# Modularity of the Consani-Scholten Quintic

with an Appendix by José Burgos Gil and Ariel Pacetti

Luis Dieulefait [1], Ariel Pacetti[2] and Matthias Schütt[3, 4]

Received: June 22, 2010
Revised: May 23, 2012

Communicated by Don Blasius

Abstract. We prove that the Consani-Scholten quintic, a Calabi-Yau threefold over $\mathbb{Q}$, is Hilbert modular. For this, we refine several techniques known from the context of modular forms. Most notably, we extend the Faltings-Serre-Livné method to induced four-dimensional Galois representations over $\mathbb{Q}$. We also need a Sturm bound for Hilbert modular forms; this is developed in an appendix by José Burgos Gil and the second author.

2000 Mathematics Subject Classification: Primary: 11F41; Secondary: 11F80, 11G40, 14G10, 14J32
Keywords and Phrases: Consani-Scholten quintic, Hilbert modular form, Faltings–Serre–Livné method, Sturm bound

## 1 Introduction

The modularity conjecture for Calabi-Yau threefolds defined over $\mathbb{Q}$ is a particular instance of the Langlands correspondence. Given a Calabi-Yau threefold $X$ over $\mathbb{Q}$ we consider the compatible family of Galois representations $\rho_\ell$ of dimension, say, $n$, giving the action of $G_\mathbb{Q} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{H}^3(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$: the conjecture says that there should exist an automorphic form $\pi$ of $\mathrm{GL}_n$ such that $\ell$-adic Galois representations attached to $\pi$ are isomorphic to the representations $\rho_\ell$. This implies that the $L$-functions of $\pi$ and $\rho_\ell$ agree, at

[1] LD partially supported by MICINN grants MTM2009-07024 and MTM2012-33830 and by an ICREA Academia Research Prize.
[2] AP partially supported by CONICET PIP 2010-2012 and FonCyT BID-PICT 2010-0681.
[3] MS partially supported by DFG under grant Schu 2266/2-2 and by ERC through StG 279723 (SURFARI).
[4] JBG partially supported by grants MTM2009-14163-c02-01 and CSIC-2009501001.

least up to finitely many local factors. Observe that (according to Langlands functoriality) $\pi$ should be cuspidal if and only if the representations $\rho_\ell$ are absolutely irreducible.

The only case where the conjecture is known in general (among Calabi-Yau threefolds) is the rigid case, i.e., the case with $n = 2$. In this case modularity was established by the first author and Manoharmayum (cf. [DM03]) under some mild local conditions. These local assumptions are no longer required since it is known that modularity of all rigid Calabi-Yau threefolds defined over $\mathbb{Q}$ follows from Serre's conjecture and the later has recently been proved (cf. [KW09b], [KW09a]).

It was observed by Hulek and Verrill in [HV06] that the modularity result in [DM03] can be extended to show modularity of those Calabi-Yau threefolds such that the representations $\rho_\ell$ are (for every $\ell$) reducible and have 2-dimensional irreducible components. In fact, using Serre's conjecture, one can show that this is true even if reducibility occurs only after extending scalars, assuming that reducibility is a uniform property, i.e., independent of $\ell$ (this uniformity follows for instance from Tate's conjecture).

In this paper, we will prove modularity for a non-rigid Calabi-Yau threefold over $\mathbb{Q}$ such that the representations $\rho_\ell$ are absolutely irreducible. To our knowledge such an example has not been known before. We sketch the basic set-up:

In [CS01], Consani and Scholten consider a quintic threefold $\tilde{X}$ which we will review in section 3. It has good reduction outside the set $\{2, 3, 5\}$ and Hodge numbers:

$$h^{3,0} = 1 = h^{2,1}, \quad h^{2,0} = 0 = h^{1,0} \text{ and } h^{1,1} = 141.$$

In particular the third étale cohomology is four dimensional. If we fix a prime $\ell$, the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the third étale cohomology gives a 4-dimensional representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(\mathrm{H}^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)) \simeq \mathrm{GL}_4(\mathbb{Q}_\ell).$$

Let $F = \mathbb{Q}[\sqrt{5}]$ and $\mathcal{O}_F$ its ring of integers. In [CS01] it is shown that the restriction

$$\rho_\ell|_{\mathrm{Gal}(\bar{\mathbb{Q}}/F)} : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{Aut}\left(\mathrm{H}^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) \otimes \overline{\mathbb{Q}_\ell}\right),$$

is the direct sum of two 2-dimensional representations (see Theorem 3.2 of [CS01]). More precisely, if $\lambda$ is a prime of $\mathcal{O}_F$ over $\ell$, then there exists a 2-dimensional representation

$$\sigma_\lambda : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathcal{O}_\lambda),$$

such that $\rho_\ell|_{\mathrm{Gal}(\bar{\mathbb{Q}}/F)}$ is a direct sum of $\sigma_\lambda$ and $\sigma'_\lambda$ (the external conjugate of $\sigma_\lambda$) and $\rho_\ell = \mathrm{Ind}_F^{\mathbb{Q}} \sigma_\lambda$.

In the same work, an holomorphic Hilbert newform $\mathfrak{f}$ on $F$ of weight $(2,4)$ and level $\mathfrak{c}_{\mathfrak{f}} = (30)$ is constructed, whose $L$-series is conjectured to agree with that of $\sigma$. The aim of this work is to prove this modularity result.
Let $\lambda$ be a prime of $F$ over a rational prime $\ell$. Let $\mathcal{O}_\lambda$ denote the completion at $\lambda$ of $\mathcal{O}_F$. Since $\mathfrak{f}$ has $F$-rational eigenvalues, by the work of Taylor (see [Tay89]), there exists a two-dimensional continuous $\lambda$-adic Galois representation

$$\sigma_{\mathfrak{f},\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathcal{O}_\lambda),$$

with the following properties: $\sigma_{\mathfrak{f},\lambda}$ is unramified outside $\ell\mathfrak{c}$, and if $\mathfrak{p}$ is a prime of $F$ not dividing $\ell\mathfrak{c}$, then

$$\begin{aligned} \operatorname{Tr} \sigma_{\mathfrak{f},\lambda}(\operatorname{Frob} \mathfrak{p}) &= \theta(T_{\mathfrak{p}}), \\ \det \sigma_{\mathfrak{f},\lambda}(\operatorname{Frob} \mathfrak{p}) &= \theta(S_{\mathfrak{p}})\mathcal{N}\,\mathfrak{p}. \end{aligned}$$

Here $T_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-th Hecke operator, $S_{\mathfrak{p}}$ denotes the diamond operator (given by the action of the matrix $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$, for $\alpha = \prod_{\mathfrak{p}} \pi_{\mathfrak{q}}^{v_{\mathfrak{q}}(\mathfrak{p})}$ and $\pi_{\mathfrak{q}}$ a local uniformizer) and $\theta(T)$ is the eigenvalue of the Hecke operator $T$ on $\mathfrak{f}$. Let $\tau(\mathfrak{f})$ be the Hilbert modular form which is the external Galois conjugate of $\mathfrak{f}$, where $\tau$ is the order two element in $\mathrm{Gal}(F/\mathbb{Q})$. Observe that the $\lambda$-adic Galois representations attached to $\tau(\mathfrak{f})$ are obtained by applying $\tau$ to the traces of the images of Frobenius in the ones attached to $\mathfrak{f}$. Our result can be stated as:

Theorem 1.1. *The representations $\sigma_\lambda$ and $\sigma_{\nu(\mathfrak{f}),\lambda}$ are isomorphic, where $\nu$ is either the identity or $\tau$.*

In particular the theorem implies that the $L$-series of $\sigma_\lambda$ and $\sigma_{\nu(\mathfrak{f}),\lambda}$ agree. This solves the conjecture from [CS01].

*Remark* 1.2. By known cases of automorphic base change (theta lift) and functoriality, Theorem 1.1 is known to imply that $\rho_\ell$ corresponds to a Siegel modular form of genus 2 and to a cuspidal automorphic form of $\mathrm{GL}_4$.

*Remark* 1.3. Dimitrov has proved a Modularity Lifting Theorem that applies to Hilbert modular forms of non-parallel weight (cf. [Dim09]), and he and the first author checked that for $\ell = 7$ the representation $\sigma$ satisfies all the technical conditions of this theorem (cf. [DD06]). Thus it would be enough to prove residual modularity modulo 7 to deduce the modularity of $\sigma$ from this result. We will follow, however, a different path.

We give an outline of the proof of Theorem 1.1. Since both Galois representations come in compatible families, it is enough to prove that they are isomorphic for a specific choice of primes $\lambda$ over $\ell$. We choose $\ell = 2$ so as to apply a Faltings-Serre method of proving that two given 2-adic Galois representations are isomorphic (cf. [Liv87]). Actually, in [CS01] it is proven that $\sigma_\lambda$ exists, but its trace at a prime is only determined up to conjugation by $\tau$. Hence in Theorem 4.3 we give a version of the Faltings-Serre method that applies to reducible 4-dimensional representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$.

Theorem 4.3 implies that the 2-dimensional Galois representations $\sigma_\lambda, \sigma_{\nu(\mathfrak{f}),\lambda}$ have isomorphic semisimplifications. Since $\mathfrak{f}$ is a cuspidal Hilbert eigenform, its $\lambda$-adic Galois representations is irreducible for all primes $\lambda$ and Livné's Theorem asserts in particular that the same is true for the representations attached to $\tilde{X}$. Thus we deduce Theorem 1.1.

In the present situation, the problem is non-trivial notably because 2 is inert in $\mathcal{O}_F$. Hence the residual representations lie a priori in $\mathrm{GL}_2(\mathbb{F}_4)$. Actually, they lie in $\mathrm{SL}_2(\mathbb{F}_4)$. This is clear for both representations: the representation $\sigma_{\mathfrak{f},\lambda}$ has trivial nebentypus so the determinant image lies in $\mathbb{F}_2^\times$ while the representation $\sigma_\lambda$ at a prime ideal $\mathfrak{p}$ has real determinant of absolute value $\mathcal{N}\mathfrak{p}^3$.
The group $\mathrm{SL}_2(\mathbb{F}_4)$ is not a solvable group (it is in fact isomorphic to $A_5$, the alternating group in 5 elements). We will overcome this subtlety by showing that the images of the residual representations are 2-groups. For $\sigma_{\mathfrak{f},2}$, this will be achieved in section 2 by combining three techniques: the theory of congruences between Hilbert cuspforms, the explicit approach from [DGP10] and a Sturm bound for Hilbert modular forms that is developed by Burgos and the second author in the Appendix B. For $\sigma_2$, we will use the Lefschetz trace formula and automorphisms on the Calabi-Yau threefold $\tilde{X}$ (section 3). We collect the necessary data for a proof of Theorem 1.1 in section 4.

Acknowledgements: We would like to thank Lassina Démbelé for many suggestions concerning computing with Hilbert modular forms. Also we would like to thank José Burgos Gil for his contribution to the appendix with the proof of a Sturm bound. The computations of the $a_\mathfrak{p}$ where done using the Pari/GP system [PAR08]. We would like to thank Bill Allombert for implementing a routine in PARI that was not included in the original software for dealing with elements of small norm under a positive definite quadratic form. Special thanks are due to the referee for his comments and suggestions.

## 2 Computing the residual image of the Galois representation $\sigma_{\mathfrak{f},2}$

This section deals with the holomorphic Hilbert newform $\mathfrak{f}$ on $F = \mathbb{Q}(\sqrt{5})$ of weight $(2,4)$ and conductor $\mathfrak{c}_\mathfrak{f} = (30)$ constructed in [CS01]. The aim of this section is to prove that the image of the residual 2-adic Galois representation $\bar{\sigma}_{\mathfrak{f},2}$ attached to $\mathfrak{f}$ has image a 2-group. This will enable us to apply methods for even trace Galois representations to $\sigma_{\mathfrak{f},2}$.

### 2.1 Properties of the Hilbert modular form $\mathfrak{f}$.

Let us recall some definitions of Hilbert modular forms. For $\mathfrak{c} \subset \mathcal{O}_F$, let $\Gamma_0(\mathfrak{c})$ be the subgroup of $\mathrm{SL}_2(\mathcal{O}_F)$ whose second row and first column entry is divisible by $\mathfrak{c}$. Let $\mathfrak{H}$ denote the Poincare upper half plane. Then given $\vec{k} = (k_1, k_2)$, with $k_1 \equiv k_2 \pmod 2$, a weight $\vec{k}$ Hilbert modular form of level $\mathfrak{c}$ is an holomorphic function $f : \mathfrak{H}^2 \mapsto \mathbb{C}$ such that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{c})$,

$$f(\gamma \cdot z_1, \tau(\gamma) \cdot z_2) = f(z_1, z_2)(cz_1 + d)^{k_1}(\tau(c)z_2 + \tau(d))^{k_2},$$

with the usual holomorphicity condition at the cusps. We denote such space $M_{\vec{k}}(\mathfrak{c})$, and $S_{\vec{k}}(\mathfrak{c})$ the subspace of cuspidal forms.
We start studying some properties of the form $\mathfrak{f}$. In sections 6 and 7 of [CS01] such form was constructed using Eichler's method on definite quaternion algebras and in Theorem 8.3 of loc. cit. it is proved that its coefficient field is exactly $\mathbb{Q}(\sqrt{5})$.
Since the primes 2 and 3 divide the level of the form $\mathfrak{f}$ to the first power, the automorphic representation attached to $\mathfrak{f}$ is Steinberg at both primes. To know its behaviour at the prime $\sqrt{5}$, we consider its twist by a suitable character.

