

NONSOLVABLE NUMBER FIELDS RAMIFIED ONLY AT 3 AND 5

LASSINA DEMBÉLÉ, MATTHEW GREENBERG, AND JOHN VOIGHT

ABSTRACT. For $p = 3$ and $p = 5$, we exhibit a finite nonsolvable extension of \mathbb{Q} which is ramified only at p via explicit computations with Hilbert modular forms.

The study of Galois number fields with prescribed ramification remains a central question in number theory. Class field theory, a triumph of early twentieth century algebraic number theory, provides a satisfactory way to understand solvable extensions of a number field. To investigate nonsolvable extensions, the use of the modern techniques of arithmetic geometry is essential.

Implicit in his work on algebraic modular forms on groups of higher rank, Gross [17] proposed the following conjecture.

Conjecture. *For any prime p , there exists a nonsolvable Galois number field ramified only at p .*

In his analysis of Galois representations associated to classical cusp forms, Serre [32, 33] has shown that for each prime $p \geq 11$, indeed there exists a nonsolvable Galois number field ramified only at p . Conversely, it is a consequence of the proof of Serre's conjecture by Khare and Wintenberger [22] together with standard level lowering arguments that if $p \leq 7$ then any odd representation of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\text{GL}_2(\overline{\mathbb{F}}_p)$ is necessarily reducible.

Therefore, to find nonsolvable number fields which are ramified only at a prime $p \leq 7$ we are led to consider more general settings. Computations by Lansky and Pollack [24] predict the existence of a $G_2(\mathbb{F}_5)$ -extension of \mathbb{Q} ramified only at 5; however, the general theory which would provably attach a Galois representation to such an automorphic form is absent (see [18]). Following a suggestion of Gross, the first author [9] has recently constructed a nonsolvable extension ramified only at $p = 2$ by instead enlarging the base field: he exhibits two Hilbert modular forms of level 1 and parallel weight 2 over the totally real subfield $F = \mathbb{Q}(\zeta_{32})^+$ of $\mathbb{Q}(\zeta_{32})$ whose mod 2 Galois representations cut out a number field with Galois group $8 \cdot \text{SL}_2(\mathbb{F}_{2^8})^2$ ramified only at 2. (See also the introduction in his work [9] for a survey of the history of Gross' conjecture.)

In this paper, we pursue these ideas further and prove that Gross' conjecture is true for $p = 3$ (Theorem 1.3) and $p = 5$ (Theorem 2.7).

Theorem. *For $p = 3$ and $p = 5$, there exist nonsolvable Galois number fields ramified only at p .*

We construct these extensions by looking at the reduction of Hilbert modular forms of parallel weight 2 defined over $\mathbb{Q}(\zeta_{27})^+$ for $p = 3$ and the degree 5 (totally real) subfield of $\mathbb{Q}(\zeta_{25})$ for $p = 5$. We compute with spaces of Hilbert modular forms via the Jacquet-Langlands correspondence, which allows us to locate systems of Hecke eigenvalues in the (degree 1) cohomology of a Shimura curve. We combine methods of the first author [9] with those of the second and third authors [16] to compute with these spaces explicitly.

This article is organized as follows. In Sections 1 and 2, we consider the cases $p = 3$ and $p = 5$, respectively. In Section 3, we consider the case $p = 7$ and discuss the obstacles we face in applying our methods in this instance. Throughout, our computations are performed in the Magma computer algebra system [1].

The authors would like to thank Dick Gross for many helpful email exchanges and suggestions. They would also like to thank the Magma group at the University of Sydney for their continued hospitality and especially Steve Donnelly for his assistance. The first author was supported by a SFB/TR 45 of the Deutsche Forschungsgemeinschaft research grant while the second author acknowledges the support of an NSERC discovery grant.

1. A NONSOLVABLE GALOIS NUMBER FIELD RAMIFIED ONLY AT 3

In this section, we prove that Gross' conjecture is true for $p = 3$. We refer to the work of the second and third author [16] as a reference for the method employed.

To begin, we choose a totally real base field F which is ramified only at $p = 3$. The enumeration of such fields with small degree has been extensively studied by Jones [20], Jones and Roberts [21], Brueggeman [3], Lesseni [25, 26], and others. Ordering fields by degree and then discriminant, we find up to degree 9 that the only such fields $F \neq \mathbb{Q}$ are the (totally real) subfields of $\mathbb{Q}(\zeta_{27})$, namely $\mathbb{Q}(\zeta_9)^+$ and $\mathbb{Q}(\zeta_{27})^+$ having degrees 3 and 9, respectively.

Degree 3. First consider the field $F = \mathbb{Q}(\zeta_9)^+$ of degree 3, and let \mathbb{Z}_F denote its ring of integers. By the Jacquet-Langlands correspondence (see e.g. Hida [19, Proposition 2.12]), the space of Hilbert modular cusp forms over F is isomorphic as a Hecke module to the space of quaternionic modular forms over the quaternion algebra B which is ramified at 2 of 3 real places and no finite place. Let $X(1)$ be the Shimura curve associated to a maximal order in B . It is well-known that $X(1)$ has genus zero—in fact, it corresponds to the $(2, 3, 9)$ -triangle group—and consequently there are no Hilbert cusp forms of level 1 associated to this field. Raising the level at 3, the first form occurs in level $3\mathbb{Z}_F = \mathfrak{p}_3^3$ (where \mathfrak{p}_3 is a prime in \mathbb{Z}_F of norm 3). By

Buzzard, Diamond and Jarvis [5, Proposition 4.13(a)] it then follows that there are only reducible forms in higher powers of \mathfrak{p}_3 . Indeed, in level $3\mathbb{Z}_F$, the corresponding Shimura curve $X_0(3)$ has genus 1 and is defined over \mathbb{Q} , and Elkies [11] has shown that it is isomorphic to the elliptic curve A defined by $y^2 = x^3 - 432$ (or more symmetrically by $x^3 + y^3 = 1$) with $j(A) = 0$. However, since $A[3](\mathbb{Q}) = A[3](F) \cong \mathbb{Z}/3\mathbb{Z}$ the mod 3 representation associated to E is reducible. (See also Brueggeman [4] for an argument with Odlyzko bounds which proves assuming the GRH that there are only finitely many nonsolvable finite extensions of F with Galois group contained in $\mathrm{GL}_2(\overline{\mathbb{F}}_3)$.)

Degree 9, level 1. So we are led to consider instead the field $F = \mathbb{Q}(\zeta_{27})^+$; here we will find our nonsolvable extension. Let \mathbb{Z}_F again denote the ring of integers of F . The field F is a cyclic extension of \mathbb{Q} of degree 9 with discriminant $d_F = 3^{22}$, and F is generated by $\lambda = 2 \cos(2\pi/27) = \zeta_{27} + 1/\zeta_{27}$, an element which satisfies

$$\lambda^9 - 9\lambda^7 + 27\lambda^5 - 30\lambda^3 + 9\lambda - 1 = 0.$$

Moreover, the field F has strict class number 1.

