HYPERGEOMETRIC MOTIVES AND THE GENERALIZED FERMAT EQUATION

FRANCO GOLFIERI MADRIAGA AND ARIEL PACETTI

with an Appendix by Ariel Pacetti and Fernando Rodriguez Villegas

Abstract. In the beautiful article [16] Darmon proposed a program to study integral solutions of the generalized Fermat equation $Ax^q + By^p + Cz^r = 0$. In the aforementioned article, Darmon proved many steps of the program, by exhibiting models of hyperelliptic/superelliptic curves lifting what he called "Frey representations", Galois representations over a finite field of characteristic p. The goal of the present article is to show how hypergeometric motives are more natural objects to obtain the global representations constructed by Darmon, allowing to prove most steps of his program.

1. Introduction

The study of Diophantine's equations is probably one of the oldest research areas in mathematics, which got a lot of attention after Fermat's statement that the equation

$$x^n + y^n = z^n$$

does not have any non-trivial solution if $n \geq 3$ (non-trivial meaning none coordinate equal to 0). After Wiles' groundbreaking proof of Fermat's statement (in [53]) a lot of attention has been given to the study of the so called *generalized Fermat equation*. Let A, B, C be non-zero pairwise coprime integers and let p, q, r be positive integers. The *generalized Fermat equation* is the affine surface given by the equation

$$Ax^q + By^p + Cz^r = 0. \tag{1}$$

A challenging problem is that of understanding its set of integral points. The name "generalized Fermat equation" comes from the observation that setting $A = B = C = 1$ and $p = q = r$ we recover Fermat's classical equation. However, Fermat's equation determines a curve in the projective plane, while the generalized Fermat equation determines a surface in the affine plane, making its study a harder problem. Two well known conjectures regarding solutions to the generalized Fermat equation are the following.

Conjecture (Beal's conjecture)**.** *For any triple of exponents (p, q, r), with $p, q, r \geq 3$, the equation*

$$x^q + y^p = z^r,$$

has no primitive non-trivial solution.

Recall the following definition.

Definition. *A solution (α, β, γ) of (1) is called primitive if* $\gcd(\alpha, \beta, \gamma) = 1$.

2020 *Mathematics Subject Classification.* 11D41,11F80,33C05.

Key words and phrases. Diophantine equations, Hypergeometric Series, Hypergeometric Motives.

The second author was funded by the Portuguese Foundation for Science and Technology (FCT) Individual Call to Scientific Employment Stimulus (https://doi.org/10.54499/2020.02775.CEECIND/CP1589/CT0032). This work was supported by CIDMA and is funded by the FCT, under grant UIDB/04106/2020 (https://doi.org/10.54499/UIDB/04106/2020).

Beal's conjecture (with a one million dollars reward) is deeply related to the so called *Fermat-Catalan* conjecture.

Conjecture (Fermat-Catalan's conjecture)**.** *The set of triples* (α, β, γ) *which are primitive solutions of the equation*

$$x^q + y^p = z^r,$$

for any triple of exponents (q, p, r) *with* $\frac{1}{q} + \frac{1}{p} + \frac{1}{r} < 1$ *is finite.*

Actually there exists a candidate for the finite list of solutions (as given in page 515 of [17]), based on numerical experiments. The restriction $p, q, r \geq 3$ in Beal's conjecture has to do with the geometry of the surface S defined by equation (1). The *characteristic* χ of the surface S is defined by

$$\chi := \frac{1}{q} + \frac{1}{p} + \frac{1}{r} - 1. \tag{2}$$

The case $\chi > 0$ is similar to the case of a genus zero curve, namely it has either zero or infinitely many integral points (as proved by Beukers in [8]). In practice, there is a finite list of exponents (p, q, r) with $\chi > 0$, allowing to study each of them individually:

- The solutions to (1) for $(q, p, r) = (2, 2, r \geq 2), (3, 3, 2), (2, 3, 4), (2, 4, 3)$ were given in [8] using Zagier's factorization.
- The remaining case where $\chi > 1$ corresponds to $(q, p, r) = (2, 3, 5)$ studied by Thiboutot (and completely solved in [23]).

Similarly, one can study the finite list of exponents (q, p, r) having characteristic 0. They correspond (up to a change of variables in equation (1)) to the triples $(2, 3, 6), (2, 6, 3), (3, 3, 3)$, $(4, 4, 2)$ and $(4, 2, 4)$. The set of solutions for each of them is well known:

- The case $(3, 3, 3)$ corresponds to the Fermat cubic (hence there are no non-trivial solutions).
- The case $(2, 6, 3)$ has no non-trivial solution, while the case $(3, 2, 6)$ has the unique non-trivial solution $(-2, \pm 3, 1)$ as proved by Bachet (see §6.2 of [17]).
- The case $(2, 4, 4)$ has no non-trivial proper solution (as proved by Leibniz) while the case $(4, 4, 2)$ was proved by Fermat.

We suggest readers interested in the subject to look at [17] (§6) for solutions to the general Fermat equation when $\chi = 0$ (i.e. when one allows general coefficients in the equation).

