Rigid local systems, Hilbert modular forms, and Fermat's last theorem

Henri Darmon

March 3, 1999

Contents

Introduction

Historically, two approaches have been followed to study the classical Fermat equation $x^r + y^r = z^r$. The first, based on cyclotomic fields, leads to questions about abelian extensions and class numbers of $K = \mathbb{Q}(\zeta_r)$ and values of the Dedekind zeta-function $\zeta_K(s)$ at $s = 0$. Many open questions remain, such as Vandiver's conjecture that r does not divide the class number of $\mathbb{Q}(\zeta_r)^+$. The second approach is based on modular forms and the study of two-dimensional representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Even though two-dimensional representations are more subtle than abelian ones, it is by this route that Fermat's Last Theorem was finally proved. (Cf. [Fre], [Se2], [Ri2], [W3], and [TW], or [DDT] for a general overview.)

This article examines the equation

$$\boxed{x^p + y^q = z^r.} \tag{1}$$

Certain two-dimensional representations of $\mathrm{Gal}(\bar{K}/K)$, where K is the real subfield of a cyclotomic field, emerge naturally in the study of equation (1), giving rise to a blend of the cyclotomic and modular approaches. The special values $\zeta_K(-1)$ – which in certain cases are related to the class numbers of totally definite quaternion algebras over K – appear as *obstructions* to proving that (1) has no solutions. The condition that r is a regular prime also plays a key role in the analysis leading to one of our main results about the equation $x^p + y^p = z^r$ (theorem 3.22).

One is interested in *primitive* solutions (a, b, c) to equation (1), i.e., those satisfying $\gcd(a, b, c) = 1$. (Such a condition is natural in light of the abc conjecture for example. See also [Da1].) A solution is called *non-trivial* if $abc \neq 0$. It will be assumed from now on that the exponents p, q, and r are prime and that p is odd.

Let (a, b, c) be a non-trivial primitive solution to equation (1). One wishes to show that it does not exist. The program for obtaining the desired contradiction, following the argument initiated by Frey and brought to a successful conclusion by Wiles in the case of $x^p + y^p = z^p$, can be divided into four steps.

Step 1: (Frey, Serre) Associate to (a, b, c) a mod p Galois representation

$$\rho : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathbf{GL}_2(\mathbb{F})$$

having "very little ramification": i.e., whose ramification can be bounded precisely and *a priori* independently of the solution (a, b, c). Here K is a number field and $\mathbb{F}$ is a finite field. For the Fermat equation $x^p + y^p = z^p$, one may take $K = \mathbb{Q}$ and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$: the representation ρ is then obtained by considering the action of $G_{\mathbb{Q}}$ on the p-division points of the Frey elliptic curve $y^2 = x(x - a^p)(x + b^p)$. As will be explained in section 1, one is essentially forced to take $K = \mathbb{Q}(\zeta_q, \zeta_r)^+$ and $\mathbb{F}$ the residue field of K at a prime above p in studying equation (1).

Step 2: (Wiles) Prove that ρ is modular, i.e., arises from a Hilbert modular form on $\mathbf{GL}_2(K)$. In the setting of Fermat's equation, Wiles proves that all semistable elliptic curves over $\mathbb{Q}$ arise from a modular form, which implies the modularity of ρ.

Step 3: (Ribet) Assuming step 2, show that ρ comes from a modular form of small level, and deduce (in favorable circumstances) that its image is *small*, i.e., contained in a Borel subgroup or in the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F})$. In the setting of Fermat's equation, Ribet showed that ρ has to be *reducible*; for reasons that will be explained in section 3, one cannot rule out the case where the image of ρ is contained in the normalizer of a Cartan subgroup when dealing with equation (1).

Step 4: (Mazur) Show that the image of ρ is *large*; for example, that it contains $\mathbf{SL}_2(\mathbb{F})$. Historically, this is the step in the proof of Fermat's Last Theorem that was carried out first, in the seminal papers [Ma1] and [Ma2] which also introduced many of the tools used in steps 2 and 3.

In the classical setting, combining the conclusions of steps 3 and 4 leads to a contradiction and shows that (a, b, c) does not exist, thus proving Fermat's Last Theorem. In [Da2] and [DMr], it was observed that the program above can be used to show that $x^p + y^p = z^r$ has no non-trivial primitive solutions when $r = 2, 3$ and $p \geq 6 - r$. (The result for $r = 3$ being conditional on the Shimura-Taniyama conjecture, which is still unproved for certain elliptic curves whose conductor is divisible by 27.) The purpose of this article is to generalize the analysis to the general case of equation (1).

Sections 1, 2, 3, and 4 describe the generalizations of steps 1, 2, 3 and 4 respectively. As a concrete application, the main results of section 3 relate solutions to $x^p+y^p = z^r$ to questions about p-division points of certain abelian varieties with real multiplications by $\mathbb{Q}(\cos(2\pi/r))$. Alas, our understanding of these questions (and of the arithmetic of Hilbert modular forms over totally real fields) is too poor to yield unconditional statements. For the time being, the methods of this paper should be envisaged as as a way of tying equation (1) to questions which are more central, concerning Galois representations, modular forms, and division points of abelian varieties.

Acknowledgements: The author is grateful to F. Diamond, J. Ellenberg, A. Kraus, and K. Ribet for their helpful comments, and to N. Katz and J.-F. Mestre for pointing out a key construction used in section 1. The author greatly benefitted from the support of CICMA and the hospitality of the Université Paris VI (Jussieu) and the Institut Henri Poincaré where the work on this paper was started, and of the ETH in Zürich where it was completed. This work was partly funded by grants from NSERC and FCAR and by an Alfred P. Sloan research award.

1 Frey representations

1.1 Definition

If K is any field of characteristic 0, write $G_K := \mathrm{Gal}(\bar{K}/K)$ for its absolute Galois group. Typically, K will be a number field; let $K(t)$ be the function field over K in an indeterminate t. The group $G_{K(t)}$ fits into the exact sequence

$$1 \longrightarrow G_{\bar{K}(t)} \longrightarrow G_{K(t)} \longrightarrow G_K \longrightarrow 1.$$

Let $\mathbb{F}$ be a finite field, embedded in a fixed algebraic closure of its prime field.

Definition 1.1 *A* Frey representation *associated to the equation $x^p+y^q = z^r$ over K is a Galois representation*

$$\varrho = \varrho(t) : G_{K(t)} \longrightarrow \mathbf{GL}_2(\mathbb{F})$$

satisfying

1. *The restriction of ϱ to $G_{\bar{K}(t)}$ has trivial determinant and is irreducible. Let*

$$\bar{\varrho}^{geom} : G_{\bar{K}(t)} \longrightarrow \mathbf{PSL}_2(\mathbb{F})$$

   be the projectivization of this representation.

2. *The homomorphism $\bar{\varrho}^{geom}$ is unramified outside $\{0, 1, \infty\}$.*

3. *It maps the inertia groups at 0, 1 and ∞ to subgroups of $\mathbf{PSL}_2(\mathbb{F})$ of order p, q and r respectively.*

The characteristic of $\mathbb{F}$ is also called the characteristic *of the Frey representation.*

One should think of $\varrho = \varrho(t)$ as a one-parameter family of Galois representations of G_K indexed by the parameter t. Condition 1 in the definition ensures that this family has constant determinant but is otherwise "truly varying" with t. The motivation for the definition of $\varrho(t)$ is the following:

Lemma 1.2 *There exists a finite set of primes S of K depending on ϱ in an explicit way, such that, for all primitive solutions (a, b, c) to the generalized Fermat equation $x^p + y^q = z^r$, the representation $\rho := \varrho(a^p/c^r)$ has a quadratic twist which is unramified outside S.*

Sketch of proof: Let

$$\bar{\varrho} : G_{K(t)} \longrightarrow \mathbf{PGL}_2(\mathbb{F})$$

be the projective representation deduced from ϱ. The field fixed by the kernel of $\bar{\varrho}$ is a finite extension of $K(t)$, whose Galois group is identified with a subgroup G of $\mathbf{PGL}_2(\mathbb{F})$ by $\bar{\varrho}$; in other words, it is the function field of a G-covering of $\mathbf{P}_1$ over K. This covering is unramified outside $\{0, 1, \infty\}$ and its ramification indices are p, q and r above those three points: it is a G-covering of "signature (p, q, r)" in the sense of [Se1], sec. 6.4. The lemma now follows from a variant of the Chevalley-Weil theorem for branched coverings. (See for example [Be] or [Da1].)

Definition 1.3 *Two Frey representations ϱ_1 and ϱ_2 attached to equation (1) are said to be* equivalent *if their corresponding projective representations $\bar{\varrho}_1$ and $\bar{\varrho}_2$ differ by an inner automorphism of $\mathbf{PGL}_2(\bar{\mathbb{F}})$, i.e., if ϱ_1 is conjugate (over $\bar{\mathbb{F}}$) to a central twist of ϱ_2.*

To a Frey representation ϱ we assign a triple $(\sigma_0, \sigma_1, \sigma_\infty)$ of elements in $\mathbf{PSL}_2(\mathbb{F})$ of orders p, q and r satisfying $\sigma_0\sigma_1\sigma_\infty = 1$ as follows. (Cf. [Se1], ch. 6.) The element σ_j is defined as the image by $\bar{\varrho}^{geom}$ of a generator of the inertia subgroup of $G_{\bar{K}(t)}$ at $t = j$. The elements σ_0, σ_1, and σ_∞ are well-defined up to conjugation once primitive p, q and r-th roots of unity have been chosen. One can choose the decomposition groups in such a way that the relation $\sigma_0\sigma_1\sigma_\infty = 1$ is satisfied (cf. [Se1], th. 6.3.2.). The triple $(\sigma_0, \sigma_1, \sigma_\infty)$ is then well-defined up to conjugation.

If C_j is the conjugacy class of σ_j in $\mathbf{PSL}_2(\mathbb{F})$, one says that the Frey representation ϱ is of type (C_0, C_1, C_∞).

For the following definition, assume that the exponents p, q and r are odd, so that σ_0, σ_1 and σ_∞ lift to unique elements $\tilde{\sigma}_0$, $\tilde{\sigma}_1$ and $\tilde{\sigma}_\infty$ of $\mathbf{SL}_2(\mathbb{F})$ of orders p, q and r respectively.

Definition 1.4 *The Frey representation attached to $x^p + y^q = z^r$ is said to be* odd *if $\tilde{\sigma}_0\tilde{\sigma}_1\tilde{\sigma}_\infty = -1$, and is said to be* even *if $\tilde{\sigma}_0\tilde{\sigma}_1\tilde{\sigma}_\infty = 1$.*

1.2 Classification: the rigidity method

If n is an integer, let ζ_n denote a primitive nth root of unity. Given an odd prime p, write $p^* := (-1)^{(p-1)/2}p$, so that $\mathbb{Q}(\sqrt{p^*})$ is the quadratic subfield of $\mathbb{Q}(\zeta_p)$. We now turn to the classification of Frey representations, beginning with the classical Fermat equation.

The equation $x^p + y^p = z^p$

Theorem 1.5 *Let p be an odd prime. There is a unique Frey representation $\varrho(t)$ of characteristic p (up to equivalence) associated to the Fermat equation $x^p + y^p = z^p$. One may take $K = \mathbb{Q}$ and $\mathbb{F} = \mathbb{F}_p$, and the representation $\varrho(t)$ is odd.*

Remark: This theorem is originally due to Hecke [He], where it is expressed as a characterization of a certain field of modular functions of level p.

Proof of theorem 1.5: Set $\mathbb{F} = \mathbb{F}_p$. We begin by classifying conjugacy classes of triples σ_0, σ_1 and σ_∞ of elements of order p in $\mathbf{PSL}_2(\mathbb{F})$ satisfying $\sigma_0\sigma_1\sigma_\infty = 1$. There are two conjugacy classes of elements of order p in $\mathbf{PSL}_2(\mathbb{F})$, denoted pA and pB respectively. The class pA (resp. pB) is represented by an upper-triangular unipotent matrix whose upper right-hand entry is a square (resp. a non-square). These two classes are *rational* over $\mathbb{Q}(\sqrt{p^*})$ in the sense of [Se1], sec. 7.1, and are interchanged by the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ as well as by the non-trivial outer automorphism of $\mathbf{PSL}_2(\mathbb{F})$. Lift σ_0, σ_1, and σ_∞ to elements $\tilde\sigma_0$, $\tilde\sigma_1$ and $\tilde\sigma_\infty$ of order p in $\mathbf{SL}_2(\mathbb{F})$. The group $\mathbf{SL}_2(\mathbb{F})$ acts on the space $V = \mathbb{F}^2$ of column vectors with entries in $\mathbb{F}$. Since $\tilde\sigma_j$ is unipotent, there are non-zero vectors v_1 and v_2 in V which are fixed by $\tilde\sigma_0$ and $\tilde\sigma_1$ respectively. Because σ_0 and σ_1 do not commute, the vectors v_1 and v_2 form a basis for V. Scale v_2 so that $\tilde\sigma_0$ is expressed by the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in this basis; let $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ be the matrix representing $\tilde\sigma_1$. Since $\tilde\sigma_\infty$ has trace 2, the relation $\tilde\sigma_0\tilde\sigma_1 = \tilde\sigma_\infty^{-1}$ forces $x = 0$, which is impossible since σ_1 is of order p. Hence there are no even Frey representations of characteristic p. The relation $\tilde\sigma_0\tilde\sigma_1 = -\tilde\sigma_\infty^{-1}$ gives $x = -4$. Note that the resulting elements σ_0, σ_1, and σ_∞ belong to the same conjugacy class in $\mathbf{PSL}_2(\mathbb{F})$. It is well-known that they generate $\mathbf{PSL}_2(\mathbb{F})$. Hence there are exactly two distinct conjugacy classes of surjective homomorphisms

$$\bar\varrho_A^{geom}, \bar\varrho_B^{geom} : G_{\bar{\mathbb{Q}}(t)} \longrightarrow \mathbf{PSL}_2(\mathbb{F}),$$

of type (pA, pA, pA) and (pB, pB, pB) respectively, which are interchanged by the outer automorphism of $\mathbf{PSL}_2(\mathbb{F})$. By the rigidity theorem of Belyi, Fried, Thompson and Matzat (cf. [Se1], sec. 7), $\bar\varrho_A^{geom}$ and $\bar\varrho_B^{geom}$ extend uniquely to homomorphisms

$$\bar\varrho_A, \bar\varrho_B : G_{\mathbb{Q}(t)} \longrightarrow \mathbf{PGL}_2(\mathbb{F}) = \mathrm{Aut}(\mathbf{PSL}_2(\mathbb{F}))$$

which are conjugate to each other.Thus there is at most one Frey representation ϱ attached to $x^p+y^p = z^p$, whose corresponding projective representation $\bar\varrho$ is conjugate to $\bar\varrho_A$ and $\bar\varrho_B$. To prove the existence of ϱ, it is necessary to show that $\bar\varrho_A$ (say) lifts to a linear representation $G_{\mathbb{Q}(t)} \longrightarrow \mathbf{GL}_2(\mathbb{F})$. The obstruction to such a lifting is given by a cohomology class c in $H^2(\mathbb{Q}(t), \pm 1)$. We note that (for $j = 0$, 1, and ∞) the homomorphism $\bar\varrho_A$ maps the decomposition group at $t = j$ to the normalizer of σ_j, which is the image in $\mathbf{PGL}_2(\mathbb{F}_p)$ of a Borel subgroup B of upper triangular matrices. Since the inclusion $\mathbb{F}_p^\times \longrightarrow B$ splits, it follows that the restrictions c_0, c_1 and c_∞ of the cohomology class c in $H^2(\mathbb{Q}((t)), \pm 1)$, $H^2(\mathbb{Q}((t-1)), \pm 1)$ and $H^2(\mathbb{Q}((1/t)), \pm 1)$ vanish. In particular, c has trivial "residues" at $t = 0$, 1,

∞ in the sense of [Se3], chapter II, annexe §2. Hence c is "constant", i.e., comes from $H^2(\mathbb{Q}, \pm 1)$ by inflation ([Se3], chapter II, annexe, §4). Therefore it vanishes, since $H^2(\mathbb{Q}, \pm 1)$ injects in $H^2(\mathbb{Q}((t)), \pm 1)$.