Lemma 2.1. *There exists a unique non-trivial quadratic Hecke character $\chi_{\sqrt{5}}$ of $\mathcal{O}_F$ (of infinity type* (sign, sign)*), whose conductor is $\sqrt{5}$. The quadratic twist of $\mathfrak{f}$ by $\chi_{\sqrt{5}}$ corresponds to a Hilbert newform of level $6\sqrt{5}$ and weight* $(2,4)$ *which we denote by $\mathfrak{f}\otimes\chi_{\sqrt{5}}$.*

*Proof.* For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, whose residue field has prime order $p$, we can consider the quotient map

$$\mathcal{O}_F \twoheadrightarrow \mathcal{O}_F/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z},$$

to get a Dirichlet character $\chi_{\mathfrak{p}}$ in $\mathcal{O}_F$. To get the Hecke character we just need the infinity characters, but note that the infinite type $(\mathrm{sign}^{\epsilon_1}, \mathrm{sign}^{\epsilon_2})$ is uniquely defined by the conditions

$$\begin{aligned} \chi_{\mathfrak{p}}(-1) &= (-1)^{\epsilon_1+\epsilon_2}, \\ \chi_{\mathfrak{p}}\left(\frac{1+\sqrt{5}}{2}\right) &= (-1)^{\epsilon_2}. \end{aligned}$$

The uniqueness comes from the fact that the fundamental unit is not totally positive (which is equivalent to say that the class number and the narrow class number are the same). In our case, $\chi_{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right) = -1$, and $\chi_{\sqrt{5}}(-1) = 1$ so the first assertion follows.
For the second statement of the Lemma, it is clear (as in the classical case) that the twist will have trivial character and level at most 30 (see for example [Shi78, Proposition 4.4]), so the proof goes by elimination. The data used was supplied by Lassina Démbelé, but is now available in the new versions of MAGMA for example. Here is a resume:

- The space $S_{(2,4)}(30)$ is of dimension 74.
- Its subspace of newforms is of dimension 22.
- There are 16 eigenforms in the new subspace whose coefficient field is $F$ and 2 eigenforms whose coefficient field has degree 3 over it.
- The space $S_{(2,4)}(6\sqrt{5})$ is of dimension 14.

- Its subspace of newforms is of dimension 4.
- There are 4 eigenforms in the new subspace whose coefficient field is $F$.

By computing the Hecke eigenvalue at the primes above 11 in the newspace of level 30, we find a unique form matching the eigenvalue of $\mathfrak{f}$ (in version 2.16 of Magma, the form is the first one to appear), so the form $\mathfrak{f}\otimes\chi_{\sqrt{5}}$ does not lie in the newspace of level 30. Since the primes of norm 11 are generated by $\frac{7+\sqrt{5}}{2}$ and $\frac{7-\sqrt{5}}{2}$, and $\chi_{\sqrt{5}}\left(\frac{7+\sqrt{5}}{2}\right)=1$, we search for a form with the same eigenvalue in level $6\sqrt{5}$ and find a unique one (the third one), but none in level 6, hence $\mathfrak{f}\otimes\chi_{\sqrt{5}}$ has level $6\sqrt{5}$. □

This implies the following.

Corollary 2.2. *The form $\mathfrak{f}$ is also Steinberg at the prime $\sqrt{5}$.*

Since the form $\mathfrak{f}$ and $\mathfrak{f}\otimes\sqrt{5}$ are congruent modulo 2, we can work with the latter form which has smaller level.

## 2.2 Properties of the residual image of $\sigma_{\mathfrak{f},2}$

For reasons that will become clear later, we consider not the form $\mathfrak{f}$ but a form congruent to it modulo 2 and of parallel weight 2.

Lemma 2.3. *If the residual image of $\sigma_{\mathfrak{f},2}$ is irreducible, then there exists a Hilbert newform $\mathfrak{g}$ of level $12\sqrt{5}$ and parallel weight 2 which is congruent to $\mathfrak{f}$ modulo 2.*

*Proof.* This follows from results on the determination of Serre's weights, for example from [BDJ10], Corollary 2.12. In fact, item (2) of this corollary gives the sought for congruence, except for the fact that the value of the maximal power of 2 in the level of the Hilbert modular form of parallel weight 2, which is 4, follows from a close inspection of the proof of this corollary but is not given in the statement of item (2) (compare also with [BDJ10], Prop. 4.13 (a)).
Since the value of the power of 2 is not specified in item (2), let us prove that this value is correct using item (3) of Corollary 2.12. The reader is warned that in doing this we are following a rather indirect path, because we are twisting by a character and then twisting back by its inverse, so from the conceptual point of view this is very unnatural: we just follow this path in order to show that the result we want follows immediately from a case covered by Corollary 2.12 as it is, but a direct and natural proof could be obtained by a detailed explanation of how this power of 2 in the level can be determined DIRECTLY using the techniques in [BDJ10].
This being said, we apply Corollary 2.12 (3) in loc. cit. and obtain a Hilbert modular form $\mathfrak{g}'$ of parallel weight 2 congruent modulo 2 to a twist by some character $\mu$ of $\mathfrak{f}\otimes\chi_{\sqrt{5}}$ such that the level at 2 of $\mathfrak{g}'$ is 2. The level at 3 and at $\sqrt{5}$ of this form are the same as those of $\mathfrak{f}\otimes\chi_{\sqrt{5}}$, but it can have some extra primes

in the level, due to the fact that the global character $\mu$ whose local behaviour at 2 is prescribed in such a way that it changes the weight as desired, is only known to exist after allowing ramification at some auxiliary primes. From this congruence, we simply twist both sides by the inverse of $\mu$ and obtain what we wanted, the sought for form of parallel weight 2 is $\mathfrak{g} = \mathfrak{g}' \otimes \mu^{-1}$, which is easily seen to satisfy all the required properties: Notably it is congruent modulo 2 to $\mathfrak{f} \otimes \chi_{\sqrt{5}}$, and its level only contains the primes 2, 3 and $\sqrt{5}$ because the auxiliary primes introduced to the level while twisting by $\mu$ are removed after twisting by its inverse. In order to bound the level at 2 of $\mathfrak{g}$ recall that the level of $\mathfrak{g}'$ at 2 is 2 and apply the well-known formula for the behaviour of levels under twists. As final ingredient observe that the conductor at 2 of $\mu$ is just 2 because the order of this character is odd (it takes values on the multiplicative group of a finite field of characteristic 2) and 2 is inert in the quadratic field $\mathbb{Q}(\sqrt{5})$ (thus a character of conductor 2 has order 3 while a character whose conductor at 2 is at least 4 has even order). $\square$

For proving that the image of the residual 2-adic Galois representation attached to $\mathfrak{g}$ has image a 2-group, eventually we will pursue a similar approach as in [DGP10]. We start by computing all subgroups of $A_5$.

Lemma 2.4. *Any proper subgroup of $A_5$ is isomorphic to one of the following:*

$$\{\{1\}, C_2, C_3, C_2 \times C_2, C_5, S_3, D_5, A_4\}.$$

There is an easy classification of the orders of the elements in $\mathrm{SL}_2(\mathbb{F}_4)$ in terms of the traces.

Lemma 2.5. *If $M \in \mathrm{SL}_2(\mathbb{F}_4)$, then*

$$\mathit{ord}(M) = \begin{cases} 1 & \text{if } M = \mathrm{id}, \\ 2 & \text{if } \mathrm{Tr}(M) = 0 \text{ and } M \neq \mathrm{id}, \\ 3 & \text{if } \mathrm{Tr}(M) = 1, \\ 5 & \text{if } \mathrm{Tr}(M) \notin \mathbb{F}_2. \end{cases}$$

Recall how to derive a Fourier expansion at $\infty$ for a Hilbert modular form over $F$. Let $\tau$ denote the generator of $\mathrm{Gal}(F/\mathbb{Q})$. An element $\nu \in F$ is called totally positive if both $\nu > 0$ and $\tau(\nu) > 0$. We denote this by $\nu \gg 0$. Since $F$ has strict class number one, any Hilbert modular form $G$ over $F$ has a $q$-expansion

$$G(z_1, z_2) = \sum_{\substack{\xi \in \frac{\mathcal{O}_F}{\sqrt{5}} \\ \xi \gg 0}} \exp(\xi z_1 + \tau(\xi) z_2), \tag{1}$$

where $\exp(z) = e^{2\pi i z}$.
Recall that $\mathrm{Aut}(\mathbb{C})$ acts on the space of Hilbert modular forms, just by acting on Fourier expansions. The following result is due to Shimura (see Proposition 1.2 of [Shi78]).

Proposition 2.6. *Let $\sigma \in \operatorname{Aut}(\mathbb{C})$, then $\sigma(M_{\vec{k}}) = M_{\vec{l}}$, where $\vec{l} = \vec{k}^\sigma$.*

In particular, for parallel weight $\vec{k}$, we have $\sigma(M_{\vec{k}}) = M_{\vec{k}}$ for all $\sigma \in \operatorname{Aut}(\mathbb{C})$. This applies to the Hilbert modular form $\mathfrak{g}$ and thus indirectly to $\mathfrak{f}$:

Proposition 2.7. *The residual image of $\sigma_{\mathfrak{f},2}$ is not $D_5$ nor $A_5$.*

*Proof.* Suppose the residual image of $\sigma_{\mathfrak{f},2}$ is $D_5$ or $A_5$. In particular it is absolutely irreducible and Lemma 2.3 implies the existence of a parallel weight 2 form $\mathfrak{g}$ whose residual image (at 2) equals that of $\mathfrak{f}$. Let $L$ be denote the coefficient field of $\mathfrak{g}$ and $M$ its Galois closure. Due to the assumption on the coefficients of $\mathfrak{f}$ and the definition of $\mathfrak{g}$, we know that the residue field of (the ring of integers of) $L$ modulo some prime ideal $\hat{2}$ dividing 2 equals $\mathbb{F}_4$.
The groups $D_5$ and $A_5$ both have order 5 elements, so by Lemma 2.5 there exists a prime $\mathfrak{p}_0$ such that the $\mathfrak{p}_0$-th Hecke eigenvalue $a_{\mathfrak{p}_0}$ of $\mathfrak{g}$ lies in $\mathbb{F}_4$, but not in $\mathbb{F}_2$. Consider the form $\mathfrak{g} + \mu(\mathfrak{g})$, where $\mu$ is an element of $\operatorname{Gal}(M/\mathbb{Q})$ lying in the decomposition group of a prime above $\hat{2}$ and such that it lifts a generator of $\operatorname{Gal}(\mathbb{F}_4/\mathbb{F}_2)$. It is a parallel weight 2 Hilbert modular form (by Proposition 2.6), whose $\mathfrak{p}_0$-th Fourier coefficient is non-zero modulo 2.
We computed all Hecke eigenvalues with ideals generated by an element of trace smaller than 395 of $\mathfrak{f}$ and checked that they all lie in $2\mathcal{O}_F$ (a table for such eigenvalues can be found at [DPS]). In particular, all the Fourier coefficients of the Hilbert modular form $\mathfrak{g} + \mu(\mathfrak{g})$ with trace smaller than 395 are zero modulo the ideal $\hat{2}$, so the Sturm bound (Theorem B.21) implies that all Fourier coefficients of $\mathfrak{g} + \mu(\mathfrak{g})$ are zero modulo $\hat{2}$, which contradicts the fact that its $\mathfrak{p}_0$-th coefficient is not. □

It remains to prove that the residual image at 2 cannot be any of the groups $\{C_3, C_5, S_3, A_4\}$. We recall some well known results from Class Field Theory:

Theorem 2.8. *If $L/F$ be an abelian Galois extension unramified outside the set of places $\{\mathfrak{p}_i\}_{i=1}^n$ then there exists a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ such that $\operatorname{Gal}(L/F)$ corresponds to a subgroup of the ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$.*

A bound for $e(\mathfrak{p})$ is given by the following result.

Proposition 2.9. *Let $L/F$ be an abelian Galois extension of prime degree $p$. Consider a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ associated to the extension $L/F$ by Theorem 2.8. If $\mathfrak{p}$ ramifies in $L/F$, then*

$$\begin{cases} e(\mathfrak{p}) = 1 & \text{if } \mathfrak{p} \nmid p \\ 2 \leq e(\mathfrak{p}) \leq \left\lfloor \frac{pe(\mathfrak{p}|p)}{p-1} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid p, \end{cases}$$

*where $\mathfrak{p}$ is a prime above the rational prime $p$ and $e(\mathfrak{p}|p)$ is the ramification index of $\mathfrak{p}$ in $F/\mathbb{Q}$.*

*Proof.* See [Coh00] Proposition 3.3.21 and Proposition 3.3.22. □

Using these two results, we can compute for each possible Galois group all Galois extensions of $F$ unramified outside $\{2,3,5\}$. In each extension, we find a prime $\mathfrak{p}$ where the Frobenius has non-zero trace (in $\mathbb{F}_4$). If $a_{\mathfrak{p}} \equiv 0 \pmod 2$, for all such primes we are done:

PROPOSITION 2.10. *The residual representation $\bar{\sigma}_{\mathfrak{f},2}$ has image a 2-group.*

*Proof.* Consider the different cases:

• The group $A_4$ has $C_2 \times C_2$ as a normal subgroup (with generators (12)(34) and (13)(24)). The quotient by this subgroup is a cyclic group of order 3, so the extension contains a cubic Galois subfield. Since there are no elements of order 6 in $A_4$, a non trivial element in this Galois group will have odd trace. Thus the case $A_4$ and $C_3$ can be discarded at the same time.
In order to do so, we can take $\mathfrak{m} = 2 \cdot 3^2 \cdot \sqrt{5}$ as the maximal modulus by Proposition 2.10. The ray class group $Cl(\mathcal{O}_F, \mathfrak{m})$ is isomorphic to $C_{12} \times C_6$ so there are 4 cubic extensions ramified at these primes. We consider the characters as additive characters (by taking logarithms), and denote by $\psi_1$ and $\psi_2$ two characters that generate the group of characters of order 3 (we take the fourth and the second power of the characters in the previous basis). Instead of computing a prime ideal where each character is non-zero, we compute two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that

$$\langle (\psi_1(\mathfrak{p}_1), \psi_2(\mathfrak{p}_1)), (\psi_1(\mathfrak{p}_2), \psi_2(\mathfrak{p}_2)) \rangle = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Then Proposition 5.4 of [DGP10] implies that any cubic character is non-trivial in one of these two ideals. The two ideals above the prime 11 have values $(1,0)$ and $(1,2)$, which is a basis for $\mathbb{F}_3 \times \mathbb{F}_3$. Since the modular form has even traces (in $\mathbb{F}_2$) at both primes (see Table of [CS01]), we conclude that the residual representation cannot have image isomorphic to $C_3$ nor $A_4$.