Let B be the quaternion algebra $B = \left(\frac{-1, u}{F} \right)$ where

$$u = -\lambda^6 + \lambda^5 + 5\lambda^4 - 4\lambda^3 - 6\lambda^2 + 3\lambda,$$

i.e., B is generated by α, β as an F -algebra subject to $\alpha^2 = -1$, $\beta^2 = u$ and $\beta\alpha = -\alpha\beta$. The algebra B is ramified at 8 of the 9 real places of F and at no finite place. Indeed, the element $u \in \mathbb{Z}_F^*$ is a unit with $v(u) < 0$ for a unique real place v of F . The order $\mathcal{O} \subset B$ generated as a \mathbb{Z}_F -algebra by α and

$$\frac{1}{2}((\lambda^8 + \lambda^6 + \lambda^4 + \lambda^3 + 1) + (\lambda^8 + \lambda^7 + \lambda^2 + \lambda + 1)\alpha + \beta)$$

is a maximal order of B . Let $\Gamma = \Gamma(1)$ denote the Fuchsian group associated to the order \mathcal{O} and let $X = X(1) = \Gamma \backslash \mathcal{H}$ be the associated Shimura curve.

We compute [38] that the signature of the group Γ is $(45; 2^{19}, 3^{13}, 9, 27)$, that is to say, X is a curve of genus 45 and Γ has 19, 13, 1, 1 elliptic cycles of order 2, 3, 9, 27, respectively; though we will independently (and unconditionally) verify this computation below, we note that this computation took several CPU hours on a standard desktop machine to compute the relevant class numbers assuming the GRH. The hyperbolic area of X is equal to $5833/54$.

Next, we compute [37] a fundamental domain for the action of Γ by computing a Dirichlet domain D centered at $2i \in \mathcal{H}$. We exhibit the domain D inside the unit disc \mathcal{D} in Figure 1.1, mapping $2i \mapsto 0 \in \mathcal{D}$. The domain D has 630 sides (counted according to convention), and this calculation took a CPU week. The computation of the domain D yields an explicit presentation of the group, verifies that X has genus 45, and gives representatives for the $19 + 13 + 1 + 1 = 34$ elliptic cycles.

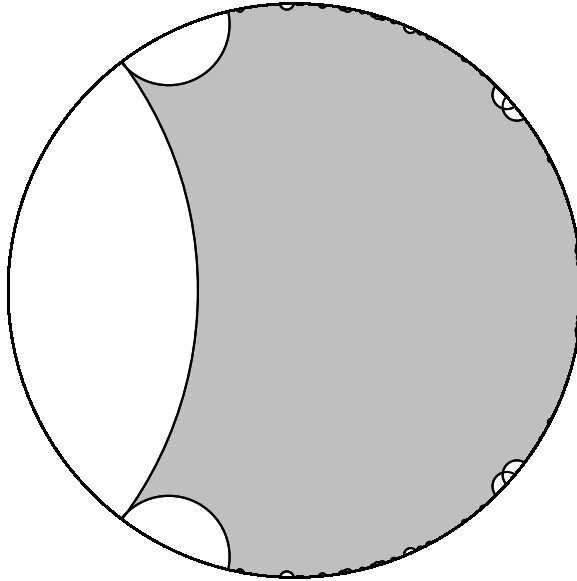


Figure 1.1: A fundamental domain for the Shimura curve $X(1)$ over $F = \mathbb{Q}(\zeta_{27})^+$

We then compute [16] the finite set of normalized Hecke eigenforms in the space $S_2(1)$, the space of Hilbert cusp forms associated to F or equivalently the space of quaternionic modular forms associated to \mathcal{O} , by computing normalized Hecke eigenforms in the cohomology group $H^1(\Gamma, \mathbb{Z})^+$. We find three Hecke-irreducible components of $S_2(1)$ with dimensions 3, 6, and 36.

Let \mathbb{T} denote the Hecke algebra acting on $S_2(1)$, the \mathbb{Z} -subalgebra of $\text{End}(S_2(1))$ generated by the Hecke operators $T_{\mathfrak{p}}$ with \mathfrak{p} a prime of \mathbb{Z}_F . Let f be a newform which represents the equivalence class of the third component of $S_2(1)$, having dimension 36. (We will see in Remark 1.2 below that the other two components do not give rise to interesting Galois representations modulo 3.) Let $H_f = \mathbb{Q}(a_{\mathfrak{p}}(f))$ be the field of coefficients of f . Then, by theory of Eichler and Shimura [34] (see also Knapp [23, Chap. XII]), there is an abelian variety A_f associated to f of dimension 36 defined over F which is a quotient of the Jacobian $J(1)$ of $X(1)$ with the additional properties that A_f has real multiplication by H_f and has everywhere good reduction.

We identify the field H_f as follows. Let E be the (totally real) field generated by a root c of the polynomial $x^4 + x^3 - 5x^2 - x + 3$; the field E has discriminant $d_E = 9301 = 71 \cdot 131$ and Galois group S_4 . Then H_f is the ray class field with conductor

$$\mathfrak{P}_3^2 \mathfrak{P}_7 \mathfrak{P}_{6481} = (1089c^3 + 134c^2 - 5551c + 3747),$$

where \mathfrak{P}_3 and \mathfrak{P}_{6481} are the unique primes in \mathbb{Z}_E of norm 3 and 6481, respectively, and $\mathfrak{P}_7 = (10c^3 + c^2 - 51c + 35)\mathbb{Z}_E$ is one of two primes of norm 7. The discriminant of H_f is then computed to be $d_{H_f} = 3^{12} 7^6 71^9 131^9 6481^8$.

By a ray class group computation, we find that $\text{Gal}(H_f/E) \cong \mathbb{Z}/9\mathbb{Z}$. Let \mathbb{T}_f be the (restriction) of the Hecke algebra acting on the constituent of f ; then \mathbb{T}_f is an order of conductor \mathfrak{P}_3^6 in the ring of integers \mathbb{Z}_{H_f} , where $3\mathbb{Z}_{H_f} = \mathfrak{P}_3\mathfrak{P}_3^3$ and the primes $\mathfrak{P}_3, \mathfrak{P}_3'$ in \mathbb{T}_f have inertial degrees 27, 3. In particular, the order \mathbb{T}_f is maximal at the prime \mathfrak{P}_3 .

Now, by the work of Carayol [7] (see also Taylor [36]), there exists a totally odd Galois representation

$$\rho_f : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(\mathbb{T}_f \otimes \mathbb{Z}_3)$$

such that for any prime $\mathfrak{p} \nmid 3$ of \mathbb{Z}_F we have $\text{tr}(\rho_f(\text{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}(f)$ and $\det(\rho_f(\text{Frob}_{\mathfrak{p}})) = N_{\mathfrak{p}}$, where $f|_{T_{\mathfrak{p}}} = a_{\mathfrak{p}}(f)f$. In our set up, where the degree of the basis field F is odd, the representation ρ_f can be realized explicitly in the 3-adic Tate module of the abelian variety A_f . (It is still a conjecture that the 2-adic representations that appear in work of the first author [9] can be realized in the same way.)

Remark 1.2. In our analysis, we consider only the prime \mathfrak{P}_3 of inertial degree 27 in the constituent of f of dimension 36. Consider instead the other primes above 3 in $\mathbb{T} \otimes \mathbb{Z}_3$. In all cases, the Hecke algebra is not maximal at these primes (there are unique primes above 3 for the components of dimensions 3 and 6, respectively, and one other prime above 3 for the component of dimension 36). In other words, for every such prime $\mathfrak{P} \neq \mathfrak{P}_3$ of $\mathbb{T} \otimes \mathbb{Z}_3$ with $\mathfrak{P} \mid 3$, the Hecke operator $T_{\mathfrak{p}}$ is divisible by a prime above 3, and so the reduction modulo \mathfrak{p} is zero.