The equation $x^p + y^p = z^r$

Let us now turn to the equation $x^p + y^p = z^r$, where r and p are distinct primes. One is faced here with the choice of considering either Frey representations of characteristic p, or of characteristic r. From now on, we adopt the convention that the prime p is always used to denote the characteristic of the Frey representation, so that the equations $x^p + y^p = z^r$ and $x^r + y^r = z^p$ will require seperate consideration.

The following theorem is inspired from the proof given in [Se1], prop. 7.4.3 and 7.4.4 for the case $r = 2$ and $r = 3$, the general case following from an identical argument. (See also [DMs].)

Theorem 1.6 *Suppose that r and p are distinct primes and that $p \neq 2$. There exists a Frey representation of characteristic p over K associated to $x^p + y^p = z^r$ if and only if*

1. *The field $\mathbb{F}$ contains the residue field of $\mathbb{Q}(\zeta_r)^+$ at a prime $\mathfrak{p}$ above p, and*

2. *The field K contains $\mathbb{Q}(\zeta_r)^+$.*

When these two conditions are satisfied, there are exactly $r - 1$ Frey representations up to equivalence. When $r \neq 2$, exactly $(r-1)/2$ of these are odd, and $(r-1)/2$ are even.

Proof: For condition 3 in definition 1.1 to be satisfied, it is necessary that $\mathbf{PSL}_2(\mathbb{F})$ contain an element of order r. This is the reason for condition 1 in theorem 1.6. Condition 2 arises from the fact that (for $r \neq 2$) the $(r-1)/2$ distinct conjugacy classes of elements of order r in $\mathbf{PSL}_2(\mathbb{F})$ are rational over $\mathbb{Q}(\zeta_r)^+$ and are not rational over any smaller extension. Assume conversely that conditions 1 and 2 are satisfied. Let σ_0, σ_1, and σ_∞ be chosen as in the proof of theorem 1.5, and let $\tilde{\sigma}_j$ be the lift of σ_j to $\mathbf{SL}_2(\mathbb{F})$ of order p when $j = 0, 1$. Finally, let $\tilde{\sigma}_\infty$ be a lift of σ_∞ to an element of order r if r is odd, and to an element of order 4 if $r = 2$. Let $\bar{\omega} \in \mathbb{F}$ be the trace of $\tilde{\sigma}_\infty$. When $r = 2$ one has $\bar{\omega} = 0$, and when r is odd, $\bar{\omega}$ is of the form $\varphi(\zeta_r + \zeta_r^{-1})$ where φ is a homomorphism from $\mathbb{Z}[\zeta_r + \zeta_r^{-1}]^+$ to $\mathbb{F}$. Note that there are exactly $(r-1)/2$ such φ's. One now finds, as in the proof of theorem 1.5, that $(\tilde\sigma_0, \tilde\sigma_1, \tilde\sigma_\infty)$ is conjugate to one of the following two triples:

$$\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -(2+\bar\omega) & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -2-\bar\omega & 1+\bar\omega \end{pmatrix}\right),$$

$$\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -(2-\bar\omega) & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 2-\bar\omega & -1+\bar\omega \end{pmatrix}\right).$$

When $r = 2$, these triples are equal in $\mathbf{PSL}_2(\mathbb{F})$. When r is odd, they are distinct. An argument based on rigidity as in the proof of theorem 1.5 produces $(r-1)$ inequivalent homomorphisms from $G_{K(t)}$ to $\mathbf{GL}_2(\mathbb{F})$, yielding the desired odd and even Frey representations. These Frey representations will be constructed explicitly in section 1.3 (cf. lemma 1.9 and theorem 1.10).

The equation $x^r + y^r = z^p$

Theorem 1.7 *Suppose that r and p are distinct odd primes. There exists a Frey representation of characteristic p over K associated to $x^r + y^r = z^p$ if and only if*

1. *The field $\mathbb{F}$ contains the residue field of $\mathbb{Q}(\zeta_r)^+$ at a prime $\mathfrak{p}$ above p, and*
2. *The field K contains $\mathbb{Q}(\zeta_r)^+$.*

When these two conditions are satisfied, there are exactly $(r-1)(r-2)/2$ inequivalent Frey representations: $(r-1)^2/4$ odd representations, and $(r-1)(r-3)/4$ even representations.

Although the conclusion is somewhat different, the proof of theorem 1.7 follows the same ideas as the proof of theorem 1.6. Each triple (C_0, C_1, pA), where C_0 and C_1 each range over the $(r-1)/2$ possible conjugacy classes of elements of order r in $\mathbf{PSL}_2(\mathbb{F})$ gives rise to a unique odd and even projective representation of $G_{K(t)}$ of type (C_0, C_1, pA), with one caveat: there is no even representation of type (C_0, C_1, pA) when $C_0 = C_1$.

The equation $x^p + y^q = z^r$
We finally come to the general case of equation (1). Assume that the exponents p, q and r are distinct primes and that p is odd.

Theorem 1.8 *There exists a Frey representation of characteristic p over K associated to $x^p + y^q = z^r$ if and only if*

1. *The field $\mathbb{F}$ contains the residue fields of $\mathbb{Q}(\zeta_q)^+$ and of $\mathbb{Q}(\zeta_r)^+$ at a prime $\mathfrak{p}$ above p, and*

2. *The field K contains $\mathbb{Q}(\zeta_q)^+$ and $\mathbb{Q}(\zeta_r)^+$.*

When these two conditions are satisfied, there are $(r-1)(q-1)/2$ inequivalent Frey representations over $\mathbb{Q}(\zeta_q, \zeta_r)^+$. If $q, r \neq 2$, then $(r-1)(q-1)/4$ of these are odd, and $(r-1)(q-1)/4$ are even.

The proof is the same as for theorems 1.5, 1.6 and 1.7.

1.3 Construction: hypergeometric abelian varieties

The equation $x^p + y^p = z^p$
One can construct the Frey representation $\varrho(t)$ of theorem 1.5 explicitly, by considering the Legendre family of elliptic curves

$$J = J(t) : y^2 = x(x-1)(x-t).$$

It is an elliptic curve over $\mathbb{Q}(t)$ which has multiplicative reduction at $t = 0$ and 1, and potentially multiplicative reduction at $t = \infty$. The module $J[p]$ of its p-division points is a two-dimensional $\mathbb{F}$-vector space on which $G_{\mathbb{Q}(t)}$ acts linearly. The corresponding representation $\varrho(t)$ is the Frey representation of characteristic p attached to $x^p + y^p = z^p$.

The equation $x^p + y^p = z^r$
When $r = 2$, let $C_2(t)$ be the elliptic curve over $\mathbb{Q}(t)$ given by the equation

$$C_2(t) \quad : \quad y^2 = x^3 + 2x^2 + tx. \tag{2}$$

Lemma 1.9 *The mod p Galois representation associated to C_2 is the Frey representation associated to $x^p + y^p = z^2$.*

The proof of this lemma is omitted: it follows the same ideas but is simpler than the proof of theorem 1.10 below for the case of odd r, for which all the details are given.

Suppose now that r is an odd prime. Let $\omega_j = \zeta_r^j + \zeta_r^{-j}$, and write ω for ω_1, so that $K = \mathbb{Q}(\omega)$ is the real subfield of the cyclotomic field $\mathbb{Q}(\zeta_r)$. Let $d = (r-1)/2$ be the degree of K over $\mathbb{Q}$.

Let $g(x) = \prod_{j=1}^{d}(x+\omega_j)$ be the characteristic polynomial of $-\omega$, and let $f(x)$ be an antiderivative of $\pm r g(x)g(-x)$; for example, we will take:

$$f(x) = xg(x^2-2) = g(-x)^2(x-2)+2 = g(x)^2(x+2)-2.$$

Following [TTV], consider the following hyperelliptic curves over $\mathbb{Q}(t)$ of genus d:

$$C_r^-(t) \quad : \quad y^2 = f(x)+2-4t, \tag{3}$$
$$C_r^+(t) \quad : \quad y^2 = (x+2)(f(x)+2-4t). \tag{4}$$

Let $J_r^- = J_r^-(t)$ and $J_r^+ = J_r^+(t)$ be their jacobians over $\mathbb{Q}(t)$.

In [TTV], Tautz, Top, and Verberkmoes show that these families of hyperelliptic curves have real multiplications by K, i.e., that

$$\mathrm{End}_{\bar{\mathbb{Q}}(t)}(J_r^\pm) = \mathcal{O}_K. \tag{5}$$

Their proof shows that the endomorphisms of $J_r^\pm$ are in fact defined over K, and that the natural action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{End}_{K(t)}(J_r^\pm)$ and on $\mathcal{O}_K$ are compatible with the identification of equation (5) above, which is canonical. (See also [DMs].)

Fix a residue field $\mathbb{F}$ of K at a prime above p, and let φ be a homomorphism of $\mathcal{O}_K$ to $\mathbb{F}$. The module $J_r^\pm[p]\otimes_\varphi\mathbb{F}$ is a two-dimensional $\mathbb{F}$-vector space on which G_K acts $\mathbb{F}$-linearly. By choosing an $\mathbb{F}$-basis for this vector space one obtains Galois representations (depending on the choice of φ, although this dependence is supressed from the notations)

$$\varrho_r^\pm(t) : G_{K(t)} \longrightarrow \mathbf{GL}_2(\mathbb{F}).$$

Theorem 1.10 *The representations $\varrho_r^-(t)$ and $\varrho_r^+(t)$ (as φ varies over the $(r-1)/2$ possible homomorphisms from $\mathcal{O}_K$ to $\mathbb{F}$) are the $r-1$ distinct Frey representations of characteristic p associated to $x^p+y^p=z^r$. The representations ϱ_r^- are odd, and the representations ϱ_r^+ are even.*

Proof: (See also [DMs], prop. 2.2, 2.3.) Observe that

1. Outside of $t = 0, 1, \infty$, the curves $C_r^{\pm}(t)$ have good reduction. Hence $\varrho_r^{\pm}(t)$ satisfies condition 2 in definition 1.1 of a Frey representation.

2. The $C_r^{\pm}(t)$ are *Mumford curves* over $\mathrm{Spec}(K[[t]])$ and $\mathrm{Spec}(K[[t-1]])$, i.e., the special fiber of $C_r^{\pm}(t)$ over these bases is a union of projective lines intersecting transversally at ordinary double points. For example, replacing y by $2y + (x+2)g(x)$ yields the following equation for $C_r^+(t)$, whose special fiber is the union of two projective lines crossing at the $d+1$ ordinary double points $(x, y) = (-2, 0)$, $(-\omega_j, 0)$:

$$y^2 + (x+2)g(x)y + t(x+2) = 0. \tag{6}$$

Likewise, replacing y by $2y + xg(-x)$ gives the following equation for $C_r^+(t)$ over $\mathrm{Spec}(K[[t-1]])$:

$$y^2 + xg(-x)y + g(-x)^2 + (x+2)(t-1) = 0. \tag{7}$$

Its special fiber is a projective line with the d ordinary double points $(x, y) = (\omega_j, 0)$. A similar analysis can be carried out for $C_r^-(t)$. By Mumford's theory, the Jacobians $J_r^{\pm}(t)$ have purely toric reduction at $t = 0$ and $t = 1$, and hence $\varrho_r^{\pm}$ maps the inertia at these points to unipotent elements of $\mathbf{SL}_2(\mathbb{F})$.

3. The curve $C_r^-(t)$ has a quadratic twist which acquires good reduction over $K[[(1/t)^{\frac{1}{r}}]]$, while $C_r^+(t)$ acquires good reduction over this base. For example, setting $\tilde{t} = (1/t)^{\frac{1}{r}}$ and replacing x by $1/x$ and y by $(2y+1)/x^{(r+1)/2}$ in equation (4) for $C_r^+(t)$ gives the model:

$$y^2 + y = x^r + \tilde{t}h(x, y, \tilde{t}/2), \tag{8}$$

where h is a polynomial with coefficients in $\mathbb{Z}$. Therefore ϱ_r^- (resp. ϱ_r^+) maps the inertia at $t = \infty$ to an element of order $2r$ (resp. r) of $\mathbf{SL}_2(\mathbb{F})$ whose image in $\mathbf{PSL}_2(\mathbb{F})$ is of order r.

It follows from 2 and 3 that $\varrho_r^{\pm}(t)$ satisfies condition 3 in definition 1.1.

4. A strong version of property 1 now follows from the following group-theoretic lemma:

Lemma 1.11 *Let σ_0, σ_1, and σ_∞ be elements of $\mathbf{PSL}_2(\mathbb{F})$ of order p, p, and r satisfying $\sigma_0\sigma_1\sigma_\infty = 1$. Then σ_0, σ_1, and σ_∞ generate $\mathbf{PSL}_2(\mathbb{F})$ unless $(p, r) = (3, 5)$ and $\tilde{\sigma}_0\tilde{\sigma}_1\tilde{\sigma}_\infty = -1$, in which case they generate an exceptional subgroup isomorphic to $A_5 \subset \mathbf{PSL}_2(\mathbb{F}_9)$.*

Proof: Let G be the subgroup of $\mathbf{PSL}_2(\mathbb{F})$ generated by the images of σ_0, σ_1, and σ_∞. The proper maximal subgroups of $\mathbf{PSL}_2(\mathbb{F})$ are conjugate to one of the groups in the following list (Cf. for example [Hu], ch. II.8 th. 8.27)

1. The Borel subgroup of upper triangular matrices.

2. The normalizer of a Cartan subgroup.

3. A group isomorphic to $\mathbf{PSL}_2(\mathbb{F}')$ or $\mathbf{PGL}_2(\mathbb{F}')$ for some $\mathbb{F}' \subset \mathbb{F}$.

4. One of the exceptional subgroups A_4, S_4 or A_5.

The fact that G contains two unipotent elements that do not commute rules out the possibility that G is contained in a Borel subgroup or the normalizer of a Cartan subgroup, and the fact that it contains an element of order r rules out the groups isomorphic to $\mathbf{PSL}_2(\mathbb{F}')$ or $\mathbf{PGL}_2(\mathbb{F}')$. Obviously, G can be contained in one of the exceptional subgroups only if both p and r are ≤ 5, i.e., if $(r,p) = (2,3)$, $(2,5)$, $(3,5)$ or $(5,3)$. In the first three cases G is isomorphic to $\mathbf{PSL}_2(\mathbb{F}_p)$. (Note that $\mathbf{PSL}_2(\mathbb{F}_3) \simeq A_4$ and that $\mathbf{PSL}_2(\mathbb{F}_5) \simeq A_5$.) When $(r,p) = (5,3)$ and $\tilde{\sigma}_0\tilde{\sigma}_1\tilde{\sigma}_\infty = -1$, one checks directly that G is isomorphic to the exceptional subgroup $A_5 \subset \mathbf{PSL}_2(\mathbb{F}_9)$.