• To discard the $C_5$ case, we take $\mathfrak{m} = 2 \cdot 3 \cdot (\sqrt{5})^3$. The ray class group for this module is cyclic of order 10. The generator at primes above 11 has value 9, in particular the order 5 characters do not vanish at this primes. But the trace of Frobenius lies in $\mathbb{F}_2$ at these primes (as mentioned in the previous case), so the image cannot be cyclic of order 5.

• To discard the $S_3$ case, we start by computing all the quadratic extensions of $F$ ramified outside the set of primes $\{2,3,5\}$. The modulus in this case is $\mathfrak{m} = 2^3 \cdot 3 \cdot \sqrt{5}$. The ray class group is isomorphic to $C_4 \times C_4 \times C_2 \times C_2 \times C_2$ so there are 31 such extensions. In Table 2.1 we put all the information of these extensions; the first column has an equation for each such extension, the second column its discriminant over $\mathbb{Q}$, the third column the modulus considered (where by $\mathfrak{p}_2$ (respectively $\mathfrak{p}_5$) we denote the unique prime ideal in the extension above the rational prime 2 (respectively 5)), the fourth column the ray class group and the last column the rational primes whose prime divisors in $F$ generate the $\mathbb{F}_3$ vector space of cubic characters.

| Equation over $F$ | Disc. over $\mathbb{Q}$ | Modulus | Ray Class Group | Rational Primes |
|---:|---:|---:|---:|---:|
| $x^2-6\sqrt{5}$ | $-2^6\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{72}\times C_6\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2+6\sqrt{5}$ | $-2^6\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{72}\times C_6\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2+\sqrt{5}+1$ | $-2^6\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_3$ | $\{7,11,13,19\}$ |
| $x^2-\sqrt{5}-1$ | $-2^6\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_3$ | $\{7,11,13,19\}$ |
| $x^2-3\sqrt{5}-3$ | $-2^6\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{36}\times C_6\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2+3\sqrt{5}+3$ | $-2^6\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{36}\times C_6\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2+2\sqrt{5}$ | $-2^6\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2-2\sqrt{5}$ | $-2^6\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2+\frac{3}{2}\sqrt{5}+\frac{3}{2}$ | $-2^4\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{36}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2-\frac{3}{2}\sqrt{5}-\frac{3}{2}$ | $-2^4\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{36}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2-\sqrt{5}$ | $-2^4\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2+\sqrt{5}$ | $-2^4\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2+3\sqrt{5}$ | $-2^4\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2-3\sqrt{5}$ | $-2^4\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{24}\times C_6\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2-\frac{1}{2}\sqrt{5}-\frac{1}{2}$ | $-2^4\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2+\frac{1}{2}\sqrt{5}+\frac{1}{2}$ | $-2^4\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2+\sqrt{5}+5$ | $2^6\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{60}\times C_6\times C_3\times C_3$ | $\{7,11,13,23\}$ |
| $x^2-6$ | $2^6\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_6$ | $\{7,11,13,23\}$ |
| $x^2+2$ | $2^6\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{24}\times C_{12}\times C_3\times C_3\times C_3$ | $\{7,11,13,23\}$ |
| $x^2-3\sqrt{5}-15$ | $2^6\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{12}\times C_6$ | $\{7,11,13\}$ |
| $x^2+6$ | $2^6\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{72}\times C_{12}\times C_3\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2-\sqrt{5}-5$ | $2^6\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{36}\times C_{18}\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2+3\sqrt{5}+15$ | $2^6\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{12}\times C_6\times C_6$ | $\{7,11,13,61\}$ |
| $x^2-2$ | $2^6\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{36}\times C_{18}\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2+\frac{3}{2}\sqrt{5}+\frac{15}{2}$ | $2^4\cdot 3^2\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{36}\times C_{18}\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2+3$ | $3^2\cdot 5^2$ | $18\cdot\sqrt{5}$ | $C_{36}\times C_3\times C_3\times C_3\times C_3\times C_3$ | $\{7,11,13,17,19,23\}$ |
| $x^2+1$ | $2^4\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{24}\times C_{12}\times C_3\times C_3$ | $\{7,11,13,17\}$ |
| $x^2+\frac{1}{2}\sqrt{5}+\frac{5}{2}$ | $5^3$ | $18\cdot\mathfrak{p}_5$ | $C_{60}\times C_3\times C_3\times C_3$ | $\{7,11,13\}$ |
| $x^2-\frac{1}{2}\sqrt{5}-\frac{5}{2}$ | $2^4\cdot 5^3$ | $9\cdot\mathfrak{p}_2\cdot\mathfrak{p}_5$ | $C_{12}\times C_6$ | $\{7,11,13\}$ |
| $x^2-3$ | $2^4\cdot 3^2\cdot 5^2$ | $9\cdot\mathfrak{p}_2\cdot\sqrt{5}$ | $C_{12}\times C_6\times C_6\times C_3$ | $\{7,11,13\}$ |
| $x^2-\frac{3}{2}\sqrt{5}-\frac{15}{2}$ | $3^2\cdot 5^3$ | $18\cdot\mathfrak{p}_5$ | $C_6\times C_6$ | $\{7,11,13\}$ |

Table 2.1: Quadratic extensions of $F$ unramified outside $\{2,3,5\}$

Note that the first 16 extensions are not Galois over $\mathbb{Q}$ and are listed so that they are isomorphic in pairs. The last 15 are indeed Galois over $\mathbb{Q}$. This implies that we could consider one element of each pair for the first fields. Note that the primes at conjugate fields are the same, since the Frobenius at a prime in $F$ of a field is the same as the Frobenius at the conjugate of the prime in the conjugate extension.
The traces of Frobenius are even in all such primes (see Table of [CS01]), so we conclude that the image of the residual representation $\bar{\sigma}_{\mathfrak{f},2}$ cannot be isomorphic to $S_3$ either. $\square$

## 3 Computing the residual image of the Galois representation $\sigma_2$

In this section we consider the Consani-Scholten quintic $\tilde{X}$ from [CS01]. Our goal is to prove that the $\ell$-adic Galois representations $\rho$ of $\mathrm{H}^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ have 4-divisible trace. This will be used in 3.5 to deduce that modulo 2 the restricted 2-adic two-dimensional Galois representations have image in $\mathrm{SL}_2(\mathbb{F}_2)$, and in fact even trace, so that we can apply an adaptation of the Faltings-Serre-Livné method in order to prove Theorem 1.1.

### 3.1 Setup

Consider the Chebyshev polynomial

$$P(y,z) = (y^5 + z^5) - 5yz(y^2 + z^2) + 5yz(y+z) + 5(y^2+z^2) - 5(y+z).$$

Then we define an affine variety $X$ in $\mathbb{A}^4$ by

$$X: \quad P(x_1, x_2) = P(x_4, x_5).$$

Let $\bar{X} \subset \mathbb{P}^4$ denote the projective closure of $X$. Then $\bar{X}$ has 120 ordinary double points. Let $\tilde{X}$ denote a desingularisation obtained by blowing up $\bar{X}$ at the singularities.

*Remark* 3.1. We might also consider a small resolution $\hat{X}$, as many of the nodes lie on products of lines. Then we would have to check that $\hat{X}$ is projective and can be defined over $\mathbb{Q}$. This desingularisation would have the advantage of producing an honest Calabi-Yau threefold, but it does not affect the question of Hilbert modularity.

Consani and Scholten compute the Hodge diamond of $\tilde{X}$ as follows:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 0 & & 0 & & \\ & 0 & & 141 & & 0 & \\ 1 & & 1 & & 1 & & 1 \\ & 0 & & 141 & & 0 & \\ & & 0 & & 0 & & \\ & & & 1 & & & \end{array}$$

Hence the étale cohomology groups $\mathrm{H}^3(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ ($\ell$ prime) give rise to a compatible system of four-dimensional Galois representations $\{\rho_\ell\}$. Since $\tilde{X}$ has good reduction outside $\{2,3,5\}$, $\rho_\ell$ is unramified outside $\{2,3,5,\ell\}$.
Let $F = \mathbb{Q}(\sqrt{5})$ and fix some prime $\ell \in \mathbb{N}$ and a prime $\lambda$ of $F$ above $\ell$. Then Consani and Scholten prove for the $\ell$- resp. $\lambda$-adic representations:

Theorem 3.2 (Consani-Scholten [CS01]). *The restriction $\rho|_{\mathrm{Gal}(\bar{\mathbb{Q}}/F)}$ is reducible as a representation into $\mathrm{GL}_4(F_\lambda)$: There is a Galois representation*

$$\sigma : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_2(F_\lambda)$$

*such that $\rho = \mathrm{Ind}_F^{\mathbb{Q}} \sigma$.*

The theorem implies in particular that internal and external conjugation have the same effect on $\sigma$. Here we want to prove the following property:

Proposition 3.3. *The Galois representation $\rho$ has 4-divisible trace, and so has any restriction to a finite extension of $\mathbb{Q}$. That is, $\rho(\mathrm{Frob}_q) \equiv 0 \mod 4$ for any odd prime power $q$.*

In fact, for $q \equiv 2, 3 \mod 5$, Consani-Scholten proved that $\rho(\mathrm{Frob}_q)$ has zero trace. Hence we would only have to consider the case $q \equiv 1, 4 \mod 5$, although we will treat the problem in full generality.
As a corollary, we will deduce that $\sigma$ is even in 3.5 as required for the proof of Theorem 1.1.

### 3.2 Lefschetz fixed point formula

Choose a prime $p \neq \ell$ of good reduction for $\tilde{X}$ and let $q = p^r$. Consider the geometric Frobenius endomorphism $\mathrm{Frob}_q$ on $\tilde{X}/\mathbb{F}_p$, raising coordinates to their $q$-th powers. Then the Lefschetz fixed point formula tells us that

$$\#\tilde{X}(\mathbb{F}_q) \quad = \quad \sum_{i=0}^{6} (-1)^i \,\mathrm{trace}\, \mathrm{Frob}_q^*(\mathrm{H}^i(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)).$$

In our situation, this simplifies as follows: $h^1 = h^5 = 0$; $\mathrm{H}^2(\tilde{X})$ and $\mathrm{H}^4(\tilde{X})$ are algebraic by virtue of the exponential sequence and Poincaré duality. Moreover $\mathrm{Frob}_q^*$ factors through a permutation on $\mathrm{H}^2(\tilde{X})$, i.e. all eigenvalues have the shape $\zeta q$ where $\zeta$ is some root of unity. Denote the sum of these roots of unity by $h_q$ (which is an integer in $\mathbb{Z}$ by the Weil conjectures). Finally geometric and algebraic Frobenius are compatible through $\rho$. Hence

$$t_q = \mathrm{trace}\, \rho(\mathrm{Frob}_q) = 1 + h_q\, q(1+q) + q^3 - \#\tilde{X}(\mathbb{F}_q). \tag{2}$$

Prop. 3.3 claims that the left hand side is divisible by 4. If $q \equiv -1 \mod 4$, this is a consequence of the following

Lemma 3.4. *For any good prime $p$ and $q = p^r$, $\#\tilde{X}(\mathbb{F}_q) \equiv 0 \mod 4$.*

If $q \equiv 1 \mod 4$, then we furthermore need the following

Lemma 3.5. *For any good prime $p$ and $q = p^r$, $h_q$ is odd.*

### 3.3 Proof of Lemma 3.4

To prove Lemma 3.4, we use the action of the dihedral group $D_4$ on $\tilde{X}$ and the knowledge about the exceptional divisors from Consani-Scholten.
Let $\zeta_n$ denote a primitive $n$-th root of unity. Then all the nodes are defined over $\mathbb{Q}(\zeta_{15})$. A detailed list can be found in [CS01]. Over the field of definition of the node, the exceptional divisor $E$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. Hence $\#E(\mathbb{F}_q) = (q+1)^2$ if the node is defined over $\mathbb{F}_q$.