We are now ready to prove the following theorem.

Theorem 1.3. *There exists a Galois extension K of \mathbb{Q} that is ramified only at 3 with Galois group $\text{Gal}(K/\mathbb{Q}) \cong 9 \cdot \text{PGL}_2(\mathbb{F}_{3^{27}})$.*

Proof. We reduce the representation ρ_f modulo the prime \mathfrak{P}_3 of \mathbb{T}_f of degree 27 to obtain a representation

$$\overline{\rho}_f : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(k)$$

where $k = \mathbb{F}_{3^{27}}$. Let α satisfy $\alpha^{27} - \alpha^7 + 1 = 0$ so that $k = \mathbb{F}_3(\alpha)$ and k^\times is generated by α , and let $q = \#k = 3^{27}$.

In Table 1.4, we tabulate the discrete logarithm to the base α of the eigenvalues $\overline{a}_{\mathfrak{p}}(f) = \text{tr}(\overline{\rho}_f(\text{Frob}_{\mathfrak{p}})) \in k$ occurring in the representation $\overline{\rho}_f$.

For example, we have

$$\begin{aligned} \overline{a}_{\mathfrak{p}_{53}}(f) &= \alpha^{4309388243332} \\ &= -\alpha^{25} + \alpha^{24} + \alpha^{23} - \alpha^{21} - \alpha^{18} + \alpha^{15} + \alpha^{13} + \alpha^{11} \\ &\quad - \alpha^{10} - \alpha^9 - \alpha^8 - \alpha^6 - \alpha^5 - \alpha^4 + \alpha^2 \end{aligned}$$

and $\overline{a}_{\mathfrak{p}_{53}}(f)$ satisfies the polynomial

$$\begin{aligned} &x^{27} - x^{24} - x^{23} + x^{22} - x^{20} + x^{19} + x^{18} - x^{17} - x^{16} - x^{15} \\ &\quad - x^{14} - x^{13} + x^{11} - x^6 + x^5 + x^4 + x^3 + x - 1. \end{aligned}$$

$N\mathfrak{p}$	$\log_{\alpha} \bar{a}_{\mathfrak{p}}(f)$	$o_{\mathfrak{p}}(f)$
3	5279259797298	—
53	4309388243332	$q - 1$
107	3543848555542	$q - 1$
109	5965238429265	$(q - 1)/2$
163	3456998555640	$(q - 1)/2$
269	2951025230806	$(q - 1)/109$
271	2766037528324	$(q + 1)/4$

Table 1.4: Hecke data for the representation $\bar{\rho}_f$ of level 1 for $F = \mathbb{Q}(\zeta_{27})^+$

In Table 1.4, we list values for one choice of prime \mathfrak{p} above $N\mathfrak{p}$; the full set of Hecke eigenvalues for the primes \mathfrak{p} with $\mathfrak{p} \nmid 3$ are simply $\sigma^i(\bar{a}_{\mathfrak{p}}(f))$ for $i = 0, \dots, 8$, where σ is the 27-power Frobenius $\alpha \mapsto \alpha^{27}$ on k .

We consider the projection $P\bar{\rho}_f$ of $\bar{\rho}_f$ to $\mathrm{PGL}_2(k)$ and prove that the image is surjective. Since the element $\bar{\rho}_f(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p} \nmid 3$ has characteristic polynomial $x^2 - \bar{a}_{\mathfrak{p}}(f)x + N\mathfrak{p}$ modulo 3, we can compute the order $o_{\mathfrak{p}}(f)$ of $\bar{\rho}_f(\mathrm{Frob}_{\mathfrak{p}})$ for the primes in Table 1.4 and these orders are independent of the choice of prime \mathfrak{p} above $N\mathfrak{p}$.

With these orders in hand, we refer to Dickson’s classification [10] of subgroups of $\mathrm{PGL}_2(k)$. The image of $P\bar{\rho}_f$ is obviously not an exceptional group; it is not cyclic or dihedral; it is not affine since it contains elements dividing both $q - 1$ and $q + 1$; and it cannot be contained in $\mathrm{PSL}_2(k)$ since $\bar{\rho}_f$ is totally odd and -1 is not a square in k . Therefore the image $P\bar{\rho}_f$ is projective and of the form $\mathrm{PGL}_2(k')$ with $k' \subseteq k$ a subfield, but already the fact that $\mathrm{lcm}(q - 1, (q + 1)/4) \mid \#\mathrm{PGL}_2(k')$ requires that $k' = k$.

The desired field K is then simply the Galois extension of F cut out by $\ker(P\bar{\rho}_f)$, considered as an extension of \mathbb{Q} . \square

We observed earlier that the residual representation $\bar{\rho}_f$ can be realized in the 3-torsion of the abelian variety A_f , which has good reduction everywhere. Thus we can apply a result of Fontaine [14, Corollaire 3.3.2] to bound the root discriminant of K as $\delta_K \leq \delta_F \cdot 3^{1 + \frac{1}{3-1}} = 3^{22/9+3/2} \leq 76.21$.

Degree 9, level \mathfrak{p}_3 . We conclude this section with results of computations for the field $F = \mathbb{Q}(\zeta_{27})^+$ with level \mathfrak{p}_3 . We compute the space of Hilbert modular cusp newforms $S_2(\mathfrak{p}_3)^{\mathrm{new}}$ of level \mathfrak{p}_3 in two ways. As above, we can compute the Hecke module $S_2(\mathfrak{p}_3)^{\mathrm{new}}$ in the cohomology of the Shimura curve $X_0(\mathfrak{p}_3)$. On the other hand, by the Jacquet-Langlands correspondence, we can compute this space [9] as the space of cuspidal automorphic forms associated to a maximal order of the totally definite quaternion algebra over F which is ramified at \mathfrak{p}_3 and all 9 real places of F —and in this case, the computations were performed by Steve Donnelly.

Agreeably, we find in each case that the space $S_2(\mathfrak{p}_3)^{\mathrm{new}}$ has dimension 117 and decomposes into irreducible Hecke constituents of dimensions 53 and

64. Due to high complexity we do not perform the same detailed analysis of the coefficient field for these spaces as we did before. Nevertheless, we again obtain a Galois representation

$$\bar{\rho} : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(\mathbb{T} \otimes \mathbb{F}_3).$$

The \mathbb{F}_3 -algebra $\mathbb{T} \otimes \mathbb{F}_3$ has 12 non-Eisenstein maximal ideals. In Table 1.5, we group these maximal ideals according to the degree of their residue fields and note the action of $\text{Gal}(F/\mathbb{Q})$, generated by σ .

Inertial degree	Number of ideals	Galois action
1	9	σ permutes
18	2	σ fixes
36	1	σ fixes

Table 1.5: Hecke data for the representation $\bar{\rho}$ of level \mathfrak{p}_3 for $F = \mathbb{Q}(\zeta_{27})^+$

Arguing as above, we find four other Galois extensions ramified only at 3 with Galois groups: one with (solvable) Galois group $9 \cdot \text{PGL}_2(\mathbb{F}_3)^9$, two with Galois group $9 \cdot \text{PGL}_2(\mathbb{F}_{3^{18}})$, and one with Galois group $9 \cdot \text{PGL}_2(\mathbb{F}_{3^{36}})$. In order to estimate the root discriminants of these fields, we note that by consideration of inertial degrees, there is no congruence modulo 3 between the forms computed here and the forms of level 1. Therefore, the restrictions to the decomposition group at \mathfrak{p}_3 of the corresponding residual Galois representations are *très ramifiée* and we cannot directly apply the result of Fontaine as above (though his remark [14, Remarque 3.3.3] implies that one should be able to adapt the argument). We use instead a result of Moon [29, Lemma 2.1] to obtain that the root discriminants are respectively bounded by $3^{\frac{22}{9} + \frac{14}{9}(1 - \frac{1}{9})} = 3^{310/81} \leq 66.992$, $3^{317/81} \leq 73.664$, and $3^{641/162} \leq 77.245$, respectively.

