular group of level N. There is a one-to-one correspondence:*

isogeny classes of abelian surfaces $A_{/\mathbb{Q}}$ of conductor N with $\mathrm{End}_{\mathbb{Q}} A = \mathbb{Z}$	$\leftrightarrow$	weight 2 *non-lifts* f on $K(N)$, with rational eigenvalues (up to scalar multiplication)

such that (i) $L(A, s) = L(f, s)$ and

(ii) the ℓ-adic representations of $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ and that of f should be isomorphic (for any ℓ prime to N).

We expect the extension to abelian varieties A of dimension $2d$ with $\mathrm{End}_{\mathbb{Q}} A$ an order $\mathfrak{o}$ in a totally real field of degree d.

Here we should have a Galois representation

$$G_{\mathbb{Q}} \to \mathrm{GSp}(\mathbb{T}_\ell(A)) = \mathrm{GSp}_4(\mathfrak{o})$$

and $L(A,s) = \prod(L(f^\sigma, s)$ over the conjugates of the non-lifts paramodular form.

Problem: How does one find such abelian varieties?

Our conjecture holds for Weil restrictions of modular elliptic curves $E/\mathbb{Q}(\sqrt{d})$, not isogenous to their conjugate (Johnson-Leung-Roberts if $d > 0$) and (Berger-Dembélé-Pacetti-Şengün if $d < 0$). Also some abelian surfaces with potential real multiplication have been handled, by Dembélé and A. Kumar. It is also compatible with twists (JL-R). I expect this will be explained in later talks.

But, so far, no genuinely GSp_4 example has been verified!

We must bound the two sides of our conjecture. Upper bounds are given by Poor-Yuen on the analytic side. In BK1, we showed for many odd N with no weight 2 non-lift on $K(N)$, that no semi-stable abelian surface A of conductor N exists. This required a detailed study of the group schemes $A[2^n]$ extending methods of Fontaine and Schoof. A couple of sample results:

- a semi-stable paramodular abelian variety of odd conductor $N < 300$ exists only for $N = 249$, 277 and 295, and at least one abelian surface is known. For 277, we have the Jacobian A_{277} of the hyperelliptic curve:

$$C_{277} : y^2 + y = x^5 - 2x^3 + 2x^2 - x.$$

- If $N < 500$ is prime, then N could only be 277, 349, 353, 389 or 461. Again we know Jacobians.

We could find Jacobians in the isogeny classes thanks to

Thm.[B-K] A semistable abelian surface A of conductor mp, with $p \geq 11$ and $\mathrm{rad}(m) \leq 10$, is $\mathbb{Q}$-isogenous to a Jacobian.

Hint: Apply the Khare-Wintenberger's theorem to a polarization of minimal degree in the isogeny class.

However, $H : z^4 + 2yz^3 + (y - 2x)y^2z + (x - y)y(x^2 - 2z^2)$ admits a degree 2 map to the elliptic curve E_{11}, so

$$0 \to P \to \mathrm{Jac}(H) \to E_{11} \to 0.$$

The Prym P has conductor $11 * 67$, minimal polarization $(1, 2)$ and

$$0 \to E_{11}[2] \to P[2] \to E_{67}[2] \to 0$$

is induced by the kernel of the polarization $\varphi : P \to \hat{P}$.

Let $\mathcal{A}(T)$ be the set of isogeny classes of simple abelian varieties over $\mathbb{Q}$ with good reduction outside a finite set T and $\mathcal{S}(T)$ the subset of classes of semi-stable abelian varieties. The subset $\mathcal{A}_d(T)$ of $\mathcal{A}(T)$ of dimension d is finite (Faltings).

- $|\mathcal{A}(\phi)| = 0$ (Abrashkin and Fontaine).
- $|\mathcal{A}_2(2)| \geq 165 + 50$ with 165 classes of Jacobians of curves good outside 2 (Merriman-Smart) and 50 additional classes of Weil restrictions or factors of $J_0(2^{10})$.
- $\mathcal{S}(N) = \{J_0(N)\}$ for all odd squarefree $N \leq 29$ (Schoof).

Using the Odlyzko and Fontaine discriminants bounds, Schoof determines all simple finite flat group schemes of 2-primary order over $\mathbb{Z}\left[\frac{1}{N}\right]$, and their extensions by one another.

Question: For $p \neq N$, is the rank of simple p-primary finite flat group schemes over $\mathbb{Z}\left[\frac{1}{N}\right]$ bounded?