Lemma 3.6. *For any good prime $p$ and $q = p^r$, $\#\tilde{X}(\mathbb{F}_q) \equiv \#\bar{X}(\mathbb{F}_q) \mod 32$.*

*Proof:* By [CS01], we have

$$\#\{\text{nodes over } \mathbb{F}_q\} = \begin{cases} 0, & q \equiv 2,7,8,13 \mod 15, \\ 8, & q \equiv 14 \mod 15, \\ 24, & q \equiv 4 \mod 15, \\ 104, & q \equiv 11 \mod 15, \\ 120, & q \equiv 1 \mod 15. \end{cases}$$

Since the number of points on the exceptional divisor is the same for all nodes defined over $\mathbb{F}_q$, the claim follows. □

Lemma 3.7. *For any good prime $p$ and $q = p^r$, $\#\bar{X}(\mathbb{F}_q) \equiv \#X(\mathbb{F}_q) - q \mod 4$.*

*Proof:* The affine variety $X$ is compactified by adding a smooth surface at $\infty$. In fact, this is the Fermat surface of degree five:

$$S = \{x_0^5 + x_1^5 - x_3^5 - x_4^5 = 0\} \subset \mathbb{P}^3.$$

Hence $\#\bar{X}(\mathbb{F}_q) - \#X(\mathbb{F}_q) = \#S(\mathbb{F}_q)$. Thus Lemma 3.7 amounts to the following

Lemma 3.8. *For $p \neq 5$ and $q = p^r$, $\#S(\mathbb{F}_q) \equiv 1 + q + q^2 \mod 4$.*

The proof of this lemma will be postponed to the end of this subsection. Lemma 3.7 follows. □

To prove the corresponding statement about the affine variety $X$, we use the action of the dihedral group $D_4$ generated by the involutions

$$(x_1, x_2, x_3, x_4) \mapsto (x_2, x_1, x_3, x_4), \quad (x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_4, x_3)$$

and by the cyclic permutation

$$\gamma : \quad (x_1, x_2, x_3, x_4) \mapsto (x_3, x_4, x_2, x_1). \tag{3}$$

It follows that

$$\#X(\mathbb{F}_q) \equiv \#\{x \in X(\mathbb{F}_q); \#\{y \in (D_4 - \text{orbit of } x)\} < 4\} \mod 4.$$

Here $\{x \in X(\mathbb{F}_q); \#\{y \in (D_4 - \text{orbit of } x)\} < 4\} = \{(x_1, x_1, x_3, x_3) \in X(\mathbb{F}_q)\}$. We are led to consider the affine curve $C$ in $\mathbb{A}^2$ defined by

$$C: \quad P(y, y) = P(z, z).$$

Then the above subset of $X(\mathbb{F}_q)$ is in bijection with $C(\mathbb{F}_q)$, and we obtain

$$\#X(\mathbb{F}_q) \equiv C(\mathbb{F}_q) \mod 4. \tag{4}$$

Lemma 3.9. *For any good prime $p$ and $q = p^r$, $\#C(\mathbb{F}_q) \equiv q \mod 4$.*

*Proof of Lemma 3.9:* $C$ is reducible. The change of variables

$$u = \frac{y+z}{2}, \quad v = \frac{y-z}{2}$$

allows us to write

$$\begin{aligned}P(y,y) - P(z,z) &= \\ &= v(v^4 + 5(2u^2 - 4u + 1)\, v^2 + 5(u^2 - 3u + 1)(u^2 - u - 1)) = v\, G(u, v).\end{aligned}$$

Hence

$$\#C(\mathbb{F}_q) = q + \#(B(\mathbb{F}_q) \cap \{v \neq 0\}) \tag{5}$$

where $B$ is the affine curve in $\mathbb{A}^2$ given by $G(u, v) = 0$. Here $B$ is endowed with involutions

$$(u, v) \mapsto (u, -v), \quad (u, v) \mapsto (2 - u, v).$$

For the number of points, this implies

$$\begin{aligned}\#(B(\mathbb{F}_q) \cap \{v \neq 0\}) &\equiv \#(B(\mathbb{F}_q) \cap \{u = 1, v \neq 0\}) \mod 4 \\ &= \#\{v \in \mathbb{F}_q; v^4 - 5v^2 + 5 = 0\}.\end{aligned}$$

The last polynomial factors as

$$4(v^4 - 5v^2 + 5) = (2v^2 - 5 - \sqrt{5})\,(2v^2 - 5 + \sqrt{5}).$$

Since $\frac{5+\sqrt{5}}{2} \cdot \frac{5-\sqrt{5}}{2} = 4$, a square, we deduce that the last equation has either zero or four solutions in $\mathbb{F}_q$. In particular, (5) reduces to $\#C(\mathbb{F}_q) \equiv q \mod 4$, i.e. to the claim of Lemma 3.9. □

*Proof of Lemma 3.8:* We shall again use the cyclic permutation $\gamma$ from (3), but this time it operates on the homogeneous coordinates of $\mathbb{P}^3$. Hence

$$\#S(\mathbb{F}_q) \equiv \#(S \cap \mathrm{Fix}(\sigma^2))(\mathbb{F}_q) \mod 4. \tag{6}$$

Here

$$\mathrm{Fix}(\sigma^2) = \{[\lambda, \mu, \pm\lambda, \pm\mu]; [\lambda, \mu] \in \mathbb{P}^1\}.$$

One of these lines is contained in $S$, and it is easy to see that there are exactly $(5, q-1)$ further points of intersection unless $p = 2$. I.e.

$$\#(S \cap \mathrm{Fix}(\sigma^2))(\mathbb{F}_q) = 1 + q + \begin{cases} 0, & p = 2 \\ (5, q-1), & p \neq 2 \end{cases} \equiv 1 + q + q^2 \mod 4.$$

Lemma 3.8 follows from this congruence and (6). □

*Proof of Lemma 3.4:* Lemma 3.9 and (4) imply that $\#X(\mathbb{F}_q) \equiv q \mod 4$. By Lemma 3.7 this gives $\#\bar{X}(\mathbb{F}_q) \equiv 0 \mod 4$. The according statement for $\tilde{X}$ is obtained from Lemma 3.6. □

## 3.4 Proof of Lemma 3.5

Lemma 3.5 states that the trace $h_q$ of $\mathrm{Frob}_q$ on $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ is always odd. We shall first prove the following auxiliary result:

Lemma 3.10. *The Galois group* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ *acts trivially on* $\mathrm{H}^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$.

*Proof:* Denote the exceptional locus of the blow-up by $E$. Then $E$ is defined over $\mathbb{Q}$. The Leray spectral sequence for the desingularisation gives an exact sequence

$$0 \to \mathrm{H}^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)) \to \mathrm{H}^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)) \to \mathrm{H}^2(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1)). \tag{7}$$

By construction, (7) is compatible with the Galois action. Here $\mathrm{H}^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ is the same as for a general quintic hypersurface in $\mathbb{P}^4$. Hence it has dimension one and is generated by the class of a hyperplane section. In particular, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts trivially on $\mathrm{H}^2(\bar{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. Recall that every component of $E$ as well as both rulings on every component are defined over $\mathbb{Q}(\zeta_{15})$. Hence $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ acts trivially on $\mathrm{H}^2(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. By the Galois-equivariant exact sequence (7), the same holds for $\mathrm{H}^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. □

It follows from Lemma 3.10, that $h_q = 141$ if $q \equiv 1 \mod 15$. The prove the parity for the other residue classes, we need two easy statements about sums of primitive roots of unity. They involve the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$:

$$\mu(n) = \begin{cases} 0, & \text{n not squarefree,} \\ (-1)^m, & \text{n squarefree with } m \text{ prime divisors.} \end{cases}$$

Lemma 3.11. *Let* $n \in \mathbb{N}$ *and* $\zeta_n$ *a primitive* $n$*-th root of unity. Then* $\zeta_n$ *has trace* $\mu(n)$.

The lemma follows immediately from the factorisation of the cyclotomic polynomial $x^n - 1$ and the definition of $\mu(n)$.

Lemma 3.12. *Let $n \in \mathbb{N}$ and $\zeta_n$ a primitive $n$-th root of unity. Let $m = 2^s \cdot k$ with $(k, n) = 1$. Then*

$$\mu(n) = \text{trace } \zeta_n = \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^j \equiv \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj} \mod 2.$$

*Proof:* If $(m, n) = 1$, then taking $m$-th powers permutes the primitive $n$-th roots of unity and both sums coincide. Hence it suffices to consider the case where $m = 2^s (s > 0)$ and $2|n$.
If $4 \nmid n$, then $\{\zeta_n^{mj}; j \in (\mathbb{Z}/n\mathbb{Z})^*\}$ is the set of $\frac{n}{2}$-th primitive roots of unity. Hence

$$\sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj} = \mu\left(\frac{n}{2}\right) = -\mu(n)$$

and the claim follows mod 2. If $4|n$, then $\mu(n) = 0$ and every element in $\{\zeta_n^{mj}; j \in (\mathbb{Z}/n\mathbb{Z})^*\}$ appears with multiplicity $(m, n)$. Hence

$$2 \mid (m, n) \mid \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^{mj},$$

and we obtain the claimed congruence. □

*Proof of Lemma 3.5:* Let $\Xi$ be the set of eigenvalues of $\text{Frob}_q$ on $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ with multiplicities. Then

$$h_q = \sum_{\zeta \in \Xi} \zeta.$$

Recall that the Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_{15}))$ acts trivially on $H^2(\tilde{X}_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. Since $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ is Galois of degree eight, we deduce that $\zeta^8 = 1$ for each $\zeta \in \Xi$. In particular

$$\sum_{\zeta \in \Xi} \zeta^8 = 141. \tag{8}$$

In the present situation, $h_q \in \mathbb{Z}$, i.e. $h_q$ is a sum of traces of elements in $\Xi$. Hence we can apply Lemma 3.12 to deduce that $h_q$ has the same parity as the sum in (8). That is, $h_q$ is odd. □

## 3.5 Evenness of $\sigma$

In this subsection we conclude our preparations for the proof of Theorem 1.1 by proving the following corollary of Proposition 3.3:

Corollary 3.13. *The Galois representation $\sigma$ is even.*

Recall that $\sigma$ induces the 4-dimensional Galois representation $\rho$ over $\mathbb{Q}$. The proof commences by spelling out the characteristic polynomial of $\rho(\text{Frob}_q)$ for some odd prime power $q$:

$$\mu_q(T) = T^4 - t_q T^3 + uT^2 - q^3 t_q T + q^6$$

with $u = (t_q^2 - t_{q^2})/2$ using the notation of (2). By Proposition 3.3, $t_q \equiv t_{q^2} \equiv 0 \mod 4$, so $u \equiv 0 \mod 2$.
Now we turn to $\sigma$, the 2-dimensional Galois representation with values in $F = \mathbb{Q}(\sqrt{5})$ inducing $\rho$. Let $\mathfrak{q}$ denote some power of a prime ideal in $F$ with odd norm $q \in \mathbb{Z}$. We write

$$s_{\mathfrak{q}} = \operatorname{Tr} \sigma(\operatorname{Frob}_{\mathfrak{q}})$$

and consider the case $s_{\mathfrak{q}} \notin \mathbb{Z}$. Then $s_{\mathfrak{q}} = a + b\omega$ where $\omega$ solves $v^2 - v - 1 = 0$ and $a, b \in \mathbb{Z}, b \neq 0$. By Theorem 3.2 we have

$$t_q = 2a + b.$$

Since $t_q$ is even by Proposition 3.3, so is $b$, and we can write somewhat more intuitively $s_{\mathfrak{q}} = c + d\sqrt{5}$ with $c, d \in \mathbb{Z}, d \neq 0$. This already implies that the mod 2-reduction of $\sigma$ has traces in $\mathbb{F}_2$, so it will have image in $\mathrm{SL}(2, \mathbb{F}_2)$.
In the new notation, we obtain

$$t_q = 2c,$$

so by Proposition 3.3 the input $c$ is even. But then, factoring $\mu_q(T)$ into quadratic factors over $F$ corresponding to $\sigma$ and its external conjugate, the coefficient of $T^2$ reads

$$u = (c^2 - 5d^2) + 2q^3.$$

Since we have already seen that $u$ and $c$ are even, we find that $d$ is even, too. That is, $\sigma$ has even trace at $\operatorname{Frob}_{\mathfrak{q}}$. The case $s_{\mathfrak{q}} \in \mathbb{Z}$ is essentially the same argument, but even simpler. □

## 4 Proof of the Main Theorem

There is version of the Faltings-Serre method in [Liv87] that allows to compare two-dimensional 2-adic Galois representations with even traces. Here we have to modify this approach slightly since the two-dimensional Galois representation $\sigma_2$ is only determined up to conjugation of its coefficients in the quadratic field $F$. While the original result involved the notion of non-cubic test sets, in order to prove Theorem 1.1, we replace this notion by non-quartic sets:

Definition. A subset $T$ of a finite dimensional vector space $V$ is *non-quartic* if every homogeneous polynomial of degree 4 on $V$ which vanishes on $T$, vanishes in the whole $V$.

The following lemma is useful to lower the cardinality of the test set $T$.

Lemma 4.1. *Let $V$ be a finite-dimensional vector space. Let $T$ be a subset of $V$ which contains 4 distinct hyperplanes through the origin and a point outside them. Then $T \setminus \{0\}$ is non-quartic.*

*Proof.* Let $L_1, \dots, L_4$ denote linear homogeneous polynomials giving equations of the four hyperplanes. Let $P(x_1, \dots, x_n)$ be a homogeneous quartic polynomial vanishing on all points of $T$. Division with remainder gives a representation

$$P(x_1, \dots, x_n) = L_1 Q(x_1, x_2, \dots, x_n) + P_2(x_1, \dots, x_n)$$

with $L_1 \nmid P_2$. The crucial property here is the following: Since $T$ contains the hyperplane $\{L_1 = 0\}$ and $P$ vanishes on this hyperplane, $P_2$ vanishes on all of $V$. (To see this, apply a linear transformation so that $L_1 = x_1$; then $P_2 = P_2(x_2, \dots, x_n)$, and $P_2$ vanishes on the hyperplane $\{x_1 = 0\}$ if and only if it vanishes on $V$). Since the hyperplanes are linearly independent, we can apply the same argument to the other three hyperplanes (starting with $L_1 Q$ instead of $P$). We obtain

$$P(x_1, \dots, x_n) = A \cdot L_1 L_2 L_3 L_4 + \tilde{P}(x_1, \dots, x_n),$$

where $A$ is a field constant and $\tilde{P}$ vanishes identically on $V$. Since $T$ contains a point outside the union of the four hyperplanes, $A$ must be zero.
But then $P = \tilde{P}$ vanishes on all of $V$. Since this argument applies to any homogeneous quartic polynomial $P$, the test set $T \setminus \{0\}$ is non-quartic. $\square$

*Remark* 4.2. Note that Lemma 4.1 does explicitly not require the hyperplanes to be linearly independent. It is immediate from the proof of Lemma 4.1 that the same argument works for test sets for homogeneous polynomials of degree $n$ if we find $n$ distinct hyperplanes through the origin and a point outside them.