2. NONSOLVABLE GALOIS NUMBER FIELDS RAMIFIED ONLY AT 5

In this section, we prove that Gross' conjecture is true for $p = 5$. Our method follows the same lines of reasoning as in the previous section.

As above (see also Lesseni [27]), all candidates (ramified only at 5) for the base field F up to degree 10 are subfields of $\mathbb{Q}(\zeta_{25})^+$. We find only reducible representations arising from the field $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5)^+$; see work of the first author [8] for a detailed analysis of Hilbert modular forms over this quadratic field.

Degree 5, level 1. Let F be the degree 5 subfield of $\mathbb{Q}(\zeta_{25})^+$. Then F is a cyclic extension of \mathbb{Q} with discriminant $d_F = 5^8$, and $F = \mathbb{Q}(b)$ where

$$b^5 - 10b^3 - 5b^2 + 10b - 1 = 0.$$

The field F has strict class number 1.

We proceed as in Section 1. We first find a unit $u \in \mathbb{Z}_F^*$ such that the algebra $B = \left(\frac{-1, u}{F}\right)$ is ramified at all but one real place of F and no finite place. Next, we let $\mathcal{O}(1)$ be a maximal order in B , and we let $\Gamma(1)$ and $X(1)$ denote the Fuchsian group and Shimura curve associated to $\mathcal{O}(1)$, respectively. The signature of $\Gamma(1)$ is $(2; 2^5, 3^{11})$ and the area of $X(1)$ is $71/6$. Here, the field F and the curve $X(1)$ are much simpler than the case considered in the previous section and our computations are significantly less laborious. We find that the space $S_2(1)$ of Hilbert cusp forms of level 1 is irreducible (of dimension 2), corresponding to a normalized cusp form f . We compute the eigenvalues $a_{\mathfrak{p}}(f)$ of the Hecke operators $T_{\mathfrak{p}}$ in Table 2.1; here we let ω satisfy $\omega^2 + \omega - 1 = 0$ so that $\mathbb{T} = \mathbb{Z}[\omega]$ is the ring of integers in $\mathbb{Q}(\sqrt{5})$.

$N\mathfrak{p}$	$a_{\mathfrak{p}}(f)$
5	$\omega - 2$
7	ω
32	$-5\omega + 2$
43	$-3\omega - 3$
101	$4\omega - 1$
107	$-12\omega - 9$
149	$-8\omega + 1$
151	$9\omega + 9$
157	$10\omega + 7$
193	$6\omega + 4$
199	$-9\omega - 12$
243	31

Table 2.1: Hecke eigenvalues in level 1 for $F \subset \mathbb{Q}(\zeta_{25})^+$ with $[F : \mathbb{Q}] = 5$

We list only the norm of the prime \mathfrak{p} in Table 2.1 since the Hecke eigenvalue $a_{\mathfrak{p}}(f)$ is independent of the choice of prime with given norm for all such primes \mathfrak{p} . This observation suggests that the form f is the base change of a form from \mathbb{Q} . Indeed, because F has strict class number 1, the genus 2 curve $X(1)$ has a canonical model defined over F , and because the data defining B is $\text{Gal}(F/\mathbb{Q})$ -invariant, by functoriality (Galois descent) the curve $X(1)$ in fact has field of moduli equal to \mathbb{Q} . But then since $[F : \mathbb{Q}]$ is odd, and F is a field of definition for $X(1)$, the Brauer obstruction to defining $X(1)$ over \mathbb{Q} vanishes (by work of Mestre, completed by Cardona and Quer [6]), so $X(1)$ is defined over \mathbb{Q} .

In fact, we can identify this base change explicitly: let g be the newform of level $\Gamma_1(25)$ and weight 2 with \mathbb{Q} -expansion given by

$$g = q + (\zeta_5^3 - \zeta_5 - 1)q^2 + \dots + (\zeta_5^3 + \zeta_5^2)q^7 + \dots + (-3\zeta_5^3 - 3\zeta_5^2 - 3)q^{43} + \dots,$$

and $\chi : (\mathbb{Z}/25\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ its associated character. Then χ has conductor 25 and order 5; and the form g and its conjugates generate $S_2(25, \chi)^{\text{new}}$.

Lemma 2.2. *The form f is the base change of g to F .*

Proof. Let $BC_{E/F}(f)$ be the base change of f from F to $E = \mathbb{Q}(\zeta_{25})^+$; and $BC_{F/\mathbb{Q}}(g)$ (resp. $BC_{E/\mathbb{Q}}(g)$) the base change of g from \mathbb{Q} to F (resp. from \mathbb{Q} to E). Then, since f is a newform of parallel weight 2 and level 1, so is $BC_{E/F}(f)$.

Let A_g be the modular abelian variety associated to g by the Eichler-Shimura construction. By Mazur and Wiles [28, Chapter 3.2, Proposition 2] (see also Schoof [30, Theorem 1.1] and the discussion thereafter), A_g acquires everywhere good reduction above E . Hence, $BC_{E/\mathbb{Q}}(g)$ is also a newform of parallel weight 2 and level 1. By computing the space of Hilbert modular forms over E of level 1 (see the Degree 10 case later in this section for the details of this calculation), we conclude that

$$BC_{E/F}(BC_{F/\mathbb{Q}}(g)) = BC_{E/\mathbb{Q}}(g) = BC_{E/F}(f).$$

Hence, by functoriality of base change (see for example [15, Theorem 2]), we must have $BC_{F/\mathbb{Q}}(g) = f \otimes \eta$ for some character $\eta : \text{Gal}(E/F) \rightarrow \{\pm 1\}$. But we see that $a_{\mathfrak{p}}(BC_{F/\mathbb{Q}}(g)) = a_{\mathfrak{p}}(f)$ for any prime $\mathfrak{p} \mid 7$ in \mathbb{Z}_F . Thus $\eta \equiv 1$, since all the primes above 7 in \mathbb{Z}_F are inert in \mathbb{Z}_E , and $BC_{F/\mathbb{Q}}(g) = f$ as claimed. \square

Let

$$\bar{\rho}_g : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_5)$$

be the mod 5 representation associated to g . By Serre's conjecture [22], the image of $\bar{\rho}_g$ is solvable and by Lemma 2.2, we have $\bar{\rho}_f = \bar{\rho}_g|_{\text{Gal}(\bar{F}/F)}$. Therefore, the image of $\bar{\rho}_f$ is solvable as well. For completeness, we identify the field cut out by $\bar{\rho}_f$.