The equation $x^r + y^r = z^p$

Choose a parameter $j \in \{1, 3, 5, \dots, r-2\}$, and define curves over the function field $\mathbb{Q}(t)$ by the equations:

$$\begin{aligned} X^-_{r,r}(t) \quad &: \quad y^{2r} = u^2 x^{j-2}\left(\frac{x-1}{x-u}\right)^{j+2}, \\ X^+_{r,r}(t) \quad &: \quad y^{r} = u^2 x^{j-2}\left(\frac{x-1}{x-u}\right)^{j+2}, \qquad u = \frac{t}{t-1}. \end{aligned}$$

A role will be played in our construction by the Legendre family $J(t)$ of elliptic curves, whose equation we write in the more convenient form:

$$J(t) : y^2 = u^2 x^{j-2}\left(\frac{x-1}{x-u}\right)^{j+2}.$$

These curves are equipped with the following structures.

1. A canonical action of μ_r on $X^-_{r,r,}$ and $X^+_{r,r,}$ defined by

$$\zeta(x,y) = (x, \zeta y), \qquad \zeta \in \mu_r.$$

2. An involution τ on $X^-_{r,r}$, $X^+_{r,r}$ and J defined by

$$\tau(x,y) = (u/x, 1/y).$$

This involution has two fixed points on $X^+_{r,r}$, and no fixed points on $X^-_{r,r}$ and on J.

3. Maps $\pi : X^-_{r,r} \longrightarrow J$, and $\pi_r : X^-_{r,r} \longrightarrow X^+_{r,r}$ defined by

$$\pi(x,y) = (x, y^r); \qquad \pi_r(x,y) = (x, y^2).$$

These maps obey the rules

$$\tau\zeta = \zeta^{-1}\tau, \qquad \pi\zeta = \pi, \quad \pi_r\zeta = \zeta^2\pi_r, \qquad \tau\pi = \pi\tau, \quad \tau\pi_r = \pi_r\tau.$$

Let

$$C^{\pm}_{r,r} = X^{\pm}_{r,r}/\tau, \qquad J' = J/\tau.$$

The maps π and π_r commute with τ and hence induce maps from $C^-_{r,r}$ to J' and $C^+_{r,r}$ respectively, which will be denoted by the same letters by abuse of notation. Write π^* and π_r^* for the maps between the Jacobians of J', $C^+_{r,r}$ and $C^-_{r,r}$ induced by π and π_r respectively by contravariant functoriality. Finally let $J^+_{r,r}$ denote the Jacobian of $C^+_{r,r}$, and let $J^-_{r,r}$ be the quotient of the Jacobian $\mathrm{Jac}(C^-_{r,r})$ of $C^-_{r,r}$ defined by

$$J^-_{r,r} := \mathrm{Jac}(C^-_{r,r})/(\pi^*(J') + \pi_r^*(J^+_{r,r})).$$

Proposition 1.12 *The abelian varieties $J^+_{r,r}$ (resp. $J^-_{r,r}$) have dimension equal to $(r-1)/2$ when $j \in \{1,3,5,\ldots,r-4\}$ (resp. $j \in \{1,3,5,\ldots,r-2\}$). In these cases there is a natural identification*

$$\mathrm{End}_K(J^{\pm}_{r,r}) = \mathcal{O}_K$$

which is compatible with the action of $\mathrm{Gal}(K/\mathbb{Q})$ *on each side.*

Proof: The computation of the dimension of $J^{\pm}_{r,r}$ is a direct calculation based on the Riemann-Hurwitz formula. To study the endomorphism rings of $J^{\pm}_{r,r}$, let

$$\eta_\zeta : X^{\pm}_{r,r} \longrightarrow C^{\pm}_{r,r} \times C^{\pm}_{r,r}$$

be the correspondence from $C^{\pm}_{r,r}$ to $C^{\pm}_{r,r}$ given by $\eta_\zeta := (\mathrm{pr}, \mathrm{pr} \circ \zeta)$, where pr is the natural projection of $X^{\pm}_{r,r}$ to $C^{\pm}_{r,r}$. The resulting endomorphism η_ζ of $\mathrm{Pic}(C^{\pm}_{r,r})$ is defined (on effective divisors) by the equation:

$$\eta_\zeta(\mathrm{pr}P) = \mathrm{pr}(\zeta P) + \mathrm{pr}(\zeta^{-1}P).$$

The commutation relations between ζ and π and π_r show that

$$\pi\eta_\zeta = 2\pi, \qquad \pi_r\eta_\zeta = \eta_{\zeta^2}\pi_r.$$

Hence the subvarieties $\pi^*(J')$ and $\pi_r^*(J^+_{r,r})$ of $\mathrm{Jac}(C^-_{r,r})$ are preserved by these correspondances, which induce endomorphisms of $J^-_{r,r}$ as well as of $J^+_{r,r}$. The assignment $\zeta \mapsto \eta_\zeta$ yields an inclusion of $\mathcal{O}_K$ into $\mathrm{End}(J^{\pm}_{r,r})$, which is an isomorphism since $J^{\pm}_{r,r}$ is not of CM type. The result follows.

Choose as before a homomorphism $\varphi : \mathcal{O}_K \longrightarrow \mathbb{F}$ and let $\varrho^{\pm}_{r,r}$ be the Galois representations obtained from the action of $G_{K(t)}$ on the modules $J^{\pm}_{r,r}[p] \otimes_\varphi \mathbb{F}$. Note that the representations $\varrho^{\pm}_{r,r}$ depend on the choice of the parameter j as well as on the choice of φ.

Theorem 1.13 *1. The representations $\varrho^-_{r,r}$, as j ranges over $\{1, 3, \dots, r-2\}$ and φ over the different homomorphisms $\mathcal{O}_K \longrightarrow \mathbb{F}$, are the $(r-1)^2/4$ distinct odd Frey representations attached to $x^r + y^r = z^p$.*

2. The representations $\varrho^+_{r,r}$, as j ranges over $\{1, 3, \dots, r-4\}$ and φ over the different homomorphisms $\mathcal{O}_K \longrightarrow \mathbb{F}$, are the $(r-1)(r-3)/4$ distinct even Frey representations attached to $x^r + y^r = z^p$.

Proof: See for example [Ka], th. 5.4.4, or [CW].

Remarks:
1. The periods of the abelian varieties $J^{\pm}_{r,r}$, as functions of the variable t, are values of certain classical hypergeometric functions. These functions arise as solutions of a second-order differential equation having only regular singularities at $t = 0$, 1, and ∞ and monodromies of order r at 0 and 1 and quasi-unipotent monodromy (with eigenvalue -1 for the odd Frey representation, and 1 for the even Frey representation) at $t = \infty$.

2. Katz's proof, which is based on his analysis of the behaviour of the local monodromy of sheaves under the operation of "convolution on G_m", is significantly more general than the rank 2 case is used in our application. It also gives a motivic construction of rigid local systems over $\mathbf{P}^1 - \{0, 1, \infty\}$ of any rank. Katz's "hypergeometric motives" suggest the possibility of connecting equation (1) to higher-dimensional Galois representations, for which questions of modularity are less well understood.

3. In computing finer information such as the conductors of the Frey representations $\varrho^{\pm}_{r,r}(a^r/c^p)$ at the "bad primes", it may be desirable to have a direct proof of theorem 1.13 along the lines of the proof of theorem 1.10. The details, which are omitted, will be given in [DK].

The equation $x^p + y^q = z^r$

The notion of "hypergeometric abelian variety" explained in [Ka], th. 5.4.4 and [CW], sec. 3.3 also yields a construction of the $(r-1)(q-1)/2$ Frey representations of characteristic p over $K = \mathbb{Q}(\zeta_q, \zeta_r)^+$ associated to $x^p + y^q = z^r$, when p, q, r are distinct primes and p is odd. We will not describe the construction here, referring instead to [Ka], sec. 5.4 for the details. All that will be used in the sequel is the following theorem:

Theorem 1.14 *If $q, r \neq 2$ (resp. $q = 2$), there exist abelian varieties $J^-_{q,r}$ and $J^+_{q,r}$ (resp. $J_{2,r}$) over $\mathbb{Q}(t)$ of dimension $(r-1)(q-1)/2$ satisfying*

$$\mathrm{End}_K(J^{\pm}_{q,r}) = \mathcal{O}_K, \qquad (\textit{resp. } \mathrm{End}(J_{2,r}) = \mathcal{O}_K)$$

whose mod p representations give rise to all the Frey representations in characteristic p associated to $x^p + y^q = z^r$. More precisely, fix a residue field $\mathbb{F}$ of K at p, and let φ be a homomorphism of $\mathbb{Q}(\zeta_q)^+\mathbb{Q}(\zeta_r)^+$ to $\mathbb{F}$. There are $(r-1)(q-1)/4$ (resp. $(r-1)/2$) such φ's. Extending φ to a homomorphism $\mathcal{O}_K \longrightarrow \mathbb{F}$, let $\varrho^{\pm}_{q,r}$ (resp. $\varrho_{2,r}$) be the Galois representation obtained from the action of $G_{K(t)}$ on $J^{\pm}_{q,r}[p] \otimes_\varphi \mathbb{F}$ (resp. $J_{2,r}[p] \otimes_\varphi \mathbb{F}$). Then the representations $\varrho^{\pm}_{q,r}$ (resp. $\varrho_{2,r}$) are the distinct Frey representations of characteristic p attached to $x^p + y^q = z^r$. The representations $\varrho^-_{q,r}$ (resp. $\varrho^+_{q,r}$) are odd (resp. even).

Frey abelian varieties

We may now assign to each solution (a, b, c) of equation (1) a *"Frey abelian variety"*, obtained as a suitable quadratic twist of the abelian variety $J(a^p/b^p)$

for $x^p + y^p = z^p$, $J_r^{\pm}(a^p/c^r)$ for $x^p + y^p = c^r$, $J_{r,r}^{\pm}(a^r/c^p)$ for $x^r + y^r = z^p$, and $J_{q,r}^{\pm}(a^p/c^r)$ for $x^p + y^q = z^r$. These twist are chosen in such a way as to make the corresponding mod p representations as "little ramified" as possible, in accord with lemma 1.2.

The equation $x^p + y^p = z^p$
If (a, b, c) is a solution to the Fermat equation $x^p + y^q = z^r$, the elliptic curve $J(a^p/c^p)$ has equation $y^2 = x(x-1)(x - a^p/c^p)$, which is a quadratic twist (over $\mathbb{Q}(\sqrt{c})$) of the familiar Frey curve

$$J(a, b, c) : y^2 = x(x + a^p)(x - b^p).$$

Let ρ be the associated mod p representation of $G_{\mathbb{Q}}$.

The equation $x^p + y^p = z^r$
When $r = 2$, we associate to a solution (a, b, c) of equation (1) the following twist of $C_2(a^p/c^2)$):

$$C_2(a, b, c) : y^2 = x^3 + 2cx^2 + a^p x. \tag{9}$$

When r is odd, the Frey hyperelliptic curves $C_r^-(a, b, c)$ and $C_r^+(a, b, c)$ are given by the equations

$$\begin{aligned} C_r^-(a, b, c) \quad &: \quad y^2 = c^r f(x/c) - 2(a^p - b^p), \qquad (10) \\ C_r^+(a, b, c) \quad &: \quad y^2 = (x + 2c)(c^r f(x/c) - 2(a^p - b^p)). \qquad (11) \end{aligned}$$

Note that $C_r^-(a, b, c)$ is a non-trivial quadratic twist of $C_r^-(a^p/c^r)$ (over the field $\mathbb{Q}(\sqrt{c})$), while $C_r^+(a, b, c)$ is isomorphic to $C_r^+(a^p/c^r)$ over $\mathbb{Q}$.

Here are the equations of $C_r^-(a, b, c)$ for the first few values of r:

$$\begin{aligned} r = 3: &\quad y^2 = x^3 - 3c^2x - 2(a^p - b^p). \\ r = 5: &\quad y^2 = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p). \\ r = 7: &\quad y^2 = x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^p - b^p). \end{aligned}$$

Let $J_r^{\pm}(a, b, c)$ be the Jacobian of $C_r^{\pm}(a, b, c)$, and let $\rho_r^{\pm}$ be the corresponding mod p Galois representations (which depend, as always, on the choice of a homomorphism φ from $\mathcal{O}_K$ to $\mathbb{F}$). The representation $\rho_r^{\pm}$ is a quadratic twist of $\varrho_r^{\pm}(a^p/c^r)$.

We do not write down the equations for $J_{r,r}^{\pm}(a, b, c)$ or $J_{q,r}^{\pm}(a, b, c)$, as we will have no further use for them in this article. A more careful study of the

Frey abelian varieties $J^{\pm}_{r,r}(a,b,c)$ associated to $x^r + y^r = z^p$ is carried out in [DK].

Conductors
We say that a Galois representation $\rho : G_K \longrightarrow \mathbf{GL}_2(\mathbb{F})$ is *finite* at a prime λ if its restriction to a decomposition group at λ comes from the Galois action on the points of a finite flat group scheme over $\mathcal{O}_{K,\lambda}$. When $\ell \neq p$, this is equivalent to ρ being unramified. Let $N(\rho)$ denote the *conductor* of ρ, as defined for example in [DDT]. In particular, $N(\rho)$ is divisible precisely by the primes for which ρ is not finite.

The equation $x^p + y^p = z^p$
By interchanging a, b and c and changing their signs if necessary so that a is even and $b \equiv 3 \pmod 4$, one finds that the conductor of $\rho := \varrho(a,b,c)$ is equal to 2 (cf. [Se2]). The presence of the extraneous prime 2 in the conductor (in spite of the fact that all the exponents involved in the Fermat equation are odd) can be explained by the fact that the Frey representation used to construct ρ is *odd*, so that one of the monodromies of $\varrho(t)$ is necessarily of order $2p$. In contrast, we will see that the Galois representations obtained from even Frey representations are unramified at 2.

The equation $x^p + y^p = z^r$
Let $\mathfrak{r} = (2-\omega)$ be the (unique) prime ideal of K above r.

Proposition 1.15 *1. The representation ρ_r^- is finite away from $\mathfrak{r}$ and the primes above* 2.
2. The representation ρ_r^+ is finite away from $\mathfrak{r}$.