For $p = 2$ and odd $N \leq 127$, all are "classically modular", thanks to Odlyzko bounds (BK2).

In this talk, we shall explain:

I. How to modify the Faltings-Serre method to check modularity for certain abelian surfaces of conductor N.

II. Uniqueness criteria extending to larger conductors work of Schoof.

From now on, N will be a prime.

THE FALTINGS-SERRE METHOD

Let $A = A_{277}$ be the abelian surface mentioned earlier. The action of $G_{\mathbb{Q}}$ on the Tate module $\mathbb{T}_2(A) = \varprojlim A[2^n]$ yields a 2-adic representation $\rho_1 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{Z}_2)$ which is unramified outside $\{2, 277\}$ and with reduction

$$\overline{\rho}_1 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{S}_5 \subset \mathrm{GSp}_4(\mathbb{F}_2) \simeq \mathrm{S}_6.$$

Associated to the Siegel modular form f_{277} of weight 2 on $K(277)$, is a 2-adic Galois representation $\rho_2 : G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Z}_2)$ constructed by Taylor by conguences in a way similar to that of Deligne-Serre for weight one classical forms. Assume:

i) $\rho_2 : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Z}_2)$ is unramified outside $\{2, 277\}$ with similitude character equal to the cyclotomic character (Tilouine and Thorne may have a proof);

ii) $\overline{\rho}_1$ and $\overline{\rho}_2$ are isomorphic. (Checkable by targeted search?)

Let $\Sigma = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 97\}$.
If for all p in Σ, we have

$$1 + p - |\#C_{277}(\mathbb{F}_p)| = \mathrm{tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{tr}(\rho_2(\mathrm{Frob}_p)) = t_p(f_{277}),$$

then the ρ_i are equivalent and so the two L-series agree.

Thm.(Carayol) Let A be a complete local ring with maximal ideal $\mathfrak{m}$ and residue field k. Let Γ be a profinite group and $R = A[[\Gamma]]$ its completed group ring. Let $\rho_i : \Gamma \to \mathrm{GL}_n(A)$ be two representations. If $\mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g))$ for all g in Γ and the reduction $\overline{\rho}_1$ is absolutely irreducible, then ρ_1 and ρ_2 are equivalent.

Let $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{Z}_\ell)$ be two non-isomorphic ℓ-adic representations, unramified outside S, with equal similitudes and absolutely irreducible reductions $\overline{\rho}_i : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{F}_\ell)$. Let $\overline{\rho}$ be the common reduction and $\mathrm{G} \subseteq \mathrm{GSp}_4(\mathbb{F}_\ell)$ be the common image. Let $r \geq 1$ be maximal so that

$$\mathrm{tr}(\rho_1(g)) \equiv \mathrm{tr}(\rho_2(g)) \pmod{\ell^r} \text{ for all } g \in G_{\mathbb{Q}}.$$

By Carayol (and conjugation), assume that the reductions mod ℓ^r of ρ_i are equal. Define the $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell$ by

$$\tau(g) = \frac{\mathrm{tr}(\rho_1(g)) - \mathrm{tr}(\rho_2(g))}{\ell^r} \pmod{\ell}.$$

If $\rho_1(g) = (1 + \ell^r \mu(g))\rho_2(g)$ with $\mu : \mathrm{G}_{\mathbb{Q}} \to \mathrm{M}_4(\mathbb{Z}_\ell)$, then

$\tau(g) = tr(\overline{\mu}(g)\overline{\rho}(g))$ and $\overline{\mu}(g)$ is in $\mathfrak{sp}_4(\mathbb{F}_\ell)$. Let

$$\mathcal{P}(G) = \left\{ \begin{vmatrix} g & mg \\ 0 & g \end{vmatrix} \ : \ g \in G, m \in \mathfrak{sp}_4(\mathbb{F}_\ell) \right\},$$

while $\mathcal{B}(G)$ allows any entry in the top right corner. We deduce a homomorphism $\tilde{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathcal{P}(G)$ by

$$\tilde{\rho}(g) = \begin{vmatrix} \overline{\rho}(g) & \overline{\mu}(g)\overline{\rho}(g) \\ 0 & \overline{\rho}(g) \end{vmatrix}.$$

An element of $\mathcal{P}(G)$ is obstructing if the trace of its top right corner is non-trivial, a property invariant under conjugation by $\mathcal{B}(G)$. The deviation groups are the subgroups of $\mathcal{P}(G)$ that contain obstructing elements and project onto G.