Lemma 2.3. *The fields cut out by $\bar{\rho}_g$ and $\bar{\rho}_f$ are $\mathbb{Q}(\zeta_5)$ and $F(\zeta_5)$, respectively.*

Proof. Computing Hecke eigenvalues of g we confirm that

$$pa_p(g) \equiv p^3(p+1) \pmod{5}$$

for all primes p , thus $\theta g \equiv \theta^3 G_2 \pmod{5}$ where G_2 is the weight 2 Eisenstein series and θ is the usual theta operator on modular forms modulo p . It follows from this congruence that $\bar{\rho}_g$ is the direct sum of two powers of the mod 5 cyclotomic character and, thus, that $\bar{\rho}_g$ cuts out $\mathbb{Q}(\zeta_5)$; (alternatively, this follows from Ellenberg [13, Proposition 1.2]). Therefore, $\bar{\rho}_f = \bar{\rho}_g|_{\text{Gal}(\bar{F}/F)}$ cuts out $F(\zeta_5)$. \square

Degree 5, level \mathfrak{p}_5 . To find a Galois representation of F which has non-solvable image, we now raise the level. Let $\mathcal{O}_0(\mathfrak{p}_5) \subset B$ be an Eichler order of level \mathfrak{p}_5 with \mathfrak{p}_5 the unique prime above 5, and let $X_0(\mathfrak{p}_5)$ be the Shimura curve of level \mathfrak{p}_5 associated to $\mathcal{O}_0(\mathfrak{p}_5)$. Then $X_0(\mathfrak{p}_5)$ is defined over F and has genus 34.

We compute the space of Hilbert modular cusp newforms $S_2(\mathfrak{p}_5)^{\text{new}}$ of level \mathfrak{p}_5 again in two ways: the Hecke module $S_2(\mathfrak{p}_5)^{\text{new}}$ occurs both in the cohomology of the Shimura curve $X_0(\mathfrak{p}_5)$ and in the space of cuspidal automorphic forms associated to the maximal order of a totally definite quaternion algebra over F which is ramified at \mathfrak{p}_5 and all real places of F . Agreeably, we find in each case that the space has dimension 30.

Let \mathbb{T}^{new} be the Hecke algebra acting on $S_2(\mathfrak{p}_5)^{\text{new}}$, the \mathbb{Z} -subalgebra of \mathbb{T} generated by all Hecke operators $T_{\mathfrak{p}}$ with $\mathfrak{p} \neq \mathfrak{p}_5$. The space $S_2(\mathfrak{p}_5)^{\text{new}}$ has two irreducible components under the action of \mathbb{T}^{new} , of dimensions 10 and 20, corresponding to newforms f and g . Let H_f and H_g denote the field of coefficients of f and g , respectively. Again by the theory of Eichler and Shimura, we can decompose the new part of the Jacobian $J_0(\mathfrak{p}_5)^{\text{new}}$ of $X_0(\mathfrak{p}_5)$ as

$$J_0(\mathfrak{p}_5)^{\text{new}} \xrightarrow{\sim} A_f \times A_g$$

where A_f and A_g are abelian varieties of dimension 10 and 20 with good reduction outside \mathfrak{p}_5 and real multiplication by H_f and H_g , respectively.

We now identify the fields H_f and H_g by direct computation. The field H_f is the ray class field of $E_f = \mathbb{Q}(\sqrt{421})$ with conductor \mathfrak{P}_{11} , where \mathfrak{P}_{11} is a prime above 11 in \mathbb{Z}_{E_f} . We find that $d_{H_f} = 11^4 421^5$. The restriction \mathbb{T}_f of the Hecke algebra \mathbb{T}^{new} acting on the constituent of f is then identified with the maximal order \mathbb{Z}_{H_f} of H_f . The ideal 5 splits in E_f and each of these primes remain inert in H_f , so that

$$(2.4) \quad 5\mathbb{T}_f = \mathfrak{P}_5 \mathfrak{P}'_5$$

with the inertial degree of the primes $\mathfrak{P}_5, \mathfrak{P}'_5$ being equal to 5. In particular, we note that $\text{Aut}(H_f) = \text{Gal}(H_f/E_f) \cong \mathbb{Z}/5\mathbb{Z}$ fixes each of the ideals \mathfrak{P}_5 and \mathfrak{P}'_5 .

The field H_g is obtained as follows. Let E_g be the (totally real) quartic field generated by a root of the polynomial $x^4 + 2x^3 - 75x^2 - 112x + 816$. Then the field E_g has discriminant $d_{E_g} = 2^2 5^1 13936963$ and Galois group S_4 . Then the prime 71 splits completely in E_g and H_g is the ray class field of E_g of conductor \mathfrak{P}_{71} , where \mathfrak{P}_{71} is a prime above 71. We have $d_{H_g} = 2^{10} 5^5 71^4 13936963^5$. The restriction \mathbb{T}_g of \mathbb{T}^{new} to the constituent of g is a suborder of index 32 in the maximal order of H_g . Here, we have

$$(2.5) \quad 5\mathbb{Z}_{E_g} = \mathfrak{P}_5^2 \mathfrak{P}'_5;$$

the prime \mathfrak{P}_5 splits completely in H_g and the primes above \mathfrak{P}_5 in H_g are permuted by $\text{Aut}(H_g) = \text{Gal}(H_g/E_g) \cong \mathbb{Z}/5\mathbb{Z}$ whereas the prime \mathfrak{P}'_5 is inert.

As above, corresponding to the newforms f and g are representations

$$(2.6) \quad \rho_f, \rho_g : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(\mathbb{T}_f \otimes \mathbb{Z}_5), \text{GL}_2(\mathbb{T}_g \otimes \mathbb{Z}_5)$$

which arise in the 5-adic Tate modules of the abelian varieties A_f and A_g , respectively. The reduction of these forms indeed give rise to nonsolvable extensions.

Theorem 2.7. *There exist Galois extensions K, K' of \mathbb{Q} that are linearly disjoint over F and ramified only at 5 with Galois group*

$$\text{Gal}(K/\mathbb{Q}), \text{Gal}(K'/\mathbb{Q}) \cong 5 \cdot \text{PGL}_2(\mathbb{F}_{5^5}).$$

Furthermore, there exist Galois extensions L and M of \mathbb{Q} that are ramified only at 5 with Galois groups $\text{Gal}(L/\mathbb{Q}) \cong 5 \cdot \text{PGL}_2(\mathbb{F}_5)^5$ and $\text{Gal}(M/\mathbb{Q}) \cong 5 \cdot \text{PGL}_2(\mathbb{F}_{5^{10}})$.

Proof. Our proof falls into two cases, corresponding to the representations ρ_f and ρ_g in (2.6).

Case 1. We first exhibit the extensions K and K' . Let $\mathfrak{m}_f, \mathfrak{m}'_f$ be the maximal ideals of $\mathbb{T}_f \otimes \mathbb{Z}_5$ with residue field $k = \mathbb{F}_{5^5}$ by (2.4), and let $\bar{\rho}_f$ and $\bar{\rho}'_f$ be the reduction of ρ_f modulo \mathfrak{m}_f and \mathfrak{m}'_f , respectively.

We now tabulate the data for the Hecke operators for the representations $\bar{\rho}_f$ and $\bar{\rho}'_f$. Let $\alpha \in \overline{\mathbb{F}_5}$ be a root of the polynomial $x^5 - x - 2$, so that $k = \mathbb{F}_5(\alpha)$. In Table 2.8, we list for a prime \mathfrak{p} of \mathbb{Z}_F the eigenvalue $\bar{a}_{\mathfrak{p}}(f) = \text{tr}(\bar{\rho}_f(\text{Frob}_{\mathfrak{p}})) \in k$ occurring in the representation $\bar{\rho}_f$ and the order $o_{\mathfrak{p}}(f)$ of the image $\text{P}\bar{\rho}_f(\text{Frob}_{\mathfrak{p}}) \in \text{PGL}_2(k)$, and we list the similar quantities for the representation $\bar{\rho}'_f$.