Proof: The discriminants $\Delta^{\pm}$ of the polynomials used in equations (10) and (11) to define $C_r^{\pm}(a,b,c)$ are

$$\Delta^- = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r (ab)^{\frac{r-1}{2}p}; \qquad \Delta^+ = (-1)^{\frac{r+1}{2}} 2^{2(r+1)} r^r a^{\frac{r+3}{2}p} b^{\frac{r-1}{2}p}.$$

If ℓ is a prime which does not divide $\Delta^{\pm}$, then $C_r^{\pm}(a,b,c)$ has good reduction at ℓ and hence $\rho_r^{\pm}$ is finite at all primes above ℓ. So it is enough to consider the primes which divide $2ab$. Suppose first that $\ell \neq 2$ divides a, and let λ denote any prime of K above ℓ. Let K_λ be the completion of K at λ and $\mathcal{O}_\lambda$ its ring of integers, and denote by $\rho^{\pm}_{r,\lambda}$ the restriction of $\rho_r^{\pm}$ to an inertia group $I_\lambda \subset \mathrm{Gal}(\bar{K}_\lambda/K_\lambda)$ at λ. We observe that $\rho^{\pm}_{r,\lambda} = \varrho_r^{\pm}(a^p/c^r)|_{I_\lambda}$, since ℓ does not divide c. To study $\rho^{\pm}_{r,\lambda}$, we consider the curve $C^{\pm}_r$ over $\mathrm{Spec}(\mathcal{O}_\lambda[[t]])$. From the proof of theorem 1.10, one knows that $C^{\pm}_r$ is a Mumford curve over $K_\lambda[[t]]$. Hence its Jacobian $J^{\pm}_r$ is equipped with a (t)-adic analytic uniformization

$$1 \longrightarrow Q \longrightarrow T \longrightarrow J^{\pm}_r(K_\lambda((t))) \longrightarrow 1,$$

where $T \simeq (K_\lambda((t))^\times)^d$ is a torus and Q is the sublattice of multiplicative periods.
Because $J^{\pm}_r(t)$ extends to an abelian scheme over $\mathrm{Spec}(\mathcal{O}_\lambda[t, 1/t, 1/(t-1)])$, the lattice Q is generated by power series $q_1, \dots, q_d$ in $K_\lambda[[t]]$ whose leading coefficients $\alpha_1, \dots, \alpha_d$ belong to $\mathcal{O}^\times_\lambda$. It follows that the extension of K_λ cut out by $\rho^{\pm}_{r,\lambda}$ is contained in $K_\lambda(\zeta_p, \alpha_1^{1/p}, \dots, \alpha_d^{1/p}, t^{1/p})$ where $t = a^p/c^r$. Since $\mathrm{ord}_\ell(t) \equiv 0 \pmod{p}$, this extension is unramified at λ when $\ell \neq p$, and comes from a finite flat group scheme over $\mathcal{O}_\lambda$ when $\ell = p$. The proof when $\ell \neq 2$ divides b proceeds in an identical manner, considering this time $C^{\pm}_r(t)$ over $\mathrm{Spec}(\mathcal{O}_\lambda[[(t-1)]])$ and using the fact that $\mathrm{ord}_\ell(\frac{a^p}{c^r} - 1) = \mathrm{ord}_\ell(\frac{-b^p}{c^r}) \equiv 0 \pmod{p}$ to conclude. Consider finally the case where $\ell = 2$. If 2 does not divide ab, then c is even. Making the substitution $(x, y) = (1/u, (2v + 1)/u^{(r+1)/2})$, the equation of $C^+_r(a, b, c)$ becomes

$$v^2 + v = 4c(a^p - b^p)u^{r+1} - \frac{(a^p - b^p)}{2}u^r + (\text{lower order terms in } u).$$

The coefficients involved in this equation are integral at 2, and $\frac{a^p - b^p}{2}$ is odd; hence $C^+_r(a, b, c)$ has good reduction at 2, and therefore ρ^+_r is unramified at λ. If 2 divides ab, suppose without loss of generality that it divides a. Then the equation (6) for $C^+_r(t)$ also shows that $C^+_r(a, b, c)$ is a Mumford curve over K_λ, and the result follows by the same analysis as above.

Remark: The reader will find in [Ell] a more general criterion for the Galois representations arising from division points of Hilbert-Blumenthal abelian varieties to be unramified, which relies on Mumford's theory in an analogous way.

Proposition 1.15 implies that the conductor of ρ^+_r is a power of $\mathfrak{r}$, and that the conductor of ρ^-_r is divisible only by $\mathfrak{r}$ and by primes above 2. We now study the exponent of $\mathfrak{r}$ that appears in these conductors.

Proposition 1.16 *1. If r divides ab, then the conductor of ρ^-_r and ρ^+_r at $\mathfrak{r}$ divides $\mathfrak{r}$.*

2. If r does not divide ab, then the conductor of ρ_r^- and ρ_r^+ at $\mathfrak{r}$ divides $\mathfrak{r}^3$.

Proof: We treat the case of ρ_r^+, since the calculations for ρ_r^- are similar. By making the change of variable $x = (2-\omega)u - 2, y = (2-\omega)^{d+1}v$ in equation (6) one finds the new equation for C_r^+:

$$C_r^+ : v^2 + u\prod_j (u - \frac{2-\omega_j}{2-\omega})v + \frac{t}{(2-\omega)^d}u = 0. \tag{12}$$

Setting $\tilde{t} = \frac{t}{(2-\omega)^d}$, one sees that $C_r^+(\tilde{t})$ is a Mumford curve over $\mathrm{Spec}(\mathcal{O}_\mathfrak{r}[[\tilde{t}]])$. (The singular points in the special fiber have coordinates given by $(u,v) = (0,0)$ and $(\frac{2-\omega_j}{2-\omega}, 0)$, which are distinct since $\frac{2-\omega_j}{2-\omega} \equiv j^2 \pmod{\mathfrak{r}}$.) One concludes that when $\mathrm{ord}_\mathfrak{r}(t) > d$, then the representation $\varrho_r^+(t)$ is ordinary at $\mathfrak{r}$, and its conductor divides $\mathfrak{r}$. When r divides a one has $\mathrm{ord}_\mathfrak{r}(a^p/c^r) \geq pd > d$. A similar reasoning works when r divides b, and so part 1 of proposition 1.16 follows.

Part 2 is proved by analyzing $J_r^\pm(t)$ over $\mathrm{Spec}(\mathcal{O}_\mathfrak{r}[t, 1/(1-t), 1/t])$. The conductor of $J_r^\pm$ over this base is constant, and one finds that the conductor of $\rho_r^\pm$ is equal to $\mathfrak{r}^3$.

By combining the analysis of propositions 1.15 and 1.16, we have shown:

Theorem 1.17 *1. The conductor of ρ_r^- is of the form $2^u\mathfrak{r}^v$, where $u = 1$ if ab is even. One has $v = 1$ if r divides ab, and $v \leq 3$ otherwise.*

2. The conductor of ρ_r^+ divides $\mathfrak{r}$ if r divides ab, and $\mathfrak{r}^3$ otherwise.

2 Modularity

2.1 Hilbert modular forms

Let K be a totally real field of degree $d > 1$, and let $\psi_1, \ldots, \psi_d$ be the distinct real embeddings of K. They determine an embedding of the group $\Gamma = \mathbf{SL}_2(\mathcal{O}_K)$ into $\mathbf{SL}_2(\mathbb{R})^d$ by sending a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the d-tuple $\left(\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}\right)_{i=1}^d$ where $a_j = \psi_j(a)$ and likewise for b_j, c_j and d_j. Through this embedding, the group Γ acts on the product $\mathcal{H}^d$ of d copies of the complex upper half plane by Möbius transformations. More precisely, if $\tau = (\tau_1, \dots, \tau_d)$ belongs to $\mathcal{H}^d$, then

$$M\tau := \left(\frac{a_i\tau_i + b_i}{c_i\tau_i + d_i}\right)_{i=1}^{d}.$$

If f is a holomorphic function on $\mathcal{H}^d$ and $\gamma \in \mathbf{GL}_2(K)$ we define

$$(f|_2\gamma)(\tau) = \det(\gamma)\prod(c_i\tau_i + d_i)^{-2} f(\gamma\tau).$$

Let Γ be a discrete subgroup of $\mathbf{GL}_2(K)$.

Definition 2.1 *A modular form of weight* 2 *on* Γ *is a holomorphic function on* $\mathcal{H}^d$ *which satisfies the transformation rule*

$$f|_2\gamma = f,$$

for all γ *in* Γ.

A function that vanishes at the cusps is called a *cusp form* on Γ. The space of modular forms of weight 2 on Γ is denoted $M_2(\Gamma)$, and the space of cusp forms is denoted $S_2(\Gamma)$.

Let $\mathfrak{n}$ be an ideal of K. We now introduce the space $S_2(\mathfrak{n})$ of cusp forms of weight 2 level $\mathfrak{n}$, as in [W2], sec. 1.1. For this, choose a system $\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_h$ of representative ideals for the narrow ideal classes of K. Let $\mathfrak{d}$ denote the different of K, and assume that the $\mathfrak{c}_i$ have been chosen relatively prime to $\mathfrak{n}\mathfrak{d}$. Define

$$\begin{aligned}\Gamma_i(\mathfrak{n}) \quad := \quad \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2^+(K) \;\mid\; & a, d \in \mathcal{O}_K, b \in (\mathfrak{c}_i\mathfrak{d})^{-1}, \\ & c \in \mathfrak{c}_i\mathfrak{d}\mathfrak{n}, \quad ad - bc \in \mathcal{O}_K^\times\}.\end{aligned}$$

Definition 2.2 *A cusp form of weight* 2 *and level* $\mathfrak{n}$ *is an* h*-tuple of functions* $(f_1, \dots, f_h)$ *where* $f_i \in S_2(\Gamma_i(\mathfrak{n}))$.

Denote by $S_2(\mathfrak{n})$ the space of cusp forms of weight 2 and level $\mathfrak{n}$.

To the reader acquainted with the case $K = \mathbb{Q}$, the definition of $S_2(\mathfrak{n})$ may appear somewhat contrived. It becomes more natural when one considers the adelic interpretation of modular forms of level $\mathfrak{n}$ as a space of functions on the coset space $\mathbf{GL}_2(\mathbb{A}_K)/\mathbf{GL}_2(K)$. As in the case where $K = \mathbb{Q}$, the space $S_2(\mathfrak{n})$ is a finite-dimensional vector space and is endowed with an action of the commuting self-adjoint Hecke operators $T_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of K which do not divide $\mathfrak{n}$. (Cf. [W2], sec. 1.2.)

A modular form $f \in S_2(\mathfrak{n})$ is called an *eigenform* if it is a simultaneous eigenvector for these operators. In that case one denotes by $a_\mathfrak{p}(f)$ the eigenvalue of $T_\mathfrak{p}$ acting on f. Let K_f be the field generated by the coefficients $a_\mathfrak{p}(f)$. It is a finite totally real extension of $\mathbb{Q}$. If λ is any prime of K_f, let $K_{f,\lambda}$ be the completion of K_f at λ and let $\mathcal{O}_{f,\lambda}$ be its ring of integers.

Eigenforms are related to Galois representations of G_K thanks to the following theorem:

Theorem 2.3 *Let f be an eigenform in $S_2(\mathfrak{n})$. There is a compatible system of λ-adic representations*

$$\rho_{f,\lambda} : G_K \longrightarrow \mathbf{GL}_2(\mathcal{O}_{f,\lambda})$$

for each prime λ of K_f, satisfying:

$$\mathrm{trace}(\rho_{f,\lambda}(\mathrm{frob}_\mathfrak{q})) = a_\mathfrak{q}(f), \quad \det(\rho_{f,\lambda}(\mathrm{frob}_\mathfrak{q})) = Norm(\mathfrak{q}),$$

for all primes $\mathfrak{q}$ of K which do not divide $\mathfrak{n}\lambda$.

Proof: When K is of odd degree, or when K is of even degree and there is at least one finite place where f is either special or supercuspidal, this follows from work of Shimura, Jacquet-Langlands, and Carayol. (Cf. [Ca].) In this case the representation $\rho_{f,\lambda}$ can be realized on the λ-adic Tate module of an abelian variety over K. (It is a factor of the Jacobian of a Shimura curve associated to a quaternion algebra over K which is split at exactly one infinite place.) In the general case the theorem is due to Wiles [W1] (for ordinary forms) and to Taylor [Tay] for all f. The constructions of [W1] and [Tay] are more indirect than those of [Ca]: they exploit congruences between modular forms to reduce to the situation that is already dealt with in [Ca], but do not realize $\rho_{f,\lambda}$ on the division points of an abelian variety (or even on the étale cohomology of an algebraic variety).

Let A be an abelian variety over K with real multiplications by a field E. More precisely, one requires that E is a finite extension of $\mathbb{Q}$ whose degree is equal to the dimension of A, and that A is equipped with an inclusion:

$$E \longrightarrow \mathrm{End}_K(A) \otimes \mathbb{Q}.$$

Following a terminology of Ribet, call A an abelian variety *of* $\mathbf{GL}_2$*-type* over K. It gives rise to a compatible system $\rho_{A,\lambda}$ of λ-adic representations of G_K for each prime λ of E by considering the action of G_K on $(T_\ell(A)\otimes\mathbb{Q}_\ell)\otimes_E E_\lambda$. The *conductor* of A is defined to be the Artin conductor of $\rho_{A,\lambda}$ for any prime λ of good reduction for A. (One can show that this does not depend on the choice of λ.) The following conjecture is the natural generalization of the Shimura-Taniyama conjecture in the setting of abelian varieties of $\mathbf{GL}_2$-type:

Conjecture 2.4 (Shimura-Taniyama) *If A is an abelian variety of $\mathbf{GL}_2$-type over K of conductor $\mathfrak{n}$, then there exists a Hilbert modular form f over K of weight 2 and level $\mathfrak{n}$ such that*

$$\rho_{f,\lambda} \simeq \rho_{A,\lambda}$$

for all primes λ of E.

If A satisfies the conclusion of conjecture 2.4, one says that A is *modular*. Conjecture 2.4 appears to be difficult in general, even with the powerful new techniques introduced by Wiles in [W3]. In connection with equation (1), one is particularly interested in conjecture 2.4 for hypergeometric abelian varieties.

Conjecture 2.5 *For all $t \in \mathbb{Q}$, the hypergeometric abelian variety $J(t)$, (resp. $J_r^\pm(t)$, $J_{r,r}^\pm(t)$, $J_{q,r}^\pm(t)$) attached to the equation $x^p+y^p=z^p$ (resp. $x^p+y^p=z^r$, $x^r+y^r=z^p$, $x^p+y^q=z^r$) is modular over $\mathbb{Q}$ (resp. $\mathbb{Q}(\zeta_r)^+$, $\mathbb{Q}(\zeta_r)^+$, $\mathbb{Q}(\zeta_q,\zeta_r)^+$).*

2.2 Modularity of hypergeometric abelian varieties

The modularity of J

The modularity of the curves in the Legendre family J follows from Wiles' proof of the Shimura-Taniyama conjecture for semistable elliptic curves. To prove that J is modular, Wiles begins with the fact that the mod 3 representation $J[3]$ is modular; this follows from results of Langlands and Tunnell on base change, the key fact being that $\mathbf{GL}_2(\mathbb{F}_3)$ is *solvable*. Wiles then shows (at least when the representation $J[3]$ is irreducible and semi-stable) that every "sufficiently well-behaved" lift of $J[3]$ is also modular. This includes the representation arising from the 3-adic Tate module of J, and hence J itself is modular.

The modularity of $J_r^\pm$ and $J_{r,r}^\pm$
When $r = 2$ the abelian variety J_2 is an elliptic curve (which arises from the universal family on $X_0(2)$) and its modularity follows from the work of Wiles and its extensions [Di1].

Likewise when $r = 3$, the abelian varieties $J_r^\pm$ and $J_{r,r}^-$ are elliptic curves, so that their modularity follows from the Shimura-Taniyama conjecture. It is still conjectural in this case, in spite of the progress made toward the Shimura-Taniyama conjecture in [Di1] and [CDT]: for many values of t, the conductors of $J_3^\pm(t)$ and $J_{3,3}^-(t)$ are divisible by 27.

For $r > 3$, the prime 3 is never split in $\mathbb{Q}(\zeta_r)^+$, so that the image of the Galois representation acting on $J_r^\pm[3]$ or $J_{r,r}^\pm[3]$ is contained in a product of groups isomorphic to $\mathbf{GL}_2(\mathbb{F}_{3^s})$ with $s > 1$. Because $\mathbf{GL}_2(\mathbb{F}_{3^s})$ is not solvable when $s > 1$, it seems difficult to directly prove the modularity of $J_r^\pm[3]$ or $J_r^\pm[3]$ and use the prime 3 as in Wiles' original strategy.