We want to compare the two Galois representations, $\sigma_2$ and $\sigma_{\mathfrak{f},2}$. It is crucial that in the present situation we know that the external Galois conjugate representation exists: this follows in the geometric example by construction, and in the modular example we can consider the 2-adic representation attached to the conjugate Hilbert modular forms $\tau(\mathfrak{f})$, where $\tau$ is a generator of the group $\mathrm{Gal}(F/\mathbb{Q})$. For any given $\ell$-adic Galois representation $\rho$ with field of coefficients $F$ (i.e, the field generated by the traces of Frobenius elements is $F$) we will denote by $\rho'$ the external conjugate representation (if we know that such a representation exists). Since for the Calabi-Yau threefold $\tilde{X}$, we can only compute the traces of the 4-dimensional Galois representation $\sigma_2 \oplus \sigma_2'$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ (or actually of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$), we will need the following generalization of Theorem 4.3 in [Liv87] about Galois representations whose residual images are 2-groups:

Theorem 4.3. *Let $K$ be a global field, $S$ a finite set of primes of $K$ and $E$ the unramified quadratic extension of $\mathbb{Q}_2$. Denote by $K_S$ the compositum of all quadratic extensions of $K$ unramified outside $S$ and by $\mathscr{P}_2$ the maximal prime ideal of $\mathcal{O} := \mathcal{O}_E$. Suppose $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(E)$ are continuous representations, unramified outside $S$, and with field of coefficients $F$, and assume also that their external Galois conjugates exist. We suppose that the following conditions are satisfied:*

*1.* $\mathrm{Tr}(\rho_1) \equiv \mathrm{Tr}(\rho_2) \equiv 0 \pmod{\mathscr{P}_2}$ *and* $\det(\rho_1) \equiv \det(\rho_2) \equiv 1 \pmod{\mathscr{P}_2}$.

*2. There exists a set $T$ of primes of $K$, disjoint from $S$, for which*

*(i) The image of the set $\{\mathrm{Frob}_t\}_{t\in T}$ in $\mathrm{Gal}(K_S/K)\backslash\{0\}$ is non-quartic.*

*(ii)* $\mathrm{Tr}(\rho_1(\mathrm{Frob}_t)) + \mathrm{Tr}(\rho_1'(\mathrm{Frob}_t)) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_t)) + \mathrm{Tr}(\rho_2'(\mathrm{Frob}_t))$ *and* $\det(\rho_1(\mathrm{Frob}_t)) = \det(\rho_2(\mathrm{Frob}_t))$ *for all* $t \in T$.

*Then $\rho_1 \oplus \rho_1'$ and $\rho_2 \oplus \rho_2'$ have isomorphic semi-simplifications.*

*Proof.* This is just a slight generalization of Proposition 4.7 and Theorem 4.3 in [Liv87], we reproduce most of the arguments for the reader convenience, adapted to our situation.

Observe that due to assumption (1), and the fact that similar conditions hold also for $\rho_1'$ and $\rho_2'$, the image of any of the representations $\rho_1$, $\rho_1'$, $\rho_2$ and $\rho_2'$ is a pro-2-group. Let $G$ be the image of the product of the four representations. Then, $G$ is a topologically finitely generated pro-2-group and the four representations can be thought of (and we will do so for the rest of this proof) as representations of $G$, each being obtained from a suitable projection.

Set $M_2$ to be the algebra of 2 by 2 matrices with coefficients in $\mathcal{O}$. For $g \in G$, let $\rho : G \to M_2 \times M_2$ be the map:

$$\rho(g) = (\rho_1(g), \rho_2(g))$$

Keeping the notation in [Liv87], we call $\Sigma$ the subset of $G$ corresponding to $T$ (the projection of the elements in $\{\mathrm{Frob}_t\}_{t\in T}$ to $G$).

Let $M$ be the $\mathbb{Z}_2$-linear span of $\rho(G)$. Since $\mathcal{O}$ has rank 2 over $\mathbb{Z}_2$, $M$ is a subalgebra with unity of $M_2 \times M_2$ which is free of rank at most 16 as a module over $\mathbb{Z}_2$.

We consider $R = M/2M$, which is an $\mathbb{F}_2$-vector space of dimension at most 16. Denote the image of $g \in G$ in $R$ by $\bar{g}$. Set $\Gamma = \{\bar{g} \mid g \in G\}$. Then $\Gamma \subseteq R^\times$. $R$ is spanned as $\mathbb{F}_2$-vector space by $\Gamma$ and $\dim_{\mathbb{F}_2} R \leq 16$.

We will show the following:

Assertion: $R$ is spanned over $\mathbb{F}_2$ by $\{\bar{\sigma} \mid \sigma \in \Sigma \cup \{1\}\}$.

In order to do so, following [Liv87], we have first to prove that

$$\sigma \in \Sigma \Rightarrow \bar{\sigma}^2 = \bar{1} \text{ in } \Gamma. \tag{9}$$

Let $\sigma \in \Sigma$. Set $d = \det \rho_1(\sigma) = \det \rho_2(\sigma)$ (the last equality is due to assumption (2)(ii)) and $t_1 = \mathrm{Tr}\,\rho_1(\sigma)$, $t_2 = \mathrm{Tr}\,\rho_2(\sigma)$.

By the Cayley-Hamilton theorem (for 2 by 2 matrices) we have:

$$\rho(\sigma)^2 = (t_1\rho_1(g), t_2\rho_2(g)) - d(I, I)$$

in $M_2 \times M_2$, where $I$ is the 2 by 2 identity matrix.

Reducing modulo $\mathscr{P}_2$ this equality, since assumption (1) gives $t_1 \equiv t_2 \equiv 0 \pmod{\mathscr{P}_2}$ and $d \equiv 1 \pmod{\mathscr{P}_2}$ we obtain $\bar{\sigma}^2 = \bar{1}$ in $\Gamma$, and this is formula (9).

If we call $G^*$ the Frattini subgroup of $G$, and $\Gamma^*$ the one of $\Gamma$, since $G/G^* \to \Gamma/\Gamma^*$ is surjective, the image of $\Sigma$ in $\Gamma/\Gamma^*$ is non-quadratic (we use assumption (2)(i) and the fact that non-quartic easily implies non-quadratic). Then, by Lemma 4.5 in [Liv87] we see that formula (9) implies that $\Gamma^* = 1$ and hence $\Gamma \cong (\mathbb{Z}/2\mathbb{Z})^r$, for some $r$.
In particular, $\Gamma$ is commutative, and since $\Gamma$ spans $R$, $R$ is a commutative ring. Let $r \in R$ be any element and write $r = \sum_{\gamma\in\Gamma} k_\gamma \gamma$, with $k_\gamma \in \mathbb{F}_2$.
Then $r^2 = (\sum k_\gamma^2) \cdot \bar{1}$. Hence $r^2 = 0$ or else $r$ is invertible.
It follows that $R$ is a local artinian algebra over $\mathbb{F}_2$ with maximal ideal

$$P = \{r \in R \mid r^2 = 0\}$$

and $R/P = \mathbb{F}_2$. Let us now show that $P^5 = 0$. The proof of this fact goes as the one given in [Liv87], except that we consider now products of 5 elements $x_1, ..., x_5$ in $P$ (instead of 4 elements): assuming that their product is non-zero we derive a contradiction, as in [Liv87], by considering the $\mathbb{F}_2$-algebra

$$R_0 = \mathbb{F}_2[T_1, ..., T_5]/(T_1^2, ..., T_5^2)$$

and the injective map of $\mathbb{F}_2$-algebras from $R_0$ to $R$ that sends $T_i$ to $x_i$. The contradiction follows from the inequalities: $\dim_{\mathbb{F}_2} R_0 = 32 > 16 \geq \dim_{\mathbb{F}_2} R$.
Using the fact that $P^5 = 0$, the rest of the proof of the assertion follows as in [Liv87], changing "cubic polynomial" by "quartic polynomial", and "non-cubic" by "non-quartic".
The assertion being proved, we conclude as in [Liv87] from Nakayama's lemma that the $\mathbb{Z}_2$-span of $\{\rho(\sigma) \mid \sigma \in \Sigma \cup \{1\}\}$ is all of $M$ (recall that $M$ is the linear $\mathbb{Z}_2$-span of $\rho(G)$).
Here comes the only place where equality of the traces over $\Sigma$ is used in Livné's proof (cf. [Liv87]): he considers the map: $\alpha : M \to \mathcal{O}$ defined by $\alpha(a, b) = \operatorname{Tr} a - \operatorname{Tr} b$. Since this map is $\mathcal{O}$-linear and $\alpha(I, I) = 0$, assuming that $\alpha(\rho(\sigma)) = 0$ for every $\sigma \in \Sigma$ Livné concludes that $\alpha = 0$, i.e., equality of the traces of $\rho_1$ and $\rho_2$. We can argue in the same way but using the map: $\beta : M \to \mathbb{Z}_2$ given by

$$\beta(a, b) = \operatorname{Tr} a + (\operatorname{Tr} a)^\phi - \operatorname{Tr} b - (\operatorname{Tr} b)^\phi$$

where $\phi$ is the order two element in $\operatorname{Gal}(E/\mathbb{Q}_2)$. Observe that when applied to numbers in $F$, $\phi$ agrees with the order two element $\tau$ in $\operatorname{Gal}(F/\mathbb{Q})$.

Observe that if $a = \rho_1(g)$, then $(\operatorname{Tr} a)^\phi = (\operatorname{Tr} \rho_1(g))^\phi = \operatorname{Tr}(\rho_1'(g))$, and similarly for $b = \rho_2(g)$. This map is $\mathbb{Z}_2$-linear and satisfies $\beta(I, I) = 0$. Then, assumption (2) (ii) in the theorem implies that for elements of $G$ in $\Sigma$ (recall that these elements correspond to Frobenius elements for primes in $T$) the map $\beta$ vanishes, thus we conclude (as Livné does for $\alpha$) that $\beta = 0$, which is the equality of the traces of two 4-dimensional 2-adic Galois representations. Applying Brauer-Nesbitt we conclude that these 4-dimensional Galois representations have isomorphic semi-simplifications. □

### 4.1 Proof of Theorem 1.1

We want to apply Theorem 4.3 to the 2-adic Galois representations $\sigma_2, \sigma_{\mathfrak{f},2}$ over $F = K$. In Proposition 3.3 we proved that $\sigma_2$ has even traces by geometric considerations, and in Section 2 we proved that the same is true for the representation $\sigma_{\mathfrak{f},2}$. Recall from the introduction that both residual representations $\bar{\sigma}_2, \bar{\sigma}_{\mathfrak{f},2}$ have image in $\mathrm{SL}(\mathbb{F}_4)$. In particular their determinants are congruent modulo 2. Thus the first hypothesis of Theorem 4.3 is satisfied. The field $K_S$ of Theorem 4.3 is the compositum of the thirty one field extensions computed in the proof of Proposition 2.10. The set of primes in $K$ in the set

$$\begin{gathered}
T = \{\langle 61, 26-\sqrt{5}\rangle, \langle 59, \sqrt{5}+8\rangle, \langle 149, \sqrt{5}-68\rangle, \langle 211, \sqrt{5}+65\rangle, \langle 101, \sqrt{5}-45\rangle,\\
\langle 19, \sqrt{5}+9\rangle, \langle 229, \sqrt{5}-66\rangle, \langle 11, \sqrt{5}-4\rangle, \langle 11, \sqrt{5}+4\rangle, \langle 109, \sqrt{5}-21\rangle,\\
\langle 19, \sqrt{5}-9\rangle, \langle 701, \sqrt{5}-53\rangle, \langle 211, \sqrt{5}-65\rangle, \langle 29, \sqrt{5}-11\rangle, \langle 59, \sqrt{5}-8\rangle,\\
\langle 181, \sqrt{5}-27\rangle, \langle 239, \sqrt{5}+31\rangle, \langle 31, \sqrt{5}+6\rangle, \langle 79, \sqrt{5}-20\rangle, \langle 71, \sqrt{5}-17\rangle, 13,\\
\langle 401, \sqrt{5}-178\rangle, \langle 449, \sqrt{5}-118\rangle, \langle 241, \sqrt{5}-103\rangle, \langle 89, \sqrt{5}-19\rangle, 7,\\
\langle 79, \sqrt{5}+20\rangle, \langle 239, \sqrt{5}-31\rangle, \langle 41, \sqrt{5}-13\rangle, \langle 31, \sqrt{5}-6\rangle, \langle 71, \sqrt{5}+17\rangle\},
\end{gathered}$$

saturate the set $\mathrm{Gal}(K_S/K)\backslash\{0\}$. They are ordered in such a way that the primes (under class field theory) correspond to the extensions listed in Table 2.1 in the same order.

Thus $T$ saturates the set $\mathrm{Gal}(K_S/K)\backslash\{0\}$, but we can still eliminate some prime ideals of big norm by replacing $T$ by a non-quartic test set by Lemma 4.1. To do so, we fix a standard basis of $\mathbb{F}_2^5$ corresponding to the following quadratic extensions of $F$:

$$x^2 - 3\frac{\sqrt{5}-5}{2}, x^2-3, x^2+\frac{\sqrt{5}+5}{2}, x^2 2 - 3\sqrt{5}, x^2-2.$$

In this basis, the elements corresponding to the primes above 701, 449 and 401 correspond to the elements $(1,1,0,0,1)$, $(0,1,1,1,0)$ and $(1,1,0,1,0)$ respectively in $\mathbb{F}_2^5$.

We claim that the set $T'$ obtained from $T$ by removing these three elements is a non-quartic set in $\mathbb{F}_2^5$. To see this, we use Lemma 4.1 with the fact that $T' \cup \{0\}$ contains the four hyperplanes

$$\begin{cases} x_2 = 0 \\ x_4 + x_5 = 0 \\ x_1 + x_3 = 0 \\ x_1 + x_2 + x_3 + x_4 + x_5 = 0 \end{cases}$$

and the extra point $(0,1,1,0,1)$ (which corresponds to one of the primes above 59).