$N\mathfrak{p}$	$\bar{a}_{\mathfrak{p}}(f)$	$\bar{a}_{\mathfrak{p}}(f')$	$o_{\mathfrak{p}}(f)$	$o_{\mathfrak{p}}(f')$
5	4	4	—	—
7	$3\alpha^4 + 3\alpha^3 + \alpha^2 + 2\alpha + 2$	$3\alpha^4 + \alpha^3 + 4\alpha + 2$	1042	284
32	0	0	2	2
43	$2\alpha^4 + 3\alpha^3 + \alpha^2 + 4\alpha$	$3\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 2$	1042	3124
101	$2\alpha^4 + 3\alpha^3 + \alpha^2 + 4$	$2\alpha^4 + 4\alpha^3 + 4\alpha + 1$	781	1562
107	$4\alpha^4 + 4\alpha^2 + \alpha + 4$	$2\alpha^4 + 4\alpha^3 + 2\alpha^2$	3126	3124
149	$2\alpha^4 + 2\alpha^3 + 4\alpha^2 + 2\alpha + 2$	$4\alpha^4 + 4\alpha^3 + 2\alpha + 2$	1563	142
151	$3\alpha^4 + 4\alpha^3 + 4\alpha^2 + 3\alpha + 4$	$2\alpha^4 + 4\alpha^3 + 2\alpha^2 + 3\alpha + 2$	781	1563
157	$2\alpha^4 + \alpha^2 + 2\alpha + 1$	$2\alpha^4 + \alpha^3 + 4\alpha^2 + 3\alpha + 3$	1042	284
193	$3\alpha^4 + 2\alpha^3 + 4\alpha^2 + 2\alpha$	$4\alpha^4 + \alpha^3 + 4\alpha^2 + 2\alpha$	3124	3124
199	$4\alpha^4 + 2\alpha^3 + 4\alpha^2 + 1$	$3\alpha^4 + 4\alpha^3 + \alpha^2 + 4\alpha + 4$	1562	781
243	0	1	2	4
257	$2\alpha^4 + 4\alpha^3 + 2\alpha^2 + 2\alpha$	$4\alpha^4 + 3\alpha^2 + \alpha + 4$	3126	3126

Table 2.8: Hecke data for the representations $\bar{\rho}_f$ and $\bar{\rho}'_f$ of level \mathfrak{p}_5 for $F \subset \mathbb{Q}(\zeta_{25})^+$ with $[F : \mathbb{Q}] = 5$

We list in Table 2.8 the eigenvalues for a choice of prime \mathfrak{p} with specified norm; the others can be recovered from the fact that there exists $\sigma \in \text{Gal}(F/\mathbb{Q})$ such that

$$\bar{a}_{\sigma(\mathfrak{p})}(f) = \tau(\bar{a}_{\mathfrak{p}}(f))$$

where $\tau : k \rightarrow k$ given by $\alpha \mapsto \alpha^5$ is the 5-power Frobenius.

An argument as in the proof of Theorem 1.3 shows that the images $P\overline{\rho}_f$ and $P\overline{\rho}'_f$ are surjective to $\mathrm{PGL}_2(k)$. Let K and K' be the Galois extensions of F cut out by $\ker(P\overline{\rho}_f)$ and $\ker(P\overline{\rho}'_f)$, respectively, each with Galois group $5 \cdot \mathrm{PGL}_2(\mathbb{F}_{5^5})$. Since $\mathrm{Aut}(H_f) = \mathrm{Gal}(H_f/E_f)$ fixes \mathfrak{m}_f and \mathfrak{m}'_f individually, we find that K and K' are Galois over \mathbb{Q} , as claimed.

Case 2. In a similar fashion, we exhibit the extensions L and M from the form g . Now, the maximal ideals of $\mathbb{T}_g \otimes \mathbb{Z}_5$ are as follows: there are five maximal ideals $\mathfrak{m}_g^{(i)}$ for $i = 1, \dots, 5$, each with residue field \mathbb{F}_5 , and one maximal ideal \mathfrak{m}_g with residue field $\mathbb{F}_{5^{10}}$. As in Case 1, let $\overline{\rho}_g^{(i)}$ and $\overline{\rho}_g$ be the reductions of ρ_g modulo the ideals $\mathfrak{m}_g^{(i)}$ and \mathfrak{m}_g , respectively. In Table 2.9, we first list the relevant Hecke data for the representations $\overline{\rho}_g^{(i)}$.

$N\mathfrak{p}$	(1)		(2)		(3)		(4)		(5)	
	$\overline{a}_{\mathfrak{p}}(g)$	$o_{\mathfrak{p}}(g)$	$\overline{a}_{\mathfrak{p}}(g)$	$o_{\mathfrak{p}}(g)$	$\overline{a}_{\mathfrak{p}}(g)$	$o_{\mathfrak{p}}(g)$	$\overline{a}_{\mathfrak{p}}(g)$	$o_{\mathfrak{p}}(g)$	$\overline{a}_{\mathfrak{p}}(g)$	$o_{\mathfrak{p}}(g)$
5	1	—	1	—	1	—	1	—	1	—
7	4	6	4	6	2	4	0	2	0	2
32	2	4	2	4	2	4	2	4	2	4
43	1	4	1	4	3	6	1	4	2	6
101	1	3	0	2	1	3	3	5	0	2
107	3	4	2	4	2	4	3	4	1	6
149	1	5	3	3	0	2	1	5	1	5
151	4	3	2	5	3	5	0	2	0	2
157	0	2	3	4	3	4	1	6	1	6
193	0	2	1	4	2	6	3	6	4	4
199	1	5	0	2	4	5	1	5	4	5
243	0	2	0	2	0	2	0	2	0	2

Table 2.9: Hecke data for the representations $\overline{\rho}_g^{(i)}$ of level \mathfrak{p}_5 for $F \subset \mathbb{Q}(\zeta_{25})^+$ with $[F : \mathbb{Q}] = 5$

In the column labeled (i) for $i = 1, \dots, 5$ we give the data for the prime ideal $\tau^{i-1}(\mathfrak{p})$ where τ is a generator of $\mathrm{Gal}(K_g/E_g)$. We tabulate the data for a choice of prime \mathfrak{p} with specified norm, but we have the relation

$$\overline{a}_{\mathfrak{p}}(g^{(i)}) = \overline{a}_{\mathfrak{p}^{(i)}}(g),$$

i.e., the cyclic group $\mathbb{Z}/5\mathbb{Z}$ simultaneously permutes the representations and the multiset of eigenvalues (and the corresponding orders).

It is clear from the data in Table 2.9 that the representation $P\overline{\rho}_g^{(i)}$ is surjective for each $i = 1, \dots, 5$. Let L_i be the Galois extension of F cut out by $\ker(P\overline{\rho}_g^{(i)})$ for each i and let L be the compositum of the L_i . Since $\tau \in \mathrm{Aut}(H_g) = \mathrm{Gal}(H_g/E_g)$ cyclically permutes the maximal ideals $\mathfrak{m}_g^{(i)}$, the group $\mathrm{Gal}(F/\mathbb{Q})$ permutes the L_i and therefore L is Galois over \mathbb{Q} .