Consider instead the prime $\mathfrak{r}$ of norm r. Since $G_\mathbb{Q}$ fixes $\mathfrak{r}$, it acts naturally on the modules $J_r^\pm[\mathfrak{r}]$ and $J_{r,r}^\pm[\mathfrak{r}]$ of $\mathfrak{r}$-torsion points of $J_r^\pm$ and $J_{r,r}^\pm$. Furthermore, these modules are two-dimensional $\mathbb{F}_r$-vector spaces and the action of $G_\mathbb{Q}$ on them is $\mathbb{F}_r$-linear.

Theorem 2.6 *1. The modules $J_r^-[\mathfrak{r}]$ and $J_{r,r}^-[\mathfrak{r}]$ are isomorphic to a quadratic twist of the mod r representation associated to the Legendre family J.*

2. The modules $J_r^+[\mathfrak{r}]$ and $J_{r,r}^+[\mathfrak{r}]$ are reducible Galois representations.

Proof: By the same arguments as in the proof of theorem 1.10 one shows that the representations attached to $J_r^-[\mathfrak{r}]$ and $J_{r,r}^-[\mathfrak{r}]$ (resp. $J_r^+[\mathfrak{r}]$ and $J_{r,r}^+[\mathfrak{r}]$), if irreducible, are Frey representations associated to the Fermat equation $x^r + y^r = z^r$ which are odd (resp. even). By theorem 1.5, there is a unique odd Frey representation (up to twisting by a quadratic character) associated to $x^r + y^r = z^r$, which is the one associated to the r-torsion points on the Legendre family $J(t)$. Part 1 follows. Since there are no even Frey representations associated to $x^r + y^r = z^r$, the reducibility of $J_r^+[\mathfrak{r}]$ and $J_{r,r}^+[\mathfrak{r}]$ follows as well. (Alternately, in [DMs], prop. 2.3, an explicit $\mathfrak{r}$-isogeny from $J_r^+(t)$ to $J_r^+(-t)$ defined over K is constructed, which shows that the corresponding representation is reducible, and in fact that J_r^+ has a K-rational torsion point of order r.)

Let $N_r^\pm$ and $N_{r,r}^\pm$ be the conductors of the $G_\mathbb{Q}$-representations $J_r^\pm[\mathfrak{r}]$ and $J_{r,r}^\pm[\mathfrak{r}]$.

Corollary 2.7 *The $G_{\mathbb{Q}}$-representations $J_r^{\pm}[\mathfrak{r}]$ and $J_{r,r}^{\pm}[\mathfrak{r}]$ arise from a classical modular form f_0 on $\Gamma_0(N_r^{\pm})$ and $\Gamma_0(N_{r,r}^{\pm})$.*

Proof: Since the elliptic curve $J : y^2 = x(x-1)(x-t)$is modular for all $t \in \mathbb{Q}$, it is associated to a cusp form on $\Gamma_0(N_J)$ where N_J is the conductor of $J(t)$. The lowering the level result of Ribet [Ri2] ensures that there is a form f_0 of level N_r^- (resp. $N_{r,r}^-$) attached to $J_r^-[\mathfrak{r}]$ (resp. $J_{r,r}^-[\mathfrak{r}]$). In the case of the even Frey representations, the appropriate modular form f_0 can be constructed directly from Eisenstein series.

Consider now the restriction of the Galois representations $J_r^{\pm}[\mathfrak{r}]$ and $J_{r,r}^{\pm}[\mathfrak{r}]$ to G_K, which we denote with the same symbol by abuse of notation.

Theorem 2.8 *There are Hilbert modular forms f over K giving rise to $J_r^{\pm}[\mathfrak{r}]$ or $J_{r,r}^{\pm}[\mathfrak{r}]$.*

Proof: This is a consequence of cyclic base change, taking f to be the base change lift of f_0 from $\mathbb{Q}$ to K.

In light of theorem 2.8, what is needed now is a "lifting theorem" in the spirit of [TW] and [W3] for Hilbert modular forms over K, which would allow us to conclude the modularity of the $\mathfrak{r}$-adic Tate module of $J_r^{\pm}$ and $J_{r,r}^{\pm}$. The methods of [TW] are quite flexible and have recently been partially extended to the context of Hilbert modular forms over totally real fields by a number of mathematicians, notably Fujiwara [Fu] and Skinner and Wiles [SW]. Certain technical difficulties prevent one from concluding the modularity of $J_r^{\pm}$ and $J_{r,r}^{\pm}$ in full generality:

1. When r does not divide ab, the $\mathfrak{r}$-adic Tate module of $J_r^{\pm}$ is neither flat nor ordinary at $\mathfrak{r}$. One needs lifting theorems that take this into account. The work of Conrad, Diamond and Taylor [CDT] is a promising step in this direction, but many technical difficulties remain to be resolved. Even when $r = 3$, one cannot yet prove that the elliptic curves $J_3^{\pm}(t)$ and $J_{3,3}^-(t)$ are modular for all $t \in \mathbb{Q}$.

2. The reducibility of the representation $J_r^+[\mathfrak{r}]$ may cause some technical difficulties, although the recent results of Skinner and Wiles [SW] go a long way toward resolving these difficulties in the *ordinary case*.

As an application of the results of [SW], we have the following theorem:

Theorem 2.9 *1. If r divides ab, then the abelian varieties $J_r^{\pm}(a,b,c)$ are modular.*

2. If r divides c, then the abelian varieties $J_{r,r}^{\pm}(a,b,c)$ are modular.

Proof: The abelian varieties $J_r^{\pm}(a,b,c)$ and $J_{r,r}^{\pm}(a,b,c)$ have multiplicative reduction at $\mathfrak{r}$, by the proof of proposition 1.16. Hence the $\mathfrak{r}$-adic Tate modules $T_r^{\pm}$ and $T_{r,r}^{\pm}$ of these varieties, viewed as a representation of G_K, are *ordinary* at $\mathfrak{r}$. Since the residual representations $J_r^{\pm}[\mathfrak{r}]$ and $J_{r,r}^{\pm}[\mathfrak{r}]$ come from a Hilbert modular form over K, the main theorem of [SW] asserts that this property is inherited by all of their ordinary deformations, including $T_r^{\pm}$ and $T_{r,r}^{\pm}$. The result follows.

The modularity of $J_{q,r}^{\pm}$

Let $K = \mathbb{Q}(\zeta_q, \zeta_r)^+$, and let $\mathfrak{q}$ be a prime of K above q. This prime is totally ramified in $K/\mathbb{Q}(\zeta_r)^+$. Denote by $\mathfrak{q}$ also the unique prime of $\mathbb{Q}(\zeta_r)^+$ below $\mathfrak{q}$, and let $\mathbb{F}$ be the common residue field of $\mathbb{Q}(\zeta_r)^+$ and K at $\mathfrak{q}$.

As in the previous section, one notes that the action of G_K on the module $J_{q,r}^{\pm}[\mathfrak{q}]$ extends to an $\mathbb{F}$-linear action of $G_{\mathbb{Q}(\zeta_r)^+}$.

Theorem 2.10 *The module $J_{q,r}^{\pm}[\mathfrak{q}]$ is isomorphic to a quadratic twist of $J_r^{\pm}[\mathfrak{q}]$ as a $G_{\mathbb{Q}(\zeta_r)^+}$-module.*

Proof: The proof is exactly the same as the proof of theorem 2.6.

Corollary 2.11 *If $J_r^{\pm}$ is modular, then so is $J_{q,r}^{\pm}[\mathfrak{q}]$.*

Proof: The same as for corollary 2.7 and theorem 2.8, applying this time cyclic base change from $\mathbb{Q}(\zeta_r)^+$ to K.

Corollaries 2.7 and 2.11 suggest an inductive strategy for establishing the modularity of J, $J_r^{\pm}$, $J_{r,r}^{\pm}$ and $J_{q,r}^{\pm}$, combining a series of base changes with successive applications of Wiles-type lifting theorems (at the last step, for Hilbert modular forms over $\mathbb{Q}(\zeta_q, \zeta_r)^+$). This strategy, and its connections with Fermat's equation and its variants, is summarized in the flow chart below:

$$
\begin{tikzcd}
\boxed{\text{Modularity of } J[3]} \arrow[dd, dashed] & \text{Base change} \arrow[l] & \\
& \text{Wiles lifting} \arrow[l] & \\
\boxed{\text{Modularity of } J} \arrow[d] & & \\
\boxed{\text{Modularity of } J[r]} \arrow[r] \arrow[dd, dashed] & \boxed{x^r + y^r = z^r} & \\
& \begin{array}{c}\text{Theorem 2.6 \&}\\ \text{base change}\end{array} \arrow[l] & \text{Theorem 2.6} \arrow[d] \\
\boxed{\begin{array}{c}\text{Modularity of } J_r^-[\mathfrak{r}]\\ \text{and } J_{r,r}^-[\mathfrak{r}]\end{array}} \arrow[dd, dashed] & & \boxed{\begin{array}{c}\text{Modularity of } J_r^+[\mathfrak{r}]\\ \text{and } J_{r,r}^+[\mathfrak{r}]\end{array}} \arrow[dd, dashed] \\
& \begin{array}{c}\text{Generalized}\\ \text{Wiles lifting?}\end{array} \arrow[l] \arrow[r] & \\
\boxed{\begin{array}{c}\text{Modularity of } J_r^-\\ \text{and } J_{r,r}^-\end{array}} \arrow[d] & & \boxed{\begin{array}{c}\text{Modularity of } J_r^+\\ \text{and } J_{r,r}^+\end{array}} \arrow[d] \\
\boxed{\begin{array}{c}\text{Modularity of } J_r^-[\mathfrak{q}]\\ \text{and } J_{r,r}^-[\mathfrak{q}]\end{array}} \arrow[r] \arrow[dd, dashed] & \boxed{\begin{array}{c}x^q + y^q = z^r,\\ x^r + y^r = z^q\end{array}} & \boxed{\begin{array}{c}\text{Modularity of } J_r^+[\mathfrak{q}]\\ \text{and } J_{r,r}^+[\mathfrak{q}]\end{array}} \arrow[l] \arrow[dd, dashed] \\
& \begin{array}{c}\text{Theorem 2.10 \&}\\ \text{base change}\end{array} \arrow[l] \arrow[r] & \\
\boxed{\text{Modularity of } J_{q,r}^-[\mathfrak{q}]} \arrow[dd, dashed] & & \boxed{\text{Modularity of } J_{q,r}^+[\mathfrak{q}]} \arrow[dd, dashed] \\
& \begin{array}{c}\text{Generalized}\\ \text{Wiles lifting?}\end{array} \arrow[l] \arrow[r] & \\
\boxed{\text{Modularity of } J_{q,r}^-} \arrow[d] & & \boxed{\text{Modularity of } J_{q,r}^+} \arrow[d] \\
\boxed{\text{Modularity of } J_{q,r}^-[\mathfrak{p}]} \arrow[r] & \boxed{x^p + y^q = z^r} & \boxed{\text{Modularity of } J_{q,r}^+[\mathfrak{p}]} \arrow[l]
\end{tikzcd}
$$

3 Lowering the level

3.1 Ribet's theorem

Let $\rho : G_K \longrightarrow \mathbf{GL}_2(\mathbb{F})$ be a Galois representation of G_K with values in $\mathbf{GL}_2(\mathbb{F})$ where $\mathbb{F}$ is a finite field.

Definition 3.1 *We say that ρ is* modular *if there exists a Hilbert modular form f over K and a homomorphism $j : \mathcal{O}_f \longrightarrow \mathbb{F}$ such that, for all primes $\mathfrak{q}$ which are unramified for ρ,*

$$\mathrm{trace}(\rho(\mathrm{frob}_{\mathfrak{q}})) = j(a_{\mathfrak{q}}(f)).$$

If f can be chosen to be of weight k and level $\mathfrak{n}$, we say that ρ is modular of weight k and level $\mathfrak{n}$.

The following is a generalization of Serre's conjectures [Se2] to totally real fields, in a simple special case.

Conjecture 3.2 *Suppose that*

$$\rho : G_K \longrightarrow \mathbf{GL}_2(\mathbb{F})$$

is an absolutely irreducible Galois representation, where $\mathbb{F}$ is a finite field of characteristic p. Suppose also that:

1. *ρ is odd, and its determinant is the cyclotomic character.*
2. *ρ is finite at all primes $\mathfrak{p}$ dividing p.*
3. *The conductor of ρ in the sense of [Se2] is equal to $\mathfrak{n}$.*

Then ρ is modular of weight 2 and level $\mathfrak{n}$.

This conjecture also seems quite difficult. (For example, the argument in [Se2], sec. 4, th. 4 shows that conjecture 3.2 implies the generalized Shimura-Taniyama conjecture 2.4.) The following conjecture, which extends a result of Ribet [Ri2] to totally real fields, should be more approachable:

Conjecture 3.3 *Suppose that ρ satisfies the assumptions of conjecture 3.2, and that it is modular of weight 2 and some level. Then ρ is modular of weight 2 and level $\mathfrak{n}$.*

The following partial result is proved in [Ja] and [Ra], building on the methods of [Ri2]:

Theorem 3.4 *Let $\rho : G_K \longrightarrow \mathbf{GL}_2(\mathbb{F})$ be an irreducible mod p representation associated to a Hilbert cuspidal eigenform f of weight 2 and level $\mathfrak{n}\lambda$, where $\mathfrak{n}$, λ and p are mutually relatively prime. If $[K : \mathbb{Q}]$ is even, assume that f is either special or supercuspidal at a finite prime $\mathfrak{q}$ not dividing p and λ. Then if ρ is unramified at λ, ρ comes from a Hilbert cuspidal eigenform g of weight 2 and level $\mathfrak{n}$.*

3.2 Application to $x^p + y^p = z^r$

In the remainder of this article we will focus our attention on the equation $x^p + y^p = z^r$ and attack it by studying the representations $\rho_r^+ = \varrho^+(a^p/c^r)$ (and, towards the end, ρ_r^-) attached to the p-torsion of $J_r^{\pm}(a,b,c)$.

Theorem 3.5 *1. If r divides ab then ρ_r^+ (resp. ρ_r^-) comes from a modular form of weight 2 and level dividing $\mathfrak{r}$ (resp. $2^u\mathfrak{r}$, for some u).*

2.If r does not divide ab, assume further that $J_r^{\pm}(t)$ is modular and that conjecture 3.3 holds for Hilbert modular forms over K. Then ρ_r^+ (resp. ρ_r^-) comes from a modular form of weight 2 and level dividing $\mathfrak{r}^3$ (resp. $2^u\mathfrak{r}^3$, for some u).

Proof: The modularity of $J_r^{\pm}(a,b,c)$ (which when r divides ab follows from theorem 2.9) implies that $\rho_r^{\pm}$ is modular of weight 2 and some level. By theorem 1.17, ρ_r^+ has conductor dividing $\mathfrak{r}$ when $r|ab$ and dividing $\mathfrak{r}^3$ in general, and satisfies all the other hypotheses in conjecture 3.2; a similar statement holds for ρ_r^-. Conjecture 3.3 implies the conclusion. Note that when $r|ab$, the Hilbert modular form f associated to $J_r^+(a,b,c)$ is special or supercuspidal at $\mathfrak{r}$, so that the hypotheses of theorem 3.4 are satisfied. Hence theorem 3.4 can be applied to prove part 1 of theorem 3.5 unconditionally.