It was checked in [CS01] that the characteristic polynomials of the 4-dimensional Galois representations $\sigma_2 \oplus \sigma_2'$ and $\sigma_{\mathfrak{f},2} \oplus \sigma_{\tau(\mathfrak{f}),2}$ agree at the primes of $K$ above rational primes smaller than 100. For the remaining set of primes above the set of rational primes

$$\{101, 109, 149, 181, 211, 229, 239, 241\},$$

the same was checked by us, see Appendix A and the table at [DPS]. By Theorem 4.3 we conclude that the two 4-dimensional Galois representations have indeed isomorphic semi-simplifications. In particular, any irreducible component of one of them must be isomorphic to some irreducible component of the other, thus since we know that $\sigma_{\mathfrak{f},2}$ and $\sigma_{\tau(\mathfrak{f}),2}$ are irreducible, one of them must be isomorphic to $\sigma_2$ (and the other to $\sigma_2'$). This proves Theorem 1.1. $\square$

## A Appendix: Counting points

In this appendix we indicate how to count the number of points on the Consani-Scholten quintic $\tilde{X}$ over finite fields. In particular, we give the traces of the Galois representations $\sigma_\lambda, \sigma_\lambda'$ at the primes $p > 100$ needed to prove Theorem 1.1. For most part, we follow the approach from [CS01].
Recall that $\tilde{X}$ is given affinely by the symmetric equation in the Chebyshev polynomial $P_5(y, z)$:

$$X = \{P_5(x_1, x_2) = P_5(x_4, x_5)\} \subset \mathbb{A}^4.$$

Thus we can count the number of points of $\tilde{X}$ over some finite field $\mathbb{F}_q$ as follows:

1. Compute the affine number of points $\#X(\mathbb{F}_q)$.
2. For the projective closure $\bar{X} \subset \mathbb{P}^4$, let $S \subset \mathbb{P}^3$ be $\bar{X} - X$. Compute $\#S(\mathbb{F}_q)$.
3. Compute the contribution from the exceptional divisors in the resolution $\tilde{X} \to \bar{X}$.

For (1), we can proceed by counting how often each value in $\mathbb{F}_q$ is attained by the Chebyshev polynomial $P_5(y, z)$ over $\mathbb{A}^2$. Due to the symmetry, $\#X(\mathbb{F}_q)$ is the sum of the squares of these numbers.
For (2), note that $S$ is the Fermat quintic surface given by the model

$$S = \{x_1^5 + x_2^5 = x_4^5 + x_5^5\} \subset \mathbb{P}^3.$$

In [CS01] it was pointed out that for $q \not\equiv 1 \mod 5$ one has $\#S(\mathbb{F}_q) = 1 + q + q^2$. Meanwhile for $q \equiv 1 \mod 5$, we could either use the zeta function of $S$ and its description in terms of Jacobi symbols due to A. Weil or proceed along the same lines as above, i.e. count points over $\mathbb{A}^4$ using symmetry and then take into account that we are actually working over $\mathbb{P}^3$ (substract 1 and divide by

$q-1$). However either approach would a priori impose the same complexity as for computing $\#X(\mathbb{F}_q)$. Luckily counting $\{(y,z)\in\mathbb{A}^2_{\mathbb{F}_q}; y^5+z^5=a\}$ can be improved by noting that scalar multiplication acts as multiplication by fifth powers on the values. Hence $\#\{(y,z)\in\mathbb{A}^2_{\mathbb{F}_q}; y^5+z^5=0\}=(q-1)\cdot\#\{[y,z]\in\mathbb{P}^1_{\mathbb{F}_q}; y^5+z^5=0\}+1$ and for any $a\neq 0$ with $O(a)=a\cdot(\mathbb{F}_q^*)^5$ denoting the $a$-orbit under multiplication by fifth powers in $\mathbb{F}_q^*$:

$$\#\{(y,z)\in\mathbb{A}^2_{\mathbb{F}_q}; y^5+z^5=a\}=5\sum_{o\in O(a)}\#\{[y,z]\in\mathbb{P}^1_{\mathbb{F}_q}; y^5+z^5=o\}.$$

(Strictly speaking the sets on the right are ambiguous, but scalar multiples end up in the same orbit, so the contribution does not depend on the chosen representative $[y,z]\in\mathbb{P}^1$.) Essentially this simplification reduces the algorithm's running time from $q^2$ to $q$ compared with computing $\#X(\mathbb{F}_q)$.
Finally for (3) we recall from 3.3 that the 120 nodes are always defined over the extension of $\mathbb{F}_q$ containing the 15th roots of unity, and that their rulings are always defined over the same field. So if a node is defined over $\mathbb{F}_q$, then its exceptional divisor contributes $q^2+2q$ additional points. Thus we find $\#\tilde{X}(\mathbb{F}_q)$. This allows us to compute the trace

$$t_q=\text{trace Frob}_q^*(H^3(\tilde{X}_{\bar{\mathbb{Q}}},\mathbb{Q}_\ell))$$

through the Lefschetz fixed point formula (2). Here we do not need to know $h_q$ in advance since it is determined (for $q>20$ and $b_3(\tilde{X})=4$) by the inequality

$$\mid t_q\mid\leq 4q^{3/2}.$$

We obtain the characteristic polynomial of $\text{Frob}_q^*$ on $H^3(\tilde{X}_{\bar{\mathbb{Q}}},\mathbb{Q}_\ell)$:

$$\mu_q(T)=T^4-t_qT^3+\frac{1}{2}(t_q^2-t_{q^2})T^2-t_qq^3T+q^6.$$

In the present situation, we know that $L_q(T)$ will always split over $\mathbb{Q}(\sqrt{5})$:

$$\mu_q(T)=(T^2-\alpha_qT+q^3)(T^2-\alpha_q^\sigma T+q^3),\quad \alpha_q\in\mathbb{Q}(\sqrt{5}).$$

The traces $\alpha_p,\alpha_p^\sigma$ appear as eigenvalues of the Hilbert modular form. In the following table, we collect one of the traces together with the numbers of points of $X$ and $S$ over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for all primes $p>100$ needed to prove Theorem 1.1.

## B Appendix: Sturm Bound (by José Burgos Gil and Ariel Pacetti)

The aim of this appendix is to show how a Sturm bound can be obtained for the modular form of level $6\sqrt{5}$ and parallel weight 2. We expect to extend the result to any real quadratic fields in a future work. Following the previous notation, $F$ will denote the real quadratic field $\mathbb{Q}(\sqrt{5})$.

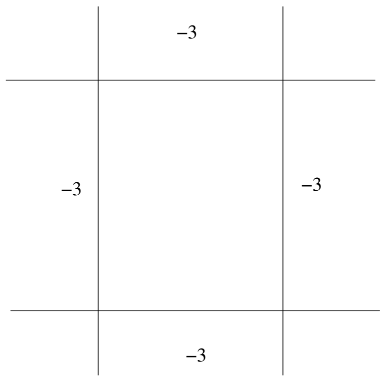
| $p$ | $\#X(\mathbb{F}_p)$ | $\#X(\mathbb{F}_{p^2})$ | $\#S(\mathbb{F}_p)$ | $\#S(\mathbb{F}_{p^2})$ | $\alpha_p$ |
|---|---|---|---|---|---|
| 101 | 1222681 | 1063601210405 | 14655 | 104338955 | $-598-476\sqrt{5}$ |
| 109 | 1338593 | 1679922873825 | 11991 | 141787855 | $890+468\sqrt{5}$ |
| 149 | 3395857 | 10952392903505 | 22351 | 494061055 | $150-344\sqrt{5}$ |
| 181 | 6562145 | 35183310464645 | 39455 | 1074841355 | $-898-288\sqrt{5}$ |
| 211 | 10261235 | 88285583898085 | 49205 | 1984280555 | $-1228-1616\sqrt{5}$ |
| 229 | 12214593 | 144270849112465 | 52671 | 2752837855 | $-210+940\sqrt{5}$ |
| 239 | 13872967 | 186440164574105 | 57361 | 3265836055 | $3240+944\sqrt{5}$ |
| 241 | 15137985 | 195998061709305 | 65255 | 3375066455 | $-4938+172\sqrt{5}$ |

## B.1 Desingularization and a Hecke bound over $\mathbb{C}$

Let $H(3)$ be the Hilbert modular surface obtained as the quotient of the product of two copies of the Poincare upper half plane modulo the action of the congruence group

$$\Gamma(3) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F) \ : \ \alpha \equiv \delta \equiv 1 \pmod 3, \beta, \gamma \in 3\mathcal{O}_F \right\}.$$

The group $\Gamma(3)$ has no fixed elliptic points for this action (see [vdG88] page 109); it has 10 non-equivalent cusps. Let $\overline{H}(3)$ be the minimal compactification of $H(3)$ obtained by adding one point for each cusp. The surface $\overline{H}(3)$ is singular at all such points. Denoting by $\widetilde{H}(3)$ the minimal desingularization of $\overline{H}(3)$, we get that the diagram of the desingularization of $\overline{H}(3)$ at any cusp is the following (see [vdG88], page 193):




Denote by $c_i$, $1 \leq i \leq 10$ the different cusps (where $c_1$ is the cusp at infinity) and denote by $S_i$, $1 \leq i \leq 10$ the exceptional divisor at the $i$-th cusp. The surface $\widetilde{H}(3)$ is of general type (by Theorem 3.4 of [vdG88]).
We want a criterion to show that a Hilbert modular form whose Fourier expansion starts with many zeroes is actually the zero modular form. This is a

generalization of the Sturm bound to Hilbert modular forms. To this end we need a nef (numerically eventually free) divisor. Let $F_1$ be the curve defined in [vdG88] page 88. It has 30 disjoint connected components made of curves with self-intersection number $-2$ and it meets each connected component of the desingularization at the cusps in three points (see [vdG88], page 193).

LEMMA B.1. *The intersection numbers between the curves $S_i$ and $F_1$ are:*

- $S_i \cdot S_j = \begin{cases} 0 & \text{if } i \neq j, \\ -4 & \text{if } i = j. \end{cases}$
- $F_1 \cdot F_1 = -60.$
- $S_i \cdot F_1 = 12.$

Consider the divisor

$$D' := \frac{1}{5}\left(\sum_{i=1}^{10} S_i + 2F_1\right).$$

LEMMA B.2. *The divisor $D'$ is nef and it agrees with the canonical divisor. Its self-intersection number is given by*

$$D' \cdot D' = 8.$$

*Proof.* In example 7.5 of [vdG88] (page 179) it is proved that $D'$ equals the canonical divisor and its self-intersection number is computed. The fact that it is nef follows from the fact that $\widetilde{H}(3)$ is a minimal surface of general type. □

*Remark* B.3. Since $\widetilde{H}(3)$ is a complex smooth projective surface, there is a unique canonical divisor (which equals the dualizing sheaf).

Let $M_{2k}(\Gamma(3))$ denote the vector space of modular forms of parallel weight $2k$ for $\Gamma(3)$. It is the space of global sections of the line bundle $\mathscr{O}(k(D'+S)) = \mathscr{O}(D'+S)^{\otimes k}$:

$$M_{2k}(\Gamma(3)) = \Gamma(\mathscr{O}(k(D'+S))),$$

where $S = \sum_{i=1}^{10} S_i$. Similarly, the space of cusp forms $S_{2k}(\Gamma(3))$ is given by the divisor $k(D'+S) - S$.

We want to add some vanishing conditions to $M_{2k}(\Gamma(3))$ such that the space of forms with these vanishing conditions is empty. Let $a$ be a positive integer, and $G$ be a Hilbert modular form. We say that $G$ vanishes with order $a$ at the cusp $c_i$ if $G$ is a section of $\mathscr{O}(k(D'+S) - aS_i) \subset \mathscr{O}(k(D'+S))$.