Now we show that $\text{Gal}(L/\mathbb{Q}) \cong 5 \cdot \text{PGL}_2(\mathbb{F}_5)^5$. It is enough to show that $\text{Gal}(L/F) \cong \text{PGL}_2(\mathbb{F}_5)^5$. We have a natural injection

$$j : \text{Gal}(L/F) \hookrightarrow \prod_{i=1}^5 \text{PGL}_2(\mathbb{F}_5)$$

$$\sigma \mapsto (\text{P}\bar{\rho}_g^{(i)} \sigma|_{L_i})_{i=1}^5.$$

Let $G = j^{-1}(\text{PSL}_2(\mathbb{F}_5)^5)$. Then since $\text{PSL}_2(\mathbb{F}_5)$ is simple, the restriction $j|_G$ of j to G has $j|_G(G) = \text{PSL}_2(\mathbb{F}_5)^m$ for some $1 \leq m \leq 5$, and hence $j(G) = \text{PGL}_2(\mathbb{F}_5)^m$ accordingly. But from Table 2.7, we see that for a prime \mathfrak{p} with $N\mathfrak{p} = 193$, we have that the elements $\bar{a}_{\mathfrak{p}}(g^{(i)})$ are pairwise distinct for $i = 1, \dots, 5$. Thus, we must have $m = 5$ since $\text{Out}(\text{PGL}_2(\mathbb{F}_5)) = \{1\}$ and inner automorphisms preserve the traces $\bar{a}_{\mathfrak{p}}(g^{(i)})$. Hence j is surjective as claimed, and we obtain the extension L as claimed.

Finally, we consider the representation $\bar{\rho}_g : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(k)$ where $k = \mathbb{F}_{5^{10}}$. Let $\beta \in \bar{\mathbb{F}}_5$ be a root of the polynomial $x^{10} + 3x^5 + 3x^4 + 2x^3 + 4x^2 + x + 2$. We compile the Hecke data for this case in Table 2.10.

$N\mathfrak{p}$	$\bar{a}_{\mathfrak{p}}(f)$	$o_{\mathfrak{p}}(f)$
5	1	—
7	$\beta^9 + 4\beta^7 + 2\beta^6 + \beta^4 + \beta$	4882813
32	$3\beta^9 + 4\beta^7 + \beta^6 + 3\beta^5 + 3\beta^4 + \beta^3 + 2\beta^2 + 3\beta + 4$	13
43	$4\beta^9 + 3\beta^7 + \beta^6 + 4\beta^5 + 4\beta^4 + 3\beta^2 + \beta + 4$	4882813
101	$\beta^9 + 4\beta^7 + 3\beta^6 + \beta^4 + 3\beta^3 + 3\beta^2 + 4\beta + 1$	4882813
107	$4\beta^9 + \beta^7 + 3\beta^6 + 4\beta^4 + 4\beta^3 + 3\beta^2 + \beta + 2$	1627604
149	$\beta^6 + \beta^3 + 2\beta^2 + 2\beta + 4$	4882813
151	$4\beta^9 + 2\beta^7 + 4\beta^6 + 4\beta^5 + 4\beta^4 + 2\beta^2 + \beta$	4882813
157	$\beta^9 + \beta^6 + 3\beta^5 + \beta^4 + 2\beta^3 + 4\beta^2 + 2\beta + 1$	1627604
193	$2\beta^9 + 4\beta^7 + \beta^6 + 2\beta^4 + 3\beta^3 + 3\beta + 1$	4882813
199	$3\beta^9 + 3\beta^7 + 3\beta^5 + 3\beta^4 + 3\beta^3 + 3\beta^2 + \beta$	4882813
243	3	6

Table 2.10: Hecke data for the representation $\bar{\rho}_g$ of level \mathfrak{p}_5 for $F \subset \mathbb{Q}(\zeta_{25})^+$ with $[F : \mathbb{Q}] = 5$

Arguments similar to the above show that the representation $\text{P}\bar{\rho}_g$ is surjective, and we obtain the field M as the fixed field of $\ker(\text{P}\bar{\rho}_g)$.

Combining these cases, we have proved the proposition. □

Remark 2.11. Because the extensions L_i in Case 2 in the proof above are of small degree, it may be possible to obtain polynomials for them. One possible way of doing this would be to adapt the work of Bosman [2] to the context of Shimura curves.

As for $p = 3$, we can estimate the root discriminants of these extensions by the result of Moon [29, Lemma 2.1], which gives $\delta_K, \delta'_K, \delta_L \leq 124.91$ and $\delta_M \leq 125.00$.

Degree 10. We conclude this section with the results of computations for the field $F = \mathbb{Q}(\zeta_{25})^+$, performed by Steve Donnelly. The space of Hilbert modular cusp forms $S_2(1)$ of level 1 for $F = \mathbb{Q}(\zeta_{25})^+$ has dimension 171; we compute with $S_2(1)$ using the totally definite quaternion algebra B over F ramified at all 10 real places of F and no finite place. The space $S_2(1)$ decomposes into irreducible Hecke constituents of dimensions 2, 4, 15 and 150 respectively, which we do not directly investigate. We instead consider the Galois representation (constructed by Taylor [36])

$$\bar{\rho}_{\mathbb{T} \otimes \mathbb{F}_5} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathbb{T} \otimes \mathbb{F}_5).$$

The \mathbb{F}_5 -algebra $\mathbb{T} \otimes \mathbb{F}_5$ has 17 non-Eisenstein maximal ideals. In Table 2.12, we group these maximal ideals according to the degree of their residue fields and note the action of $\text{Gal}(F/\mathbb{Q})$, generated by σ .

Inertial degree	Number of ideals	Galois action
2	10	σ permutes
5	2	σ permutes, σ^2 fixes
10	1	σ fixes
15	1	σ^2 fixes, but not σ
25	2	σ permutes, σ^2 fixes
40	1	σ fixes

Table 2.12: Hecke data for the representation $\bar{\rho}$ of level 1 for $F = \mathbb{Q}(\zeta_{25})^+$

Arguing as above, we find Galois extensions ramified only at 5 with Galois groups

$$10 \cdot \text{PGL}_2(\mathbb{F}_{5^2})^{10}, \quad 10 \cdot \text{PGL}_2(\mathbb{F}_{5^5})^2, \quad 10 \cdot \text{PGL}_2(\mathbb{F}_{5^{10}}), \\ 10 \cdot \text{PGL}_2(\mathbb{F}_{5^{15}}), \quad 10 \cdot \text{PGL}_2(\mathbb{F}_{5^{25}})^2, \quad 10 \cdot \text{PGL}_2(\mathbb{F}_{5^{40}}),$$

respectively. By the result of Fontaine [14, Corollaire 3.3.2], we find that the root discriminants of these fields are bounded by 115.336.

3. A NONSOLVABLE GALOIS NUMBER RAMIFIED AT 7?

To conclude our paper, we discuss the computational obstacles that we confront in applying the above techniques when $p = 7$.