Remark: Theorem 3.5 suggests that the analysis of the solutions (a,b,c) to $x^p + y^p = z^r$ splits naturally into two cases, depending on whether or not r divides ab. The following definition is inspired by Sophie Germain's classical terminology:

Definition 3.6 *A primitive solution (a,b,c) of $x^p + y^p = z^r$ is called a* first case solution *if r divides ab, and a* second case solution *otherwise.*

Remark: As with Fermat's Last Theorem, the first case seems easier to deal with than the second case. (Cf. theorem 3.22.)

Our hope is that theorem 3.5 forces the image of $\rho_r^\pm$ to be small (at least for some values of r). Before pursuing this matter further, observe that equation (1) has (up to sign) three trivial solutions: $(0,1,1)$, $(1,0,1)$ and $(1,-1,0)$.

Proposition 3.7

1. *If $(a,b,c) = (0,1,1)$ or $(1,0,1)$, then J_r^+ and J_r^- have degenerate reduction, and the representations $\rho_r^\pm$ are therefore reducible.*

2. *If $(a,b,c) = (1,-1,0)$, then $J_r^\pm$ have complex multiplication by $\mathbb{Q}(\zeta_r)$, and hence the image of $\rho_r^\pm$ is contained in the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F})$.*

Proof: This can be shown by a direct calculation. For example, the curve $C_r^+(1,-1,0)$ has equation

$$y^2 = x^{r+1} - 4x.$$

Making the substitution $(x,y) = (-1/u, (2v+1)/u^{(r+1)/2}$, one obtains the equation

$$v^2 + v = u^r,$$

and one recognizes this as the equation for the hyperelliptic quotient of the Fermat curve $x^r + y^r = z^r$ which has complex multiplication by $\mathbb{Q}(\zeta_r)$.

Proposition 3.7 suggests the following question:

Question 3.8 *Can one show that the image of $\rho_r^\pm(a,b,c)$ is necessarily contained in a Borel subgroup or in the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F})$?*

The case $r = 2$ and 3

For $r = 2$ (resp. $r = 3$) one can answer this question in the affirmative, by noting that $\rho_2(a,b,c)$ (resp. $\rho_3^+(a,b,c)$) is modular of level dividing 32 (resp. 27). (One needs to assume the Shimura-Taniyama conjecture for $r = 3$.) The space of classical cusp forms of weight 2 and level 32 (resp. 27) is one-dimensional. In fact $X_0(32)$ (resp. $X_0(27)$) is an elliptic curve with complex multiplication by $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(\zeta_3)$). (It is also a quotient of the Fermat curve $x^4+y^4=z^4$ (resp. $x^3+y^3=z^3$).) So the Galois representations arising from non-trivial primitive solutions of $x^p+y^p=z^2$ and $x^p+y^p=z^3$ are either reducible or of dihedral type. This was proved in [Da2]. (See also [DMr].)

To answer question 3.8 for specific values of $r>3$ and p requires a computation of all the Hilbert modular forms over K of weight 2 and level dividing $\mathfrak{r}^3$. We will limit ourselves to the simpler case where K has narrow class number one.

Remark: It is known that K has narrow class number one for all $r<100$ except $r=29$, when the narrow class number is equal to 8. (The author is grateful to Cornelius Greither for pointing out these facts.)

We now give a formula for the dimension of $S_2(1)$ and $S_2(\mathfrak{r}^k)$, with $k=1,\ldots,3$ under the narrow class number one assumption. To do this we need to introduce some notations:

• Recall that $d=(r-1)/2$ denotes the degree of K over $\mathbb{Q}$.

• Set $\delta_2=2$ if $r\equiv 1 \pmod 4$ and $\delta_2=0$ if $r\equiv 3 \pmod 4$. Likewise let $\delta_3=2$ if $r\equiv 1 \pmod 3$ and $\delta_3=0$ if $r\equiv 2 \pmod 3$.

• Let $\zeta_K(s)$ be the Dedekind zeta-function of K. The main contribution to the dimension of $S_2(\mathfrak{r}^k)$ is given by the special value $\zeta_K(-1)$, a rational number which can be computed from the formula:

$$\zeta_K(-1)=\frac{(-1)^d}{12}\prod_\chi \frac{B_{2,\chi}}{2}, \qquad B_{2,\chi}=\frac{1}{r}\sum_{a=1}^{r}\chi(a)a^2,$$

where the product is taken over all non-trivial even Dirichlet characters $\chi : (\mathbb{Z}/r\mathbb{Z})^\times/\langle\pm 1\rangle \longrightarrow \mathbb{C}^\times$ of conductor r.

• Let h^- be the minus part of class number of $\mathbb{Q}(\zeta_r)$. This number can be evaluated also as a product of generalized Bernouilli numbers:

$$h^-=(-1)^d 2r\prod_\chi \frac{B_{1,\chi}}{2}, \qquad B_{1,\chi}=\frac{1}{r}\sum_{a=1}^{r}\chi(a)a,$$

where the product this time is taken over the odd Dirichlet characters of conductor r.

• Let $h(a)$ be the class number of the quadratic extension $K(\sqrt{a})$, and (for $d<0$) let $q(a)$ be the index of $\mathcal{O}_K^\times \mathcal{O}_{\mathbb{Q}(\sqrt{a})}^\times$ in $\mathcal{O}_K(\sqrt{a})^\times$. One has $q(a)=1$ or 2, and $q(a)=1$ if $r \equiv 3 \pmod 4$. Only the ratios $h(-1)/q(-1)$ and $h(-3)/q(-3)$ are involved in the formula for the dimension of $S_2(\mathfrak{r}^k)$. Let χ_4 and χ_3 denote the non-trivial Dirichlet character mod 4 and 3 respectively. When K has narrow class number one, these ratios are given by the formulae:

$$\frac{h(-1)}{q(-1)} = (-1)^{d+1} \prod_\chi \frac{B_{1,\chi\chi_4}}{2}, \quad \frac{h(-3)}{q(-3)} = (-1)^{d+1} \prod_\chi \frac{B_{1,\chi\chi_3}}{2},$$

where the products are taken over the non-trivial even Dirichlet characters of conductor r. (Recall that

$$B_{1,\chi\chi_4} = \frac{1}{4r}\sum_{a=1}^{4r} a\chi\chi_4(a), \qquad B_{1,\chi\chi_3} = \frac{1}{3r}\sum_{a=1}^{3r} a\chi\chi_3(a).)$$

The following table lists these invariants for the first few values of r:

r	d	$\zeta_K(-1)$	h^-	$h(-1)/q(-1)$	$h(-3)/q(-3)$
5	2	$1/30$	1	1	1
7	3	$-1/21$	1	1	1
11	5	$-20/33$	1	1	1
13	6	$152/39$	1	3	2
17	8	$18688/51$	1	8	5
19	9	$-93504/19$	1	19	9

Let

$$\chi(\mathfrak{n}) = 1 + (-1)^d \dim(S_2(\mathfrak{n})).$$

Under the assumption that K has narrow class number one, this is the arithmetic genus of the Hilbert modular variety $\mathcal{H}^d/\Gamma_0(\mathfrak{n})$; cf. [Fr], ch. II, sec. 4, th. 4.8.

Theorem 3.9 *Assume that K has narrow class number 1. Then $\chi(\mathfrak{r}^k)$ (and* *hence, the dimension of $S_2(\mathfrak{r}^k)$) is given by the formula:*

$$\begin{aligned}
\chi(1) &= \frac{\zeta_K(-1)}{2^{d-1}} + \frac{r-1}{2r}h^- + \frac{h(-1)}{4q(-1)} + \frac{h(-3)}{3q(-3)}, \\
\chi(\mathfrak{r}) &= (r+1)\frac{\zeta_K(-1)}{2^{d-1}} + \frac{r-1}{2r}h^- + \delta_2\frac{h(-1)}{4q(-1)} + \delta_3\frac{h(-3)}{3q(-3)}, \\
\chi(\mathfrak{r}^k) &= r^{k-1}(r+1)\frac{\zeta_K(-1)}{2^{d-1}} + \delta_2\frac{h(-1)}{4q(-1)} + \delta_3\frac{h(-3)}{3q(-3)}.
\end{aligned}$$

Proof: The formula for $\chi(1)$ is given in [We], theorem 1.14 and 1.15. A routine calculation then yields the formula for $\chi(\mathfrak{r}^k)$, after noting that:

1. An elliptic fixed point of order 2 (resp. 3) on $\mathcal{H}^d$ for the action of $\mathbf{SL}_2(\mathcal{O}_K)$ lifts to δ_2 (resp. δ_3) elliptic fixed points on $\mathcal{H}^d/\Gamma_0(\mathfrak{r}^k)$ for $k \geq 1$.
2. An elliptic fixed point of order r lifts to a unique elliptic fixed point modulo $\Gamma_0(\mathfrak{r})$, and there are no elliptic fixed points of order r on $\mathcal{H}^d/\Gamma_0(\mathfrak{r}^k)$ when $k > 1$.

Noting that K has narrow class number one when $r < 23$, theorem 3.9 allows us to compute the dimensions for the relevant spaces of cusp forms:

r	$\dim(S_2(1))$	$\dim(S_2(\mathfrak{r}))$	$\dim(S_2(\mathfrak{r}^2))$	$\dim(S_2(\mathfrak{r}^3))$
5	0	0	0	2
7	0	0	1	5
11	0	1	6	56
13	1	4	24	290
17	6	55	879	14895
19	12	379	7300	138790

The case $r = 5$ and 7:
When $r = 5$, the action of the Hecke operators on the spaces $S_2(\mathfrak{n})$ over $K = \mathbb{Q}(\sqrt{5})$ can be calculated numerically by exploiting the Jacquet-Langlands correspondence between forms on $\mathbf{GL}_2(K)$ and on certain quaternion algebras. Let B be the (unique, up to isomorphism) totally definite quaternion algebra over K which is split at all finite places. The algebra B can be

identified with the standard Hamilton quaternions over K, since 2 is inert in K:

$$B = \{x + yi + zj + wk, \quad x, y, z, w \in \mathbb{Q}(\sqrt{5})\}.$$

The class number of B is equal to one: the maximal orders in B are all conjugate to the ring of *icosians*

$$R = \mathbb{Z}[\omega,\ i,\ j,\ k,\ \frac{1}{2}(1+i+j+k),\ \frac{1}{2}(i+\omega j+\bar{\omega}k)],$$

whose unit group $R^\times$ is isomorphic to the binary icosahedral group of order 120. (Cf. for example [CS], ch. 8, sec. 2.1.) Let $R_\mathfrak{n}$ be an Eichler order of level $\mathfrak{n}$ in R, and write

$$\hat{R}_\mathfrak{n} := R_\mathfrak{n} \otimes \hat{\mathbb{Z}}, \qquad \hat{B} = B \otimes \hat{\mathbb{Z}}.$$

The Jacquet-Langlands correspondence shows that $S_2(\mathfrak{n})$ is isomorphic as a Hecke module to the space

$$L^2(\hat{R}_\mathfrak{n}^\times \backslash \hat{B}^\times / B^\times),$$

on which the Hecke operators act in the standard way.

The following table lists the eigenvalues of the Hecke operators $T_\mathfrak{p}$ acting on $S_2(\mathfrak{r}^3)$, for all the primes $\mathfrak{p}$ of K of norm ≤ 50. It turns out that the two eigenforms in $S_2(\mathfrak{r}^3)$ are conjugate to each other over $\mathbb{Q}(\sqrt{5})$, so we have only displayed the eigenvalues of one of the two eigenforms.

$\mathfrak{p}$	(2)	(3)	$(3-\omega)$	$(4+\omega)$	$(4-\omega)$	$(5+\omega)$	$(5-\omega)$
$a_\mathfrak{p}(f)$	0	0	$\frac{-1-5\sqrt{5}}{2}$	$\frac{-1+5\sqrt{5}}{2}$	0	0	0

$\mathfrak{p}$		$(6+\omega)$	$(7+2\omega)$	$(5-2\omega)$	$(7+\omega)$	$(6-\omega)$	(7)
$a_\mathfrak{p}(f)$		0	$\frac{-11+5\sqrt{5}}{2}$	$\frac{-11-5\sqrt{5}}{2}$	$\frac{9+5\sqrt{5}}{2}$	$\frac{9-5\sqrt{5}}{2}$	0

Observe that $a_\mathfrak{p}(f) = 0$ for all the primes $\mathfrak{p}$ which are inert in the quadratic extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\omega)$. This suggests that f is actually of CM type, and corresponds to an abelian variety of dimension 2 with complex multiplication by $\mathbb{Q}(\zeta_5)$.

In fact, this can be proved: the abelian variety

$$J_5^+(1,-1,0) = \mathrm{Jac}(y^2 + y = x^5)$$

has complex multiplication by $\mathbb{Q}(\zeta_5)$, and its Hasse-Weil L-function is a product of Hecke L-series attached to Grossencharacters of $\mathbb{Q}(\zeta_5)$ of conductor $(1-\zeta_5)^2$. A direct calculation shows that $J_5^+(1,-1,0)$ is associated to the two eigenforms in $S_2(\sqrt{5}^3)$ over $\mathbf{GL}_2(\mathbb{Q}(\sqrt{5}))$.

When $r=7$, we did not carry out a numerical investigation of the Hecke eigenforms of level $\mathfrak{r}^2$ and $\mathfrak{r}^3$, but this turns out to be unecessary in identifying the modular forms that arise in these levels. Let A be the (unique, up to isogeny) elliptic curve over $\mathbb{Q}$ of conductor 49, which has complex multiplication by $\mathbb{Q}(\sqrt{-7})$. It corresponds to a cusp form over $\mathbb{Q}$ of level 49. Its base change lift to $K=\mathbb{Q}(\cos(2\pi/7))$ is the unique modular form of level $\mathfrak{r}^2$. The space $S_2(\mathfrak{r}^3)$ contains a two-dimensional space of old forms, and hence there are three eigenforms of level $\mathfrak{r}^3$. These must consist of the Hilbert modular forms associated to the Fermat quotient

$$J_7^+(1,-1,0): y^2+y=x^7.$$

So when $r=5$ and 7, the spaces $S_2(\mathfrak{r}^3)$ contain only eigenforms of CM type associated to hyperelliptic Fermat quotients or CM elliptic curves. Hence:

Theorem 3.10 *Let $r=5$ or 7, and let (a,b,c) be a non-trivial primitive solution to the equation $x^p+y^p=z^r$, where $p\neq r$ is an odd prime. Let $\mathfrak{p}$ be any prime of $K=\mathbb{Q}(\cos(2\pi/r))$ above p, and write $\mathbb{F}:=\mathcal{O}_K/\mathfrak{p}$. Then*

1. *If (a,b,c) is a first case solution, the mod $\mathfrak{p}$ representation associated to $J_r^+(a,b,c)$ is reducible;*

2. *If (a,b,c) is a second case solution, assume further that $J_r^+(a,b,c)$ is modular, and that Ribet's lowering the level theorem (conjecture 3.3) holds for Hilbert modular forms over K. Then the mod $\mathfrak{p}$ representation associated to $J_r^+(a,b,c)$ is either reducible, or its image is contained in the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F})$.*

Following [Se4], one can use the fact that J_r^+ is semistable to obtain more precise information in the first case.