Let $G$ be a form which vanishes with order $a$ at all the cusps and with order $a+b$ at the infinity cusp, i.e. it belongs to the space given by the divisor

$$E = k(D'+S) - aS - bS_1.$$

It follows from Lemma B.1 and Lemma B.2 that $D' \cdot S_i = 4$ for all $1 \leq i \leq 10$, so

$$E \cdot D' = k(D' \cdot D' + S \cdot D') - aS \cdot D' - bS_1 \cdot D' = 48k - 40a - 4b.$$

If $b+10a>12k$, this intersection number is negative and, since $D'$ is nef, the space of global sections of $\mathscr{O}(E)$ is the zero space. This implies

Theorem B.4. *If $G$ is a Hilbert modular form of parallel weight $2k$ for $\Gamma(3)$ which vanishes with order $a$ at all cusps and with order $a+b$ at the infinity cusp and $b+10a>12k$, then $G$ is the zero form.*

Corollary B.5. *If $G$ is a Hilbert modular form of weight $(k_1,k_2)$, with $k_1\equiv k_2 \pmod 2$, for $\Gamma(3)$ which vanishes with order $a$ at all cusps and with order $a+b$ at the infinity cusp and $b+10a>3(k_1+k_2)$, then $G$ is the zero form.*

*Proof.* Just apply the previous Theorem to the form $G(z_1,z_2)\cdot G(z_2,z_1)$. □

To relate the order of vanishing of a modular form at a cusp with the $q$-expansion we need to compute explicitly the first step of the desingularization of the cusp. In the case of the infinity cusp, this implies computing the local ring of the cusp, which is done in [vdG88] Chapter II, Section 2. The stabilizer of the infinity cusp for $\Gamma(3)$ is given by

$$\left\{\begin{pmatrix}\epsilon & \alpha\\ 0 & \epsilon^{-1}\end{pmatrix} \;:\; \alpha\in 3\mathcal{O}_F \text{ and } \epsilon\equiv 1 \pmod 3\right\},$$

i.e. it is of type $(M,V)=(3\mathcal{O}_F,U_F^8)$, where $U_F^8=\langle\frac{47}{2}+\frac{3}{2}\sqrt{5}\rangle$. The dual of $M$ is given by $M^\vee=\frac{\mathcal{O}_F^\vee}{3}=\frac{\mathcal{O}_F}{3\sqrt{5}}$, so any Hilbert modular form for $\Gamma(3)$ has a $q$-expansion at the infinity cusp of the form

$$\sum_{\substack{\xi\gg 0\\ \xi\in\frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1+\tau(\xi)z_2).$$

Let $M_+$ denote the elements of $M$ which are totally positive, and consider the embedding of $M_+$ in $(\mathbb{R}_+)^2$, given by

$$\mu\mapsto(\mu,\tau\mu).$$

Denote by $A_k=(A_k^1,A_k^2)$, $k\in\mathbb{Z}$ the vertices of the boundary of the convex hull of the image of $M_+$, ordered with the condition $A_{k+1}^1<A_k^1$ for all $k$. Any pair $(A_{k-1},A_k)$ is a basis for $M$ as $\mathbb{Z}$-module (see [vdG88] Lemma 2.1). This determines an isomorphism

$$M\backslash\mathbb{C}^2\to\mathbb{C}^\times\times\mathbb{C}^\times,$$

which maps $z=(z_1,z_2)$ to $(u_{k-1},u_k)$, where

$$\exp(z_j)=u_{k-1}^{A_{k-1}^j}u_k^{A_k^j},\qquad \text{for } j=1,2. \tag{10}$$

Let $\sigma_k$ denote the cone spanned by $A_{k-1}$ and $A_k$, i.e.

$$\sigma_k=\{sA_{k-1}+tA_k \;:\; s,t\in\mathbb{R}_+\}.$$

The desingularization of the infinity cusp is obtained by taking a copy of $\mathbb{C}^2$ for each element $\sigma_k$ and gluing them together in terms of the change of basis matrix (see [vdG88] page 31).
Let $\xi \in M^\vee$ be a totally positive element. Then in the copy corresponding to $\sigma_k$,

$$\begin{aligned}\exp(\mathrm{Tr}(\xi z)) &= \exp(\xi z_1 + \tau(\xi) z_2) = u_{k-1}^{\xi A_{k-1}^1 + \tau(\xi) A_{k-1}^2} \cdot u_k^{\xi A_k^1 + \tau(\xi) A_k^2} = \\ &= u_{k-1}^{\mathrm{Tr}(\xi A_{k-1})} \cdot u_k^{\mathrm{Tr}(\xi A_k)}.\end{aligned}$$

Now, we denote by $L_k$, the component of the exceptional divisor $S_1$, over the infinity cusp, that corresponds to the ray through $A_k$. Observe that $L_{k+4} = L_k$. We have:

Proposition B.6. *Let $G$ be a Hilbert modular form with $q$-expansion at infinity*

$$G(z_1, z_2) = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

*Let $L_k$ be as above. Then $\mathrm{ord}_{L_k}(G) > K$ if and only if $a_\xi = 0$ for all $\xi \in M^\vee$, $\xi \gg 0$ with $\mathrm{Tr}(\xi A_k) \leq K$.*

| Name | Point |
|---|---|
| $A_0$ | $3(1,1)$ |
| $A_1$ | $3(1+\omega, 1+\tau(\omega))$ |
| $A_2$ | $3(2+3\omega, 2+3\tau(\omega))$ |
| $A_3$ | $3(5+8\omega, 5+8\tau(\omega))$ |

Table B.1: First boundary points

In Table B.1 it is shown a set of nonequivalent boundary points of the convex hull of $M_+$, where $\omega$ denotes the element $\frac{1+\sqrt{5}}{2}$. It is clear that they differ by powers of $\omega^2$, and since the matrix $\begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix} \in \Gamma_0(3)$, a Hilbert modular form for $\Gamma_0(3)$ will vanish with the same order in the four components $L_k$, $k = 0, \ldots, 3$, of $S_1$. The vanishing condition corresponding to $L_0$, reads

$$\mathrm{ord}_{L_0}(\exp(\xi z)) = 3\,\mathrm{Tr}(\xi).$$

In particular, a modular form vanishes at the cusp if and only if $a_0 = 0$.
The above discussion implies the following theorem for $\Gamma_0(3)$.

Theorem B.7. *Let $G$ be a Hilbert modular form of parallel weight $2k$ for $\Gamma_0(3)$ which vanishes with order $a$ at all cusps and whose Fourier expansion at the* *infinity cusp is given by*

$$G = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

*If $a_\xi = 0$ for all $\xi$ with $\operatorname{Tr}(\xi) \leq 4k - 3a$ then $G$ is the zero form.*

*Proof.* If $a_\xi = 0$ for all $\xi$ with $\operatorname{Tr}(\xi) \leq 4k - 3a$, by Proposition B.6, $G$ vanishes with order greater than $12k - 9a$ at the infinity cusp. Thus the result follows from Theorem B.4. $\square$

Corollary B.8. *Let $G$ be a Hilbert modular form of weight $(k_1, k_2)$, with $k_1 \equiv k_2 \pmod 2$, for $\Gamma_0(3)$ which vanishes with order $a$ at all cusps and whose Fourier expansion at the infinity cusp is given by*

$$G = \sum_{\substack{\xi \gg 0 \\ \xi \in \frac{\mathcal{O}_F}{3\sqrt{5}}}} a_\xi \exp(\xi z_1 + \tau(\xi) z_2).$$

*If $a_\xi = 0$ for all $\xi$ with $\operatorname{Tr}(\xi) \leq (k_1 + k_2) - 3a$ then $G$ is the zero form.*

## B.2 Moduli interpretation and integral models

In order to make the computation of the previous section work over finite fields, we need to use the integral structure of the modular Hilbert surface and of the modular curve $X(3)$. It comes from their moduli interpretation. Let us follow the notation of [BBGK07].
We fix $\zeta_3$ a third-root of unity and we denote by $\delta = (\sqrt{5})^{-1}$ the different of $F$.
An abelian scheme $A \to S$ of relative dimension 2, together with a ring homomorphism

$$\iota : \mathcal{O}_F \to \operatorname{End}(A)$$

is called an abelian surface with multiplication by $\mathcal{O}_F$, and is denoted by the pair $(A, \iota)$. This gives an $\mathcal{O}_F$-multiplication in the dual abelian surface $A^\vee$. An element $\mu \in \operatorname{Hom}(A, A^\vee)$ is called $\mathcal{O}_F$-linear if $\mu\iota(\alpha) = \iota(\alpha)^\vee \mu$ for all $\alpha \in \mathcal{O}_F$. Denote by $\mathscr{P}(A)$ the sheaf for the étale topology on $\operatorname{Sch}/S$ defined by

$$\mathscr{P}(A)_T = \{\lambda : A_T \to A_T^\vee \ : \ \lambda \text{ is symmetric and } \mathcal{O}_F\text{-linear}\},$$

for all $T \to S$. The subsheaf $\mathscr{P}(A)^+$ is the subsheaf of polarizations in $\mathscr{P}(A)$. The pair $(A, \iota)$ is said to satisfy the Deligne-Pappas condition, denoted by (DP), if the canonical morphism of sheaves

$$A \otimes_{\mathcal{O}_F} \mathscr{P}(A) \mapsto A^\vee$$

is an isomorphism. In this case, $\mathscr{P}(A)$ is a locally constant sheaf of projective $\mathcal{O}_F$-modules of rank 1.

Since the class number of $\mathcal{O}_F$ is one, we can restrict to consider only $\mathcal{O}_F$-*polarizations*. An $\mathcal{O}_F$-polarization on a pair $(A, \iota)$ is a morphism of $\mathcal{O}_F$-modules $\psi : \mathcal{O}_F \to \mathscr{P}(A)_S$ taking $\mathcal{O}_F^+$ to $\mathscr{P}(A)^+$ such that the natural homomorphism

$$A \otimes_{\mathcal{O}_F} \mathcal{O}_F \to A^\vee, \quad a \otimes \alpha \mapsto \psi(\alpha)(a)$$

is an isomorphism.

Suppose $S$ is a scheme over $\operatorname{Spec} \mathbb{Z}[1/3]$. A level 3-structure on an abelian surface $A$ over $S$ with real multiplication by $\mathcal{O}_F$ is an $\mathcal{O}_F$-linear isomorphism

$$\varphi : (\mathcal{O}_F/3)^2_S \to A[3]$$

between the constant group scheme defined by $(\mathcal{O}_F/3)^2$ and the 3-torsion of $A$.

THEOREM B.9. *The moduli problem "Abelian surfaces over S with real multiplication by $\mathcal{O}_F$ satisfying (DP) condition, $\mathcal{O}_F$-polarization and level 3-structure" is represented by a regular algebraic scheme $\mathscr{H}(3)$ which is flat and of relative dimension two over* $\operatorname{Spec} \mathbb{Z}[1/3, \xi_3]$. *Furthermore, it is smooth over* $\operatorname{Spec} \mathbb{Z}[1/15, \xi_3]$.

*Proof.* See [Gor02] Theorem 2.17, p. 57;Lemma 5.5, p. 99. □

*Remark* B.10. The scheme $\mathscr{H}(3)$ is not geometrically irreducible, it has $\#(\mathcal{O}_F/3)^\times = 8$ connected components over $\bar{\mathbb{Q}}$. In fact, the 8 components are defined over $\operatorname{Spec} \mathbb{Z}[1/15, \xi_3]$. This definition is not the same as the one given in [Rap78] (which is connected), it is a topological cover of degree 4 of it. Let $S$ be a scheme over $\mathbb{Z}[1/3]$, then the abelian scheme $A$ has a Weil pairing $e_3 : A[3] \times A^\vee[3] \to \mu_3$, which satisfies $e_3(\alpha a, b) = e_3(a, \alpha b)$. There exists an $\mathcal{O}_F$-bilinear form $e_{\mathcal{O}_F} : A[3] \times A^\vee[3] \to (\delta^{-1}/3\delta^{-1})(1)$ such that $e_3 = \operatorname{Tr}(e_{\mathcal{O}_F})$. Any element in $\lambda \in \mathscr{P}(A)_T$ defines a homomorphism between $A$ and $A^\vee$ which is trivial on $A[3]$ if and only if $\lambda \in 3\mathscr{P}(A)_T$ for any morphism $T \to S$. Since $e_{\mathcal{O}_F}$ is non-degenerate, $\mathscr{P}(A) \otimes_{\mathcal{O}_F} \Lambda^2_{\mathcal{O}_F} A[3] = \delta^{-1}/3\delta^{-1}(1)$.

Any element $\phi \in \operatorname{Isom}(\mu_3, \mathbb{Z}/3)$ gives an isomorphism between $\delta^{-1}/3\delta^{-1}(1)$ and $\delta^{-1}/3\delta^{-1}$. In [Rap78] the only level 3-structures considered are the $\varphi$ such that in the following diagram

$$\begin{tikzcd}
\mathscr{P}(A) \otimes_{\mathcal{O}_F} \Lambda^2_{\mathcal{O}_F} A[3] \arrow[r, equal] \arrow[d, "e_{\mathcal{O}_F}\otimes\psi"', "\sim"] & \delta^{-1}/3\delta^{-1}(1) \arrow[d, dotted] \\
\delta^{-1} \otimes_{\mathcal{O}_F} \Lambda^2_{\mathcal{O}_F}(\mathcal{O}_F/3) \arrow[r, equal] & \delta^{-1}/3\delta^{-1}
\end{tikzcd}$$

the vertical dotted arrow is given by an element $\phi \in \operatorname{Isom}(\mu_3, \mathbb{Z}/3)$. Since all such maps differ by (multiplication by) an element in $(\mathcal{O}_F/3)^\times$, the two assertions follow.

*Remark* B.11. The group $\mathrm{GL}_2(\mathcal{O}_F/3)$ acts on $\mathscr{H}(3)$, where an element $M$ send a level 3-structure $\varphi$ to the level 3-structure

$\varphi \circ M$. The subgroup $\mathrm{SL}_2(\mathcal{O}_F/3)$ acts on each connected component of $\mathscr{H}(3) \otimes \bar{\mathbb{Q}}$, while the subgroup $H_F = \{\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$ such that $\alpha \in (\mathcal{O}_F/3)^\times\}$ acts transitively on the set of connected components.

Theorem B.12. *There is a toroidal compactification $h_3 : \widetilde{\mathscr{H}}(3) \to \mathbb{Z}[\zeta_3, 1/3]$ of $\mathscr{H}(3)$ that is smooth at infinity. The complement $\widetilde{\mathscr{H}}(3)\backslash\mathscr{H}(3)$ is a relative divisor with normal crossings.*

*Proof.* See [Cha90] Theorem 3.6, Theorem 4.3 and [Rap78] Theorem 5.1 and Theorem 6.7. ∎

The set of complex points of $\mathscr{H}(3)$ is equal to 8 copies of the surface $H(3)$ considered in the previous section, while the set of complex points of $\widetilde{\mathscr{H}}(3)$ is equal to 8 copies of $\widetilde{H}(3)$.
If we study the moduli problem for 1-dimensional abelian varieties (i.e. elliptic curves), we have the advantage that they are already principally polarized. As in the two-dimensional case, if $S$ is a scheme over $\mathbb{Z}[1/3]$, a level 3-structure on an elliptic curve $E$ over $S$ is a $\mathbb{Z}$-linear isomorphism

$$\varphi : (\mathbb{Z}/3)^2_S \to E[3]$$

between the constant group scheme defined by $(\mathbb{Z}/3)^2$ and the 3-torsion of $E$.