In this case, the possible base fields are the subfields of $\mathbb{Q}(\zeta_{49})$ with degrees 3 and 7. First, we consider the field $F = \mathbb{Q}(\zeta_7)^+$. At level 1, the group $\Gamma(1)$ we encounter is the celebrated $(2, 3, 7)$ -triangle group [12]; the curve $X(1)$ is the Fuchsian group with the smallest possible area, and torsion-free (normal) subgroups of $\Gamma(1)$ are associated to Hurwitz curves, i.e., curves of genus g with the largest possible order $84(g - 1)$ of their automorphism group. In particular, $X(1)$ has genus 0, as does the curve $X_0(\mathfrak{p}_7)$ for $\mathfrak{p}_7 \mid 7$. At level \mathfrak{p}_7^2 ,

we find a genus 1 curve $X_0(\mathfrak{p}_7^2)$ (in fact, an elliptic curve since $\mathbb{Q}(\zeta_7)$ has class number 1 so there is an F -rational CM point on X) which corresponds to the base change to F of the classical modular curve $X_0(49)$, or equivalently (up to isogeny) the elliptic curve over \mathbb{Q} with complex multiplication by $\mathbb{Z}[(1 + \sqrt{-7})/2]$ and j -invariant -3375 . As for $p = 3$, it then follows from Buzzard, Diamond and Jarvis [5, Proposition 4.13(a)] that there are only reducible forms in higher powers of \mathfrak{p}_7 .

Next, let F be the subfield of degree 7 in $\mathbb{Q}(\zeta_{49})$ with discriminant $d_F = 13841287201 = 7^{12}$. The corresponding Shimura curve has area $275381/6$ and signature $(22864; 2^{71}, 3^{203})$, and this places it well outside the realm of practical computations using the above techniques. We must therefore leave the problem of finding a nonsolvable Galois number field ramified only at $p = 7$ for future investigation—it is conceivable that a good choice of group and base field, as explained in the introduction, will exhibit such a field.

We note finally that if one considers the weaker question of exhibiting a nonsolvable Galois number field which is unramified outside a finite set S of primes with $7 \in S$, such as $S = \{2, 7\}$ or $S = \{3, 7\}$, then already one can find such extensions by classical forms of weight 2 over \mathbb{Q} : see work of Wiese [39, Theorem 1.1] for a much more general result.

REFERENCES

- [1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.
- [2] J. Bosman, *A polynomial with Galois group $SL_2(\mathbb{F}_{16})$* , LMS J. Comput. Math. **10** (2007), 378–388.
- [3] S. Brueggeman, *Septic number fields which are ramified only at one small prime*, J. Symb. Comp. **31** (2001), 549–555.
- [4] S. Brueggeman, *The nonexistence of certain nonsolvable Galois extensions of number fields of small degree*, Int. J. Number Theory **1** (2005), no. 1, 155–160.
- [5] K. Buzzard, F. Diamond and F. Jarvis, *On Serre’s conjecture for mod ℓ Galois representations over totally real fields*, preprint, [arXiv:0810.2106v2](https://arxiv.org/abs/0810.2106v2).
- [6] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, ed. T. Shaska, Lecture Notes Series on Computing, vol. 13, 2005, 71–83.
- [7] H. Carayol, *Sur les représentations ℓ -adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. **19** (1986), 409–468.
- [8] L. Dembélé, *Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$* , Experiment. Math. **14** (2005), no. 4, 457–466.
- [9] L. Dembélé, *A non-solvable Galois extension of \mathbb{Q} ramified at 2 only*, preprint.
- [10] L.E. Dickson, *Linear groups: with an exposition of the Galois field theory*, Dover, New York, 1958.
- [11] N. Elkies, *Explicit modular towers*, Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing, 1997, 23–32.
- [12] N. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 1–47.
- [13] J. Ellenberg, *Serre’s conjecture over \mathbb{F}_9* . Ann. of Math. (2) **161** (2005), no. 3, 1111–1142.
- [14] J.-M. Fontaine, *Il n’y a pas de variété abélienne sur \mathbb{Z}* Invent. math. **81**, 1985, 515–538.

- [15] P. Gérardin, and J. P. Labesse, *The solution of a base change problem for $GL(2)$ (following Langlands, Saito, Shintani)*, Automorphic Forms, Representations, and L-functions, Proc. Symp. in Pure Math. **33**, Amer. Math. Soc., Providence R. I. , 1979.
- [16] M. Greenberg and J. Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, preprint.
- [17] B. Gross, *Modular forms (mod p) and Galois representations*, Inter. Math. Res. Notices **16** (1998), 865–875.
- [18] B. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.
- [19] H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, American Journal of Mathematics **103** no. 4 (1981), 727–776.
- [20] J. Jones, *Tables of number fields with prescribed ramification*, <http://math.asu.edu/~jj/numberfields/>.
- [21] J. Jones and D. Roberts, *Sextic number fields with discriminant $(-1)^j 2^a 3^b$* , CRM Proceedings, vol. 19, 141–172.
- [22] C. Khare and J.-P. Wintenberger, *On Serre’s conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals*, to appear in Ann. of Math.
- [23] A. Knapp, *Elliptic curves*. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992. xvi+427 pp.
- [24] J. Lansky and D. Pollack, *Hecke algebras and automorphic forms*. *Compositio Math.* **130** (2002), no. 1, 21–48.
- [25] S. Lesseni, *The non-existence of nonsolvable octic number fields ramified only at one small prime*, Math. Comp. **75** (2006), no. 255, 1519–1526.
- [26] S. Lesseni, *Nonsolvable nonic number fields ramified only at one small prime*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 617–625.
- [27] S. Lesseni, *Decic number fields ramified only at one small prime*, preprint, www.math.unicaen.fr/~lesseni/PAGEWEB/sujet.ps.
- [28] B. Mazur and A. Wiles, *Class fields of abelian extensions of \mathbb{Q}* , Invent. Math. **76** (1984) 179–330.
- [29] H. Moon, *Finiteness results on certain mod p Galois representations*. J. Number Theory **84** (2000), no. 1, 156–165.
- [30] R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), no. 3, 413–448.
- [31] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), no. 1, 197–230.
- [32] J.-P. Serre, *Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), exp. no. 416, *Lecture Notes in Math.*, vol. 317, Springer, Berlin, 1973, 319–338.
- [33] J.-P. Serre, *Abelian ℓ -adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, Wellesley, MA, A.K. Peters, 1997.
- [34] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*. *Ann. of Math. (2)* **85**(1967) 58–159.
- [35] J. Tate, *The non-existence of certain Galois extensions of \mathbb{Q} unramified outside 2*, Contemp. Math. **174** (1994), 153–156.
- [36] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), no. 2, 265–280.
- [37] J. Voight, *Computing fundamental domains for cofinite Fuchsian groups*, J. Théorie Nombres Bordeaux (2009), no. 2, 467–489.
- [38] J. Voight, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), 1155–1172.
- [39] G. Wiese, *On projective linear groups over finite fields as Galois groups over the rational numbers*. In: ‘Modular Forms on Schiermonnikoog’ edited by Bas Edixhoven, Gerard van der Geer and Ben Moonen. Cambridge University Press, 2008, 343–350.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK, ELLERNSTRASSE 29, D-45326 ESSEN,
GERMANY

E-mail address: `lassina.dembele@uni-due.de`

UNIVERSITY OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, AB, T2N 1N4,
CANADA

E-mail address: `mgreenbe@math.ucalgary.ca`

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, 16 COL-
CHESTER AVE, BURLINGTON, VT 05401, USA

E-mail address: `jvoight@gmail.com`