Proposition 3.11 *If $r=5$ or 7 and (a,b,c) is a first case solution to $x^p+y^p=z^r$, then $J_r^+(a,b,c)$ is $\mathbb{Q}$-isogenous to an abelian variety having a rational point of order p.*

Proof: Choose a prime $\mathfrak{p}$ of K above p, and let $\chi_1 : G_K \longrightarrow \mathbb{F}^\times$ be the character giving the action of G_K on the K-rational one-dimensional $\mathbb{F}$-vector subspace L of $J_r^+[\mathfrak{p}]$. Let χ_2 be the character of G_K describing its action on $J_r^+[\mathfrak{p}]/L$. The local analysis in [Se4], sec. 5.4., lemme 6, shows that χ_1 and χ_2 are unramified outside the primes above p. Also, the set of restrictions $\{\chi_1|_{I_{\mathfrak{p}'}}, \chi_1|_{I_{\mathfrak{p}'}}\}$ to an inertia group $I_{\mathfrak{p}'}$ at a prime $\mathfrak{p}'$ above $\mathfrak{p}$ is equal to $\{\chi, 1\}$, where χ is the cyclotomic character giving the action of $I_{\mathfrak{p}'}$ on the pth roots of unity. (Use the corollary to prop. 13 of [Se4].) Hence one of χ_1 or χ_2 is everywhere unramified. (When there is a single prime of K above p, this is immediate. If p is split in K, one observes, by analyzing the image of the map $\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K \otimes \mathbb{F}_p)^\times$ and using class field theory, that the inertia groups at the various $\mathfrak{p}'$ in the maximal tamely ramified abelian extension of K unramified outside p have non-trivial intersection, and in fact are equal for all but finitely many p.) Since K has class number 1, one of χ_1 or χ_2 is trivial. If $\chi_1 = 1$, then $J_r^+[\mathfrak{p}]$ has a K-rational point whose trace gives a point of order p in $J_r^+(a,b,c)$. If $\chi_2 = 1$, the module $\tilde{L}$ generated by the $\mathcal{O}_K[G_\mathbb{Q}]$-translates of L is a $\mathbb{Q}$-rational subgroup of $J_r^+[p]$ which is of rank one over $\mathcal{O}_K \otimes \mathbb{F}_p$. The quotient $J_r^+/\tilde{L}$ has a rational point of order p.

Corollary 3.12 *If ℓ is a prime satisfying $\ell < p^{1/d} - 2p^{1/2d} + 1$, then ℓ divides ab.*

Proof: If ℓ does not divide ab, then J_r^+ has good reduction at ℓ and $\#J_r^+(\mathbb{F}_\ell) < (1+\sqrt{\ell})^{2d}$ by the Weil bounds. Hence $p > \#J_r^+(\mathbb{F}_\ell)$. This contradicts proposition 3.11, since the prime-to-ℓ part of the torsion subgroup of of $J_r^+(\mathbb{Q})$ injects into $J_r^+(\mathbb{F}_\ell)$ (and likewise for any abelian variey isogenous to J_r^+).

Theorem 3.13 *Suppose $r = 5$ or 7. There exists a constant C_r^- depending only on r such that, if $p \geq C_r^-$ and (a,b,c) is a first case solution to $x^p + y^p = z^r$, the Galois representation ρ_r^- is reducible. (In this case there is a quotient of $J_r^-(a,b,c)$ over $\mathbb{Q}$ which has a rational point of order p.)*

Proof: By corollary 3.12, if p is large enough then 2 divides ab, so that $J_r^-(a,b,c)$ is semistable. The mod $\mathfrak{p}$ representation associated to $J_r^-(a,b,c)$, if irreducible, is therefore equal to the mod $\mathfrak{p}$ rerpesentation associated to a Hilbert modular form f over K in $S_2(2\mathfrak{r})$. Corollary 3.12 further implies that if ℓ is a prime of $\mathbb{Q}$ and λ a prime of K above it, we have

$$a_\lambda(f) \equiv \mathrm{norm}(\lambda) + 1 \pmod{\mathfrak{p}}, \qquad \text{for all } \ell \leq p^{1/d} - 2p^{1/2d} + 1.$$

For each f there is a constant C_f^- such that this statement fails whenever $p > C_f^-$, since the mod $\mathfrak{p}$ representations attached to f are irreducible for almost all $\mathfrak{p}$. Now take C_r^- to be the maximum of the C_f^- as f runs over the normalized eigenforms in $S_2(2\mathfrak{r})$. The statement in parentheses follows by applying to J_r^- the same arguments used in the proof of proposition 3.11.

Remark: Although the statement of theorem 3.13 involves only ρ_r^-, note the crucial role played in its proof by the representation ρ_r^+ via corollary 3.12. This illustrates how information gleaned from one Frey representation may sometimes be used to yield insights into a second a priori unrelated Frey representation associated to the same generalized Fermat equation.

The case $r = 11$

When $r = 11$, there is a 44-dimensional space of new forms of level $\mathfrak{r}^3$, and studying the equation $x^p + y^p = z^{11}$ would require computing the Fourier coefficients associated to these newforms. We content ourselves with the following result, which requires only dealing with $S_2(\mathfrak{r})$.

Theorem 3.14 *Let (a, b, c) be a first case solution to the equation $x^p + y^p = z^{11}$, where $p > 19$ is prime, and let $\mathfrak{p}$ be any prime of $K = \mathbb{Q}(\cos(2\pi/11))$ above p Then the mod $\mathfrak{p}$ representation associated to $J_{11}^+(a, b, c)$ is reducible, and in fact $J_{11}^+(a, b, c)$ has a rational point of order p.*

Proof: Let $\mathfrak{p}$ be any ideal of K above p, and let $\rho_{\mathfrak{p}}$ denote the mod $\mathfrak{p}$ representation associated to $J_{11}^+(a, b, c)$. Suppose that it is irreducible. By exploiting the action of $\mathrm{Gal}(K/\mathbb{Q})$, it follows that $\rho_{\mathfrak{p}}$ is irreducible for all choices of $\mathfrak{p}$. Theorem 3.5 implies that $\rho_{\mathfrak{p}}$ is modular of level dividing $\mathfrak{r}$. The table above shows that the space of cusp forms of this level is one-dimensional. In fact, the unique normalized eigenform $\mathbf{f}$ of level $\mathfrak{r}$ is the base change lift to $K = \mathbb{Q}(\cos(2\pi/11))$ of the modular form $f = \eta(z)^2\eta(11z)^2$ of level 11 associated to the elliptic curve $X_0(11)$. Consider the prime ideal (2) of K above 2, of norm 32. Then

$$a_{(2)}(\mathbf{f}) = a_{32}(f) = 8.$$

This implies that

$$a_{(2)} := a_{(2)}(J_{11}^+(a, b, c)) \equiv 8 \pmod{\mathfrak{p}}$$

for all primes $\mathfrak{p}$ above p. Taking norms, one finds:

$$p^5 \text{ divides } \mathrm{norm}_{K/\mathbb{Q}}(a_{(2)} - 8).$$

By the Weil bounds, we have

$$|\mathrm{norm}_{K/\mathbb{Q}}(a_{(2)} - 8)| \leq (2\sqrt{32} + 8)^5.$$

Since $p > 20 > 8(1 + \sqrt{2})$, we must have $a_{(2)} = 8$. But this leads to a contradiction. For, if 2 divides ab, then $J_{11}^+(a, b, c)$ has purely toric reduction at 2 and $a_{(2)} = \pm 1$. If ab is odd, then $J_{11}^+(a, b, c)$ has good reduction at (2), and 11 divides $\mathrm{norm}(32 + 1 - a_{(2)}) = 25^5$ since $J_{11}^+(a, b, c)$ has a K-rational point of order 11 (by theorem 2.6). It follows that the mod p representations associated to J_{11}^+ are reducible. The proof of prop. 3.11 now shows that $J_{11}^+(\mathbb{Q})$ has a point of order p, since $\mathbb{Q}(\cos(2\pi/11))$ has class number one.

Corollary 3.15 *If ℓ is a prime satisfying $\ell < p^{1/5} - 2p^{1/10} + 1$, then ℓ divides ab.*

The proof of this corollary is the same as for corollary 3.12. Finally, we record:

Theorem 3.16 *There exists a constant C_{11}^- such that, if $p \geq C_{11}^-$ and (a, b, c) is a first case solution to $x^p + y^p = z^{11}$, the Galois representation ρ_{11}^- is reducible. (In this case there is a quotient of $J_{11}^-(a, b, c)$ over $\mathbb{Q}$ which has a rational point of order p.)*

The proof is the same as for theorem 3.13.

The case $r = 13$:
When $r = 13$ there is a unique normalized cusp form of level 1, which is the base change lift of the cusp form associated to the elliptic curve $X_1(13)$. (Note that this curve acquires good reduction over $\mathbb{Q}(\cos(2\pi/13))$.) This modular form does not pose any obstructions to studying first case solutions to $x^p + y^p = z^{13}$, since the representation attached to a solution of the equation is ramified at $\mathfrak{r}$.

On the other hand, the two-dimensional space of new forms of level $\mathfrak{r}$ would have to be studied more carefully in order to understand the (first case) solutions to $x^p + y^p = z^{13}$. The numerical calculation of eigenforms in $S_2(\mathfrak{r})$

becomes increasingly difficult as r gets larger, and it has not been carried out even for $r = 13$. One can go further without such explicit numerical calculations, (cf. theorem 3.22 below) by studying congruences (modulo $\mathfrak{r}$) for modular forms.

General r:
Let ℓ be a rational prime. The ℓ-adic Tate module $T_\ell(J_r^\pm(t)) \otimes \mathbb{Q}_\ell$ is a two-dimensional $K_\ell := K \otimes \mathbb{Q}_\ell$-vector space. When t is rational, the linear action of G_K on this vector space extends to a $G_\mathbb{Q}$-action which is G_K-semilinear, i.e., satisfies

$$\sigma(\alpha v) = \alpha^\sigma \sigma(v), \qquad \text{for all } \alpha \in K_\ell, \sigma \in G_\mathbb{Q}.$$

Letting $a_\mathfrak{q}(J_r^\pm) := \mathrm{trace}(\rho_{J,\ell}(\mathrm{frob}_\mathfrak{q}))$, it follows that

$$a_\mathfrak{q}(J_r^\pm)^\sigma = a_{\mathfrak{q}^\sigma}(J_r^\pm). \tag{13}$$

This motivates the following definition:

Definition 3.17 *A Hilbert modular form over K of level $\mathfrak{n}$ is called a* $\mathbb{Q}$-form *if for all ideals $\mathfrak{q}$ of K which are prime to $\mathfrak{n}$ it satisfies the relation*

$$a_\mathfrak{q}(f)^\sigma = a_{\mathfrak{q}^\sigma}(f), \qquad \textit{for all } \sigma \in G_\mathbb{Q}.$$

(In particular, this implies that the Fourier coefficients $a_\mathfrak{q}(f)$ belong to K.)

Equation (13) implies the following lemma, which reflects the fact that the abelian varieties $J_r^\pm(t)$ with $t \in \mathbb{Q}$ are defined over $\mathbb{Q}$ (even though their endomorphism rings are only defined over K).

Lemma 3.18 *For all $t \in \mathbb{Q}$, if the abelian varieties $J_r^-(t)$ and $J_r^+(t)$ are modular, then they are associated to a modular $\mathbb{Q}$-form over K.*

Let f be an eigenform in $S_2(\mathfrak{n})$ and let λ be a prime in the ring of Fourier coefficients $\mathcal{O}_f$. Denote by $\rho_{f,\lambda}$ the λ-adic representation associated to f by theorem 2.3 and let V be the underlying $K_{f,\lambda}$-vector space. Choose a G_K-stable $\mathcal{O}_{f,\lambda}$-lattice Λ in V. The space $\bar{\Lambda} := \Lambda/\lambda\Lambda$ gives a two-dimensional representation $\bar{\rho}_{f,\lambda}$ for G_K over the residue field $k_{f,\lambda} := \mathcal{O}_{f,\lambda}/\lambda$. In general, this representation depends on the choice of lattice, but its semi-simplification does not. One says that $\rho_{f,\lambda}$ is *residually irreducible* if $\bar{\rho}_{f,\lambda}$ is irreducible for some (and hence all) choices of lattice Λ. Otherwise one says that $\rho_{f,\lambda}$ is residually reducible. In the latter case, the semi-simplification of $\bar{\rho}_{f,\lambda}$ is a direct sum of two one-dimensional characters

$$\chi_1, \chi_2 : G_K \longrightarrow k_{f,\lambda}^\times,$$

whose product is the cyclotomic character

$$\chi : G_K \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \subset k_{f,\lambda}^\times$$

giving the action of G_K on the ℓ-th roots of unity.

Let f be a $\mathbb{Q}$-form over K in the sense of definition 3.17, so that in particular its Fourier coefficients are defined over K. We say that f is $\mathfrak{r}$-Eisenstein if its associated $\mathfrak{r}$-adic representation $\rho_{f,\mathfrak{r}}$ is residually reducible.

Proposition 3.19 *There exists a constant C_r^+ depending only on r such that, for any first case solution (a, b, c) to equation (1) with $p > C_r^+$, one of the following holds:*

1. *The representation ρ_r^+ is reducible, or*
2. *it is isomorphic to the mod $\mathfrak{p}$ representation attached to an $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-form in $S_2(\mathfrak{r})$.*

Proof: Let g be any eigenform in $S_2(\mathfrak{r})$. If g is not a $\mathbb{Q}$-form, then there exists a prime $\mathfrak{q}$ of $\mathcal{O}_g$ and a $\sigma \in G_{\mathbb{Q}}$ such that $a_{\mathfrak{q}}(g)^\sigma \neq a_{\mathfrak{q}^\sigma}(g)$. If g is a $\mathbb{Q}$-form, but is not $\mathfrak{r}$-Eisenstein, then there is a prime $\mathfrak{q}$ of K such that $\mathfrak{r}$ does not divide $a_{\mathfrak{q}}(g) - N\mathfrak{q} - 1$. In either case, one has

$$a_{\mathfrak{q}}(g) \neq a_{\mathfrak{q}}(f),$$

for all modular forms f which correspond to a $J_r^+(t)$ with $t \in \mathbb{Q}$. Indeed, such an f is a $\mathbb{Q}$-form and is $\mathfrak{r}$-Eisenstein by theorem 2.6. If $f \equiv g$ for some prime $\mathfrak{p}$ of $\mathcal{O}_g K$ above p then taking norms gives

$$p \text{ divides } \mathrm{Norm}_{K_g K/\mathbb{Q}}(a_{\mathfrak{q}}(g) - a_{\mathfrak{q}}(f)) \neq 0.$$

Let $d_g := [K_g : \mathbb{Q}]$. Applying the Weil bounds one finds:

$$|\mathrm{Norm}_{K_g K/\mathbb{Q}}(a_{\mathfrak{q}}(g) - a_{\mathfrak{q}}(f))| \leq (16\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}))^{(r-1)d_g/4},$$

so that
$$p \leq C_g := (16\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}))^{(r-1)d_g/4}.$$
In particular, if $p > C_g$, the representation ρ_r^+ is not equivalent to $\bar{\rho}_{g,\mathfrak{p}}$ for any prime of $\mathcal{O}_g K$ above p. Now set $C_r^+ := \max_g C_g$, where the maximum is taken over all eigenforms g in $S_2(\mathfrak{r})$ which are either not $\mathbb{Q}$-forms or are not $\mathfrak{r}$-Eisenstein.

In light of proposition 3.19, it becomes important to understand whether there exist $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms in $S_2(\mathfrak{r})$.