Conclusion: If the ρ_i are not isomorphic, the image $H = \tilde{\rho}(G_{\mathbb{Q}})$ is a deviation group. The field L cut out by ker(ρ) is unramified outside S and is an elementary ℓ-extension of the fixed field F of ker($\overline{\rho}$). We must find all extensions whose Galois group is isomorphic to a possible deviation group. For each such field, we must find some witness $p \notin S$ such that Frob$_p$ is in an obstructing class but also does not emulate a non-obstructing class.

Now specialize to $\ell = 2$ and $G = \mathsf{S}_5$ acting on $A[2]$.

Prop. Up to $\mathcal{B}(\mathsf{S}_5)$-conjugacy, we have 9 deviation subgroups H_i of $\mathcal{P}(\mathsf{S}_5)$, but $H_7 \simeq H_8$.

H	$\lvert H\rvert$	Cycles in S_{20} of obstructing classes	$\mathfrak{O}$
H_1	$2^{10}\cdot 5!$	$[6^1 3^4 2^1, 4^1 2^5 1^6, 8^1 4^2 2^2, 8^1 4^3, 4^3 1^8,$ $10^2, 4^1 2^4 1^8, 4^3 2^1 1^6]$	$-$
H_2	$2^9\cdot 5!$	$[6^1 3^4 2^1, 10^2]$	10
H_3	$2^6\cdot 5!$	$[10^2, 8^1 4^3, 8^1 4^2 2^2]$	8
H_4	$2^5\cdot 5!$	$[10^2]$	$8, 10$
H_5	$2^5\cdot 5!$	$[10^2]$	$8, 10$
H_6	$2\cdot 5!$	$[10^2]$	10
H_7	$2^4\cdot 5!$	$[6^1 3^4 2^1, 4^3 2^3 1^2]$	$8, 12$
H_8	$2^4\cdot 5!$	$[6^1 3^4 2^1, 4^3 2^3 1^2]$	8
H_9	$5!$	$-$	6

As usual, we denote by $a^i b^j$.. the permutation whose cycle decomposition consists of i a-cycles, j b-cycles,...

FINDING WITNESSES WITH MAGMA

Let f be a quintic with roots r_i, Galois closure F and group S_5. The pair-resolvant of F is the degree 10 subfield $K = \mathbb{Q}(r_1 + r_2)$ fixed by $\langle (12), (34), (45) \rangle$.

Every field L whose Galois group is isomorphic to some H_i above is the splitting field of a polynomial g_L of degree 20 obtained as the minimal polynomial of a quadratic extension of the pair-resolvant. For each such L and each prime $p < 1000$, factor $g_L \pmod{p}$ to see if the cycle pattern or order of Frob_p makes p a "witness".

For $N = 277$, one had to check 4095 quadratic extensions. For $N = 1051$, there are $2^{15} - 1$ such extensions, but only 26 primes "witnesses" are needed, the largest of which is 149.

One treats similarly the other cases with $A[2]$ absolutely irreducible, namely $G \simeq S_6$ and the wreath product $S_3 \wr S_2$ of order 72. We are waiting for the eigenvalues of the alleged paramodular forms ...

A UNIQUENESS RESULT

The abelian surface A of conductor N is called favorable if $F = \mathbb{Q}(A[2])$ is the Galois closure of a quintic field F_0 of discriminant $\pm 16N$ in which 2 is totally ramified.
We assume this for the remainder of the talk!

Example: The Jacobian A of $y^2 + y = g(x)$ is favorable if g is a monic quintic and $f = 1 + 4g$ has discriminant $\pm 256N$. Then A has conductor N, $E = A[2]$ is a simple finite flat group scheme over $\mathbb{Z}\left[\frac{1}{N}\right]$ and is biconnected over $\mathbb{Z}_2$. Moreover, the Galois closure $F = \mathbb{Q}(E)$ of f has Galois group $\mathrm{S}_5 \subset \mathrm{Sp}_4(\mathbb{F}_2)$.

Let K be the pair-resolvant of F and P the unique prime of K above 2. If there is at most one quadratic extension of K of modulus $P^4 \cdot \infty$ but none of modulus $P^2 \cdot \infty$, then we say that F is amiable.

Thm. 1: With A as above, assume $F = \mathbb{Q}(A[2])$ is amiable. Let B be an abelian variety of dimension $2d$ and conductor N^d, with $B[2]$ filtered by copies of $A[2]$. Then B is isogenous to A^d. In particular, F determines the isogeny class of A.