Theorem B.13. *The moduli problem "elliptic curves over $S$ with level 3-structure" is represented by a smooth affine curve $\mathscr{Y}(3)$ over $\mathbb{Z}[1/3]$. Furthermore, the category $\mathscr{M}_3[1/3]$ of "generalized elliptic curves over $S$, that have smooth generic fibres, singular fibres whose Neron polygons have 3-sides and with a level 3-structure" is a projective smooth scheme $\mathscr{X}(3)$ over $\mathbb{Z}[1/3]$.*

*Proof.* See [DR73], Corollary 2.9. ∎

*Remark* B.14. The group $\mathrm{GL}_2(\mathbb{Z}/3)$ acts on $\mathscr{X}(3)$, in the same way as in the two dimensional case, i.e. an element $M \in \mathrm{GL}_2(\mathbb{Z}/3)$ sends the level 3-structure $\varphi$ to the level 3-structure $\varphi \circ M$. The subgroup $\mathrm{SL}_2(\mathbb{Z}/3)$ acts on each connected component of $\mathscr{X}(3)\otimes\bar{\mathbb{Q}}$ while the subgroup $H_{\mathbb{Q}} = \{\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$ such that $\alpha \in (\mathbb{Z}/3)^\times\}$ acts transitively in the set of connected components.

We want to study the inclusions of $\mathscr{Y}(3)$ into $\mathscr{H}(3)$. If $E$ is an elliptic curve over $S$, the abelian variety $A_E = E \otimes_{\mathbb{Z}} \mathcal{O}_F$ has a canonical $\mathcal{O}_F$-action $\iota_E : \mathcal{O}_F \to \mathrm{End}(A_E)$. Furthermore,

$$A_E \simeq E \times_S E,$$

where the isomorphism depends on chosing a basis for $\mathcal{O}_F$ as $\mathbb{Z}$-module. The dual abelian variety $A_E^\vee$ is isomorphic to $E \otimes_{\mathbb{Z}} \delta^{-1}$. Furthermore, $\mathscr{P}(A_E) \simeq \delta^{-1} \simeq \mathcal{O}_F$ (i.e. $A_E$ has a canonical principal polarization $\psi_E$), where the isomorphism preserves positivity and the Deligne-Pappas condition holds (see [BBGK07] Lemma 5.10). Let $(E, \varphi)$ be an elliptic curve with level 3-structure.

Consider the natural inclusion $\mathrm{SL}_2(\mathbb{Z}/3) \hookrightarrow \mathrm{SL}_2(\mathcal{O}_F/3)$, and let $\mathscr{N} = \{N_i\}_{i=1}^{30}$ be a set of representatives for the quotient set $\mathrm{SL}_2(\mathcal{O}_F/3)/\mathrm{SL}_2(\mathbb{Z}/3)$. Each element $N$ of $\mathscr{N}$ gives rise to an embedding of $\mathscr{Y}(3)$ into $\mathscr{H}(3)$, which associates to the pair $(E, \varphi)$ the element $(A_E, \iota_E, \psi_E, \varphi \circ N)$. For shortness we abuse notation by writing $\varphi \circ N$. The map $\varphi$ extends by $\mathcal{O}_F$-linearity to a map

$$\widetilde{\varphi} : (\mathbb{Z}/3)^2 \otimes_{\mathbb{Z}} \mathcal{O}_F = (\mathcal{O}_F/3)^2 \to A_E[3],$$

and the element $N$ acts in $(\mathcal{O}_F/3)^2$. By choosing a connected component of $\mathscr{Y}(3) \otimes \bar{\mathbb{Q}}$ and of $\mathscr{H} \otimes \bar{\mathbb{Q}}$, the 30 embeddings obtained from the set $\mathscr{N}$ (up to composition with an element of $H_F$ if necessary) give us open dense subsets of the 30 connected components of the curve $F_1$ from the previous section.

Theorem B.15. *The closed inmersion $\mathscr{Y}(3) \hookrightarrow \mathscr{H}(3)$ of schemes over $\mathbb{Z}[\zeta_3, 1/15]$ extends to a closed inmersion $\mathscr{X}(3) \hookrightarrow \widetilde{\mathscr{H}}(3)$.*

*Proof.* Following the referee's advice, we omit the proof of this Theorem. □

Theorem B.15 has the following direct consequences. Let $\widetilde{\mathscr{H}}$ be one of the irreducible components of $\widetilde{\mathscr{H}}(3)$ over $\operatorname{Spec} \mathbb{Z}[1/15, \xi_3]$. The set of complex points of $\widetilde{\mathscr{H}}$ agrees with the surface $\widetilde{H}(3)$ of section B.1. Let $Z$ be any irreducible component of the divisor $D'$ of $\widetilde{H}(3)$ introduced in the same section. Then $Z$ is defined over $\mathbb{Q}(\zeta_3)$. Let $\mathscr{Z} = \overline{Z}$ be the Zariski closure of $Z$ in $\widetilde{\mathscr{H}}$.

Corollary B.16. *For every prime $\mathfrak{p}$ of $\mathbb{Z}[1/15, \zeta_3]$, the vertical cycle $\mathscr{Z}_{\mathfrak{p}}$ is irreducible.*

*Proof.* If $Z$ is a component of $S$ this follows directly from Theorem B.12. If $Z$ is a component of $F_1$ this follows from Theorem B.15 and Theorem B.13. □

Let $\mathscr{D}'$ be the horizontal divisor of $\widetilde{\mathscr{H}}$ determined by $D'$.

Corollary B.17. *For every prime $\mathfrak{p}$ of $\mathbb{Z}[1/15, \zeta_3]$, the divisor $\mathscr{D}'_{\mathfrak{p}}$ of the surface $\widetilde{\mathscr{H}_{\mathfrak{p}}}$ over $\operatorname{Spec} \mathbb{Z}[1/15, \zeta_3]/\mathfrak{p}$ is nef.*

*Proof.* Since the divisor $\mathscr{D}'_{\mathfrak{p}}$ is effective, we only have to show that the intersection of $\mathscr{D}'_{\mathfrak{p}}$ with any of its irreducible components is greater or equal to zero. By Corollary B.16, every irreducible component of $\mathscr{D}'_{\mathfrak{p}}$ is the specialization of a irreducible component of $D'$. Thus the result follows from the fact that $D'$ is nef and that the intersection product is preserved by specialization. □

Corollary B.18. *Let $G$ be a Hilbert modular form of weight $(k_1, k_2)$, with $k_1 \equiv k_2 \pmod 2$, for $\Gamma_0(3)$ whose coefficients generate a finite field extension $L$ of $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{L.F[\xi_3]}$ not dividing 15. If $G$ vanishes with order $a$ at all cusps of $\widetilde{\mathscr{H}_{\mathfrak{p}}}$ and if the Fourier coefficients of its $q$-expansion at the infinity cusp are algebraic integers satisfying $a_\xi \equiv 0 \pmod{\mathfrak{p}}$ for all $\xi$ with $\mathrm{Tr}(\xi) \leq (k_1 + k_2) - 3a$ then all $a_\xi$ are divisible by $\mathfrak{p}$.*

*Proof.* From the last Corollary, we have that the divisor $\mathscr{D}'_{\mathfrak{p}}$ of the surface $\widetilde{\mathscr{H}_{\mathfrak{p}}}$ over $\operatorname{Spec}\mathbb{Z}[1/15,\zeta_3]/\mathfrak{p}$ is nef, so we can apply the same argument as in the proof of Theorems B.4 and B.7. The result follows from the fact that $\mathscr{D}'_{\mathfrak{p}}$ is the specialization of the divisor $D$ consider in such theorems and the fact that intersection numbers are preserved by specialization. □

*Remark* B.19. In practice, if one starts with a form whose coefficients vanish at all cusps of the complex Hilbert surface with order at least $a$ (for example if it is a product of cusp forms, as will be the case in the next section) then it also vanishes at all the cusps of $\bar{\mathscr{H}_{\mathfrak{p}}}$ with order at least $a$.

### B.3 The case of the form $\mathfrak{g}+\mu(\mathfrak{g})$ of level $\Gamma_0(12\sqrt{5})$

We want to apply the results of the last two sections to the Hilbert cusp form $\mathfrak{g}+\mu(\mathfrak{g})$ of Section 2, which has weight $(2,2)$ and level $\Gamma_0(12\sqrt{5})$. Assuming that its $q$-expansion at the infinity cusp is zero for all elements of trace smaller than $\tilde{b}+1$ (hence the order of vanishing at the four lines $L_i$, $i=1,\dots,3$ is $3\tilde{b}+3$), we want to determine which value of $\tilde{b}$ forces the form to be the zero form. We start with some general results.

Lemma B.20. *Let $\mathfrak{p},\mathfrak{q}$ be two distinct prime ideals of $F$ relatively prime to $3$. Then the index of $\Gamma_0(3\mathfrak{p}^r\mathfrak{q}^s)$ in $\Gamma_0(3)$ is*

$$[\Gamma_0(3):\Gamma_0(3\mathfrak{p}^r\mathfrak{q}^s)] = \mathcal{N}\mathfrak{p}^{r-1}(\mathcal{N}\mathfrak{p}+1)\mathcal{N}\mathfrak{q}^{s-1}(\mathcal{N}\mathfrak{q}+1).$$

In particular,

$$[\Gamma_0(3):\Gamma_0(12\sqrt{5})] = 120. \tag{11}$$

Let $\mathfrak{h}$ be a modular form of weight $(2,2)$ for $\Gamma_0(12\sqrt{5})$, which vanishes with order 1 at all cusps, and with order $\tilde{b}+1$ at the infinity cusp. We consider its norm to $\Gamma_0(3)$,

$$G := \prod_{\gamma\in\,\Gamma_0(12\sqrt{5})\backslash\Gamma_0(3)} \mathfrak{h}|_2[\gamma].$$

It is a parallel weight $2\cdot 120$ Hilbert modular form for $\Gamma_0(3)$. Since $\mathfrak{h}$ is a cusp form, looking at its q-expansion at the different cusps it is easy to see that $G$ vanishes with order at least 16 at all cusps and with order at least $3\tilde{b}+96$ at the infinity cusp. Then Theorem B.4 and Corollary B.18 (with $a=16$, $b=3\tilde{b}+96$ and $k=120$) imply that if $\tilde{b}\geq 395$ then $G$ is the zero form. So we get

Theorem B.21. *Let $\mathfrak{h}$ be a Hilbert modular form of parallel weight $(2,2)$ for $\Gamma_0(12\sqrt{5})$. If its Fourier expansion is given by*

$$\mathfrak{h} = \sum_{\substack{\xi\gg 0\\ \xi\in\mathcal{O}_F^\vee}} a_\xi \exp(\xi z_1+\tau(\xi)z_2).$$

*with $a_\xi\equiv 0 \pmod 2$ for all $\xi$ with $\operatorname{Tr}(\xi)\leq 395$, then $a_\xi\equiv 0 \pmod 2$ for all $\xi$.*

## References


[BBGK07] Jan H. Bruinier, José I. Burgos Gil, and Ulf Kühn. Borcherds products and arithmetic intersection theory on Hilbert modular surfaces. *Duke Math. J.*, 139(1):1–88, 2007.

[BDJ10] Kevin Buzzard, Fred Diamond, and Frazer Jarvis. On Serre's conjecture for mod $\ell$ Galois representations over totally real fields. *Duke Math. J.*, 155(1):105–161, 2010.

[Cha90] C.-L. Chai. Arithmetic minimal compactification of the Hilbert-Blumenthal moduli spaces. *Ann. of Math. (2)*, 131(3):541–554, 1990.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CS01] Caterina Consani and Jasper Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.

[DD06] Luis Dieulefait and Mladen Dimitrov. Explicit determination of images of Galois representations attached to Hilbert modular forms. *J. Number Theory*, 117(2):397–405, 2006.

[DGP10] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.*, 79(270):1145–1170, 2010.

[Dim09] Mladen Dimitrov. On Ihara's lemma for Hilbert modular varieties. *Compos. Math.*, 145(5):1114–1146, 2009.

[DM03] Luis Dieulefait and Jayanta Manoharmayum. Modularity of rigid Calabi-Yau threefolds over $\mathbb{Q}$. In *Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001)*, volume 38 of *Fields Inst. Commun.*, pages 159–166. Amer. Math. Soc., Providence, RI, 2003.

[DPS] Luis Dieulefait, Ariel Pacetti, and Matthias Schütt. Table of eigenvalues of a hilbert modular form. Available from `http://www.iag.uni-hannover.de/~schuett/publik_en.html`.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[HV06] K. Hulek and H. Verrill. On the modularity of Calabi-Yau threefolds containing elliptic ruled surfaces. In *Mirror symmetry. V*, volume 38 of *AMS/IP Stud. Adv. Math.*, pages 19–34. Amer. Math. Soc., Providence, RI, 2006. With an appendix by Luis V. Dieulefait.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Liv87] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987.

[PAR08] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, 2008. available from `http://pari.math.u-bordeaux.fr/`.

[Rap78] M. Rapoport. Compactifications de l'espace de modules de Hilbert-Blumenthal. *Compositio Math.*, 36(3):255–335, 1978.

[Shi78] Goro Shimura. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.*, 45(3):637–679, 1978.

[Tay89] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[vdG88] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

Luis Dieulefait,
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
ldieulefait@ub.edu

Ariel Pacetti
Departamento de Matemática
Universidad de Buenos Aires
Pabellón I, Ciudad Universitaria.
C.P:1428
Buenos Aires, Argentina
apacetti@dm.uba.ar

Matthias Schütt
Institut für Algebraische Geometrie
Leibniz Universität Hannover
Welfengarten 1, 30167
Hannover, Germany
schuett@math.uni-hannover.de

José Burgos Gil
ICMAT-CSIC
Nicolas Cabrera 13-15
28049 Madrid, Spain
burgos@icmat.es