Proposition 3.20 *Suppose that r is a regular prime. Then there are no $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms over K of level 1 or $\mathfrak{r}$.*

Proof: Suppose on the contrary that f is a $\mathbb{Q}$-form in $S_2(\mathfrak{r})$ and that $\rho_{f,\mathfrak{r}}$ is residually reducible. Let χ_1 and χ_2 be the characters of G_K which occur in the semi-simplification of $\bar{\Lambda}$, for some (and hence all) G_K-stable lattices Λ in V. Because f is a $\mathbb{Q}$-form, it follows that χ_1 and χ_2 are powers of the cyclotomic character χ with values in $\langle \pm 1 \rangle \subset \mathbb{F}_r^\times$. Furthermore, $\chi_1\chi_2 = \chi$. Hence we may assume without loss of generality that $\chi_1 = 1$ and $\chi_2 = \chi$. By proposition (2.1) of [Ri1], there exists a G_K-stable lattice Λ for which
$$\bar{\rho}_{f,\mathfrak{r}} \simeq \begin{pmatrix} \chi_1 & \Psi_0 \\ 0 & \chi_2 \end{pmatrix} = \begin{pmatrix} 1 & \Psi_0 \\ 0 & \chi \end{pmatrix}, \tag{14}$$
and is not semi-simple. This implies that $\Psi := \Psi_0/\chi$ is a non-trivial cocycle in $H^1(K, \mathbb{Z}/r\mathbb{Z}(-1))$. Proposition 3.20 now follows from the following lemma:

Lemma 3.21 *The cocycle Ψ is unramified.*

Proof of lemma: The cocycle Ψ is unramified at all places $v \neq \mathfrak{r}$ because v does not divide the level of f. It is also unramified at $\mathfrak{r}$: if f is of level 1, this is because $\bar{\rho}_{f,\mathfrak{r}}$ comes from a finite flat group scheme over K. If f is of level $\mathfrak{r}$, then by theorem 2 of [W1], the restriction of the representation $\bar{\rho}_{f,\mathfrak{r}}$ to a decomposition group $D_\mathfrak{r}$ at $\mathfrak{r}$ is of the form
$$\bar{\rho}_{f,\mathfrak{r}}|_{D_\mathfrak{r}} \simeq \begin{pmatrix} \chi & \Psi \\ 0 & 1 \end{pmatrix}.$$
But the restriction of χ to $D_\mathfrak{r}$ is non-trivial. Comparing the equation above to equation (14), it follows that the local representation $\bar{\rho}_{f,\mathfrak{r}}|_{D_\mathfrak{r}}$ splits. Therefore the cocycle Ψ is locally trivial at $\mathfrak{r}$. This completes the proof of lemma 3.21.

Proposition 3.20 now follows directly: the cocycle Ψ cuts out an unramified cyclic extension of $\mathbb{Q}(\zeta_r)$ of degree r, which does not exist if r is a regular prime.

Theorem 3.22 *Let r be a regular prime. Then there exists a constant C_r^+ (depending only on r) such that, for all $p > C_r^+$, and all first case solutions (a, b, c) to $x^p + y^p = z^r$, the mod $\mathfrak{p}$ representation associated to $J_r^+(a, b, c)$ is reducible.*

Proof: Combine propositions 3.19 and 3.20.

Remarks:
1. The value of the constant C_r^+ depends on the structure of the space of Hilbert modular forms over $\mathbb{Q}(\cos(2\pi/r))$ of level $\mathfrak{r}$. It would be possible in principle to write down a crude estimate for C_r^+ by using the Chebotarev density theorem and known estimates for the size of fourier coefficients of Hilbert modular eigenforms, but we have not attempted to do this.

2. The consideration of $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms so crucial for the proof of theorem 3.22 is only likely to be of use in studying first case solutions. Indeed, there typically exist $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms on $S_2(\mathfrak{r}^3)$ – for example, the base change lifts from $\mathbb{Q}$ to K of certain r-Eisenstein forms on $X_0(r^2)$, or (more germane to the present discussion) the form in $S_2(\mathfrak{r}^3)$ asociated to the CM abelian variety $J_r^+(1, -1, 0)$.

3. The arguments based on $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms yield no *a priori* information about the Galois representations ρ_r^-, since the mod r representation attached to $J_r^-(a, b, c)$ is irreducible. (It is isomorphic to a twist of the representation coming from the r-torsion of the Frey curve $y^2 = x(x-a^p)(x+b^p)$, by theorem 2.6.) Nonetheless, one can still show:

Theorem 3.23 *Assume further that K has class number one. Then*
1. $J_r^+(a, b, c)$ has a rational point of order p.
2. There exists a further constant C_r^- such that if $p > C_r^-$, the abelian variety $J_r^-(a, b, c)$ also has a rational point of order p.

Proof: The proof of 1 is the same as for proposition 3.11, and 2 follows from the same reasoning as for proposition 3.13.

4 Torsion points on abelian varieties

Ultimately one wishes to extract a contradiction from theorems like theorems 3.10, 3.13, 3.14, 3.16, 3.22 and 3.23 by proving that when p is large enough (relative to r perhaps), the image of $\rho_r^{\pm}$ is large - for example, that this image contains $\mathbf{SL}_2(\mathbb{F})$; or, at the very least, that the abelian varieties $J_r^{\pm}(a,b,c)$, when semistable, cannot contain a rational point of order p. The following folklore conjecture can be viewed as a direct generalization of a conjecture of Mazur for elliptic curves.

Conjecture 4.1 *Let E be a totally real field and K a number field. There exists a constant $C(K,E)$ depending only on K and E, such that for any abelian variety A of $\mathbf{GL}_2$-type with $\mathrm{End}_K(A)\otimes\mathbb{Q} = \mathrm{End}_{\bar{K}}(A)\otimes\mathbb{Q} \simeq E$, and all primes $\mathfrak{p}$ of E of norm greater than $C(K,E)$, the image of the mod $\mathfrak{p}$ representation associated to A contains $\mathbf{SL}_2(\mathbb{F})$.*

This conjecture seems difficult: the set of abelian varieties of $\mathbf{GL}_2$-type with $\mathrm{End}(A)\otimes\mathbb{Q} \simeq E$ is parametrized by a d-dimensional Hilbert modular variety, and very little is known about the Diophantine properties of these varieties.

When $r = 2$ and $r = 3$, one has $K = E = \mathbb{Q}$ since the representations $\rho_r^{\pm}$ arise from elliptic curves. Much of conjecture 4.1 can be proved thanks to the ideas of Mazur [Ma1], [Ma2]:

• Theorem 8 of [Ma1] implies that the image of $\rho_r^{\pm}$ is not contained in a Borel subgroup of $\mathbf{GL}_2(\mathbb{F}_p)$ when $p > 5$.

• A result of Momose [Mo] building on the ideas in [Ma1] implies that this image is not contained in the normalizer of a split Cartan subgoup if $p > 17$.

• Finally, a result of Merel and the author [DMr] implies that the image of ρ_r^{+} is not contained in the normalizer of a non-split Cartan subgroup. (We were unable to prove a similar result for ρ_r^{-}.)

Combining these results with an ad-hoc study (carried out by Bjorn Poonen [Po], using traditional descent methods) of the equations $x^p + y^p = z^r$ ($r = 2, 3$) for small values of p yields the desired contradiction. Thus the main result of [DMr] provides an (essentially) complete analogue of Fermat's Last Theorem for equation (1) when $r = 2$ or 3, which one would like to emulate for higher values of r.

Theorem 4.2 ([DMr]) *1. The equation $x^p + y^p = z^2$ has no non-trivial primitive solutions when $p \geq 4$.*

2. Assume the Shimura-Taniyama conjecture. Then the equation $x^p+y^p = z^3$ has no non-trivial primitive solutions when $p \geq 3$.

Return now to the case $r > 3$. The following special case of conjecture 4.1, which is suficient for the applications to equation (1), seems more tractable:

Conjecture 4.3 *There exists a constant B_r depending only on r, such that for any $t \in \mathbb{Q}$, and all primes $\mathfrak{p}$ of $K = \mathbb{Q}(\zeta_r)^+$ of norm greater than B_r, the image of the mod $\mathfrak{p}$ representation of G_K associated to $J_r^{\pm}(t)$ is neither contained in a Borel subgroup or in the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F})$.*

A natural approach to this conjecture is to study the curves $X_0^{\pm}(\mathfrak{p})$, $X_s^{\pm}(\mathfrak{p})$ and $X_{ns}^{\pm}(\mathfrak{p})$ which classify the abelian varieties $J_r^{\pm}(t)$ with a rational subgroup, a "normalizer of split Cartan subgroup" structure, and a "normalizer of non-split Cartan subroup structure" on the $\mathfrak{p}$-division points, where $\mathfrak{p}$ is an ideal of the field K.

For the moment, we know very little about the arithmetic of these curves, except when $r = 2$ and $r = 3$ when they are closely related to classical modular curves. When $r > 3$, they appear as quotients of the upper half plane by certain non-arithmetic Fuchsian groups described in [CW]. We will content ourselves here with giving a formula for the genus of these curves. Let $\epsilon = \pm 1$ be defined by the condition $\mathbb{N}\mathfrak{p} \equiv \epsilon \pmod{r}$.

Lemma 4.4 *1. The genus of $X_0^{\pm}(\mathfrak{p})$ is equal to*

$$\frac{1}{2}(1 - \frac{1}{r} - \frac{2}{p})\mathbb{N}\mathfrak{p} - \frac{\epsilon}{2}(1 - \frac{1}{r}).$$

2. The genus of $X_s^{\pm}(\mathfrak{p})$ is equal to

$$\frac{1}{4}(1 - \frac{1}{r} - \frac{2}{p})\mathbb{N}\mathfrak{p}(\mathbb{N}\mathfrak{p} + 1) - \frac{\epsilon + 1}{4}(1 - \frac{1}{r}) + 1.$$

3. The genus of $X_{ns}^{\pm}(\mathfrak{p})$ is equal to

$$\frac{1}{4}(1 - \frac{1}{r} - \frac{2}{p})\mathbb{N}\mathfrak{p}(\mathbb{N}\mathfrak{p} - 1) + \frac{\epsilon - 1}{4}(1 - \frac{1}{r}) + 1.$$

Example: When $r = 5$ and $\mathfrak{p} = (3)$, one finds that the curves $X_0^-(3)$ and $X_0^+(3)$ are of genus 1, i.e., they are elliptic curves over $\mathbb{Q}$. A direct calculation reveals that $X_0^+(3)$ is an elliptic curve of conductor 15, denoted by $15E$ in Cremona's tables. By looking up the curve $15E$ twisted by $\mathbb{Q}(\sqrt{5})$, one finds that $15E$ has finite Mordell-Weil group over $\mathbb{Q}(\sqrt{5}$. Does $J_0^+(\mathfrak{p})$ always have a non-zero quotient with finite Mordell-Weil group over $\mathbb{Q}(\zeta_r)^+$, at least when $\mathfrak{p}$ is large enough?

References

[Atlas] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson. Atlas of finite groups: maximal subgroups and ordinary characters for simple groups. New York: Clarendon Press, 1985.

[Be] S. Beckmann, On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.* **419** (1991), 27–53.

[Ca] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. Ecole Norm. Sup.* (4) **19** (1986), no. 3, 409–468.

[CDT] B. Conrad, F. Diamond, R. Taylor, Modularity of certain potentially crystalline Galois representations, manuscript, to appear.

[CS] J.H. Conway and Sloane, Sphere packings, lattices and groups. Second edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. *Grundlehren der Mathematischen Wissenschaften* **290**. Springer-Verlag, New York, 1993.

[CW] P. Cohen, J. Wolfart, Modular embeddings for some nonarithmetic Fuchsian groups. *Acta Arith.* **56** (1990), no. 2, 93–110.

[Da1] H. Darmon, Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation, *C.R. Acad.Sci. Canada*, **19** (1997), no. 1, 3–14.

[Da2] H. Darmon, The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$. *Internat. Math. Res. Notices* **10** 1993, 263–274.

[DDT] H. Darmon, F. Diamond, and R. Taylor, Fermat's Last Theorem, *Current Developments in Mathematics* **1**, 1995, International Press, pp. 1-157.

[DK] H. Darmon, A. Kraus, On the equations $x^r + y^r = z^p$, in preparation.

[DMr] H. Darmon, L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *Journal für die Reine und Angewandte Mathematik* **490** (1997), 81–100.

[DMs] H. Darmon, J-F. Mestre, Courbes hyperelliptiques à multiplications réelles et une construction de Shih, CICMA preprint; *Canadian Math. Bull*, to appear.

[Di1] F. Diamond, On deformation rings and Hecke rings. *Annals of Math* (2) **144** (1996), no. 1, 137–166.

[Di2] F. Diamond, The Taylor-Wiles construction and multiplicity one. *Invent. Math.* **128** (1997), no. 2, 379–391.

[Ell] J. Ellenberg, Harvard PhD. Thesis, in preparation.

[Fr] E. Freitag, Hilbert Modular Forms, Springer-Verlag, 1990.

[Fre] G. Frey, Links between solutions of $A - B = C$ and elliptic curves, in: *Number theory*, Ulm 1987, Proceedings, *Lecture Notes in Math.* **1380**, Springer-Verlag, New York, 1989, 31–62.

[Fu] K. Fujiwara, Deformation rings and Hecke algebras in the totally real case, preprint.

[He] E. Hecke, Die eindeutige Bestimmung der Modulfunktionen q-ter Stufe durch algebraische Eigenschaften, *Math. Ann.* **111** (1935), 293-301 (=Math. Werke, 568-576).

[Hu] Huppert, B. Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.

[Ja] F. Jarvis, On Galois representations associated to Hilbert modular forms. *J. Reine Angew. Math.* **491** (1997), 199–216.

[Ka] N. Katz, Exponential sums and differential equations, Annals of Math. Studies, Princeton University Press, 1990.

[Ma1] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186.

[Ma2] B. Mazur, Rational isogenies of prime degree. *Invent. Math.* **44** (1978), no. 2, 129–162.

[Me] J.-F. Mestre, Familles de courbes hyperelliptiques à multiplications réelles. Arithmetic algebraic geometry (Texel, 1989), 193-208, *Progr. Math* **89** Birkhauser Boston, Boston, MA, 1991.

[Mo] F. Momose, Rational points on the modular curves $X_{\mathrm{split}}(p)$. *Compositio Math.* **52** (1984), no. 1, 115–137.

[Po] B. Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *J. of Number Theory*, to appear.

[Ra] A. Rajaei, PhD thesis, Princeton University, 1998.

[Ri1] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34**, 151-162 (1976).

[Ri2] K. Ribet, On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100**, 431–476 (1990).

[Se1] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett, 1992.

[Se2] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.* **54** (1987), no. 1, 179–230.

[Se3] J.-P. Serre, Galois cohomology. (edition revised by the author). Springer-Verlag, Berlin, 1997.

[Se4] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331.

[SW] C. Skinner, A. Wiles, in progress.

[TTV] W. Tautz, J. Top, A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.* **43** (1991) no. 5, 1055-1064.

[Tay] R. Taylor, On Galois representations associated to Hilbert modular forms. *Invent. Math.* **98** (1989), no. 2, 265–280.

[TW] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* (2) **141** (1995), no. 3, 553–572.

[Vi] M.-F. Vigneras, Arithmétique des algèbres de quaternions. *Lecture Notes in Mathematics* **800**. Springer, Berlin, 1980.

[We] D. Weisser, The arithmetic genus of the Hilbert modular variety and the elliptic fixed points of the Hilbert modular group, *Math. Ann.* **257**, 9–22 (1981).

[W1] A. Wiles, On ordinary λ-adic representations associated to modular forms. *Invent. Math.* **94** (1988), no. 3, 529–573.

[W2] A. Wiles, On p-adic representations for totally real fields. *Ann. of Math.* (2) **123** (1986), no. 3, 407–456.

[W3] A. Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) **141** (1995), no. 3, 443–551.