We know 3283 non-isogenous favorable abelian surfaces with $N < 10^7$. For 438 of the corresponding fields F_0 with N in

$$\{277, 349, 461, 797, 971, \ldots, 9929363, 9942437, 9957379\},$$

the assumptions of our theorem apply. In particular, there is exactly one isogeny class for those abelian surfaces.

Example. The theorem applies to the Jacobian of the following curve of conductor $N = 9957379$:

$$y^2 + y = x^5 - x^4 + 5x^3 + 4x^2 - x - 1.$$

KEY IDEAS INVOLVED IN MAIN THEOREM

More general statements and details are in our recent ArXiv preprint.

Def: Let $E = A[2]$ and $\underline{E}$ be the category of finite flat group schemes V over $\mathbb{Z}\left[\frac{1}{N}\right]$ satisfying the following properties:

E1. Each composition factor of V is isomorphic to E.

E2. If σ_v generates the inertia group at $v|N$, then $(\sigma_v - 1)^2$ annihilates V (Grothendieck semi-stability).

E3. The conductor exponent $\mathfrak{f}_N(V) = \mathfrak{f}_N(V^{ss}) = \text{mult}_E(V)$.

$\underline{E}$ is a full subcategory of the category of 2-primary group schemes over $\mathbb{Z}[\frac{1}{N}]$, closed under taking products, closed flat subgroup schemes and quotients by closed flat subgroup schemes. If B is isogenous to A^d, then subquotients of $B[p^r]$ are in $\underline{E}$. Thus, Thm.1 is a partial converse.

Let G be the 2-divisible group of A and H that of B. It suffices, by Faltings, to prove that $H \simeq G^d$. This follows from a very general result of Schoof, if we verify that the injection δ :

$$\mathbb{F}_2 = \mathrm{Hom}_{\mathbb{Z}[\frac{1}{N}]}(A[2], A[2]) \xrightarrow{\delta} \mathrm{Ext}^1_{\underline{E}}(A[2], A[2]),$$

induced by the cohomology sequence of

$$0 \to A[2] \to A[4] \to A[2] \to 0,$$

is an isomorphism of one-dimensional $\mathbb{F}_2$-vector spaces.

Because of the exact sequence

$$0 \to \mathrm{Ext}^1_{[2],\underline{E}}(E,\, E) \to \mathrm{Ext}^1_{\underline{E}}(E,\, E) \to \mathrm{End}_{\mathrm{Gal}}(E) = \mathbb{F}_2\,,$$

the bulk of our paper is devoted to a proof of

Thm. 2: F is amiable if and only if $\mathrm{Ext}^1_{[2],\underline{E}}(E,\, E) = 0$, that is extensions killed by 2 are split.

Ingredients: For study the extensions W of E by E in $\underline{E}$ and killed by 2, we need:

a) a complete classification of the possible Honda systems and their associated local group scheme extensions $W_{|\mathbb{Z}_2}$ over $\mathbb{Z}_2$. This leads to a conductor exponent bound of 4, for the abelian extension $\mathbb{Q}_2(W)/\mathbb{Q}_2(F_\lambda)$ with $\lambda|2$, an improvement over Fontaine's bound of 6;

b) the subgroups G of $\mathcal{P}(\mathsf{S}_5)$ available as possible images of the global representations of $G_{\mathbb{Q}}$ on W. If σ generates inertia at $v|N$, then G is the normal closure of σ (conductor bound at 2) and $\text{rank}(\sigma - 1) = 2$ (because of **E3**);

c) a comparison of the local and global structures of W.

When base-changed to $\mathbb{Q}_2$, the Galois representations of $G_{\mathbb{Q}_2}$

must agree by Schoof's Mayer-Vietoris sequence:

$$\begin{array}{l} \text{Hom}_{\mathbb{Q}_p}(V_1,V_2) \leftarrow \text{Hom}_{\mathbb{Z}_p}(V_1,V_2) \times \text{Hom}_{R'}(V_1,V_2) \leftarrow \text{Hom}_R(V_1,V_2) \leftarrow 0 \\ \quad \delta \downarrow \\ \text{Ext}^1_R(V_1,V_2) \to \text{Ext}^1_{\mathbb{Z}_p}(V_1,V_2) \times \text{Ext}^1_{R'}(V_1,V_2) \to \text{Ext}^1_{\mathbb{Q}_p}(V_1,V_2), \end{array}$$

applied with $p = 2$, $V_i = E$, $R = \mathbb{Z}\left[\frac{1}{N}\right]$ and $R' = \mathbb{Z}\left[\frac{1}{pN}\right]$.