Understanding solutions to the generalized Fermat equation when $\chi < 0$ is a very challenging open problem. A beautiful and deep result of Darmon and Granville ([17]) asserts that equation (1) has finitely many *primitive* integral points for each choice of the parameters A, B, C, p, q, r. However, the proof is non-effective (as it depends on Faltings' proof of Mordell's conjecture).

Support for Fermat-Catalan's conjecture: the ABC conjecture.

The well known ABC conjecture (due to Oesterlé and Masser) implies a strong finiteness result: there exist only finitely many triples $(A, B, C) = (x^q, y^p, z^r)$ satisfying $A + B = C$ and $\gcd(A, B, C) = 1$. Therefore the values of (x, y, z, p, q, r) for which a non-trivial solution exists belong to a finite set (see [17]). Unfortunately (as is widely believed within the mathematical community) the ABC conjecture is far from being proved, hence a different approach is needed.

The modular method.

A very powerful method to study Fermat's equation is the so called *modular method* (as developed by Frey, Hellegouarch, Mazur, Ribet, Wiles, Taylor et al.) The modular method allowed to prove non-existence of solutions for different exponents, which can be divided into two cases (see Tables 1, 2 and 3 of [5] for references):

- Specific exponents, like $(2, 3, n)$ for $n = 7, 8, 9, 10, 11, 15$, $(3, 4, 5)$, $(3, 5, 5)$,$(5, 5, 7)$ $(5, 5, 19)$ and $(7, 7, 5)$.

- Families of exponents, like $(2,4,n)$, $(2,6,n)$, $(2,2n,3)$, $(2,2n,9)$, $(3,6,n)$, $(n,n,2)$, $(n,n,3)$, $(2n,2n,5)$, $(2l,2m,n)$ (for l,m primes and $n=3,5,7,11$), $(2l,2m,13)$.

The modular method ends relating a solution of a Diophantine equation with an object (an automorphic form) belonging to a finite dimensional vector space, which (in principle) can be computed. It is not our goal to describe the modular method in great detail, but we content ourselves with a very simplified description of the steps involved:

(I) Attach to a putative solution $P=(\alpha,\beta,\gamma)$ of (1) a geometric object $\mathcal{C}$ defined over a small degree number field K. The object should have the property that the reduction of its Galois representation modulo a well chosen prime $\mathfrak{p}$ has a small ramification set (independent of the solution P). In most well known cases (like Fermat's last theorem) the geometric object $\mathcal{C}$ is an elliptic curve, either defined over $\mathbb{Q}$ or over a number field. In the remarkable article [16], Darmon attaches to a solution a hyperelliptic/superelliptic curve of GL_2-type[1] for different families of exponents (see also [9]). When possible, the field K should be totally real, since in this case many different modularity theorems are known, and Hilbert modular forms are easier to compute.

(II) Study the compatible system of Galois representations $\{\rho_{\mathcal{C},\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(\overline{\mathbb{Z}_\lambda}))\}$ attached to $\mathcal{C}$ (coming from the action of the Galois group on its étale cohomology), for λ ranging over prime ideals of the "coefficient field". The final goal of this second step is to prove that the family is *modular*, i.e. it matches the Galois representation attached to an automorphic form of weight k.

(III) Prove that the reduction of the $\mathfrak{p}$-th member of the family (for a proper choice of the prime ideal $\mathfrak{p}$ as in (1)) is absolutely irreducible, and compute its conductor $\mathfrak{n}$. Then a variant of Ribet's *lowering the level result* (proved in [44] for classical modular forms, and a stronger version in [13] for Hilbert modular forms) implies the existence of an automorphic form F of level $\mathfrak{n}$ and weight k whose residual Galois representation $\overline{\rho_{F,\mathfrak{p}}}$ is isomorphic to $\overline{\rho_{\mathcal{C},\mathfrak{p}}}$.

(IV) Compute the space of automorphic forms of level $\mathfrak{n}$ and weight k and prove that none of them can be related to a solution of (1).

Despite our naive and simplified description, each step of the program has its subtleties! Even when the first three steps of the program can be successfully applied (and it seems like a new Diophantine equation will be solved), it usually happens that the last step fails for one of the following two reasons: either the space of automorphic forms has huge dimension (hence we encounter a computational problem), or the existence of "trivial" (or small) solutions to our equation makes the elimination step (IV) to fail.

It is sometimes possible to overcome the second failure by applying the so called *multi-frey method* as developed by Siksek in [14]. Basically, the idea is to construct many different objects in step (I) attached to the same solution, and make use of them all in the elimination step (IV). Usually the construction of the geometric object $\mathcal{C}$ in step (I) is an artisan's work, making the modular method (and the multi-frey method) hard to apply in new instances.

In the beautiful article [16], Darmon introduced the notion of *Frey representations* that gives a general framework to construct the Galois representations of step (I) as we now recall. If F is a field of characteristic zero, we denote by Gal_F the Galois group $\mathrm{Gal}(\overline{F}/F)$.

Let K be a number field, let $K(t)$ be the function field in one variable over K and let $\mathbb{F}$ be a finite field of characteristic p.

Definition. *A Frey representation is a continuous Galois representation*

$$\rho_t : \mathrm{Gal}_{K(t)} \to \mathrm{GL}_2(\mathbb{F}),$$

[1] To our knowledge there is no application of the modular method where the geometric objects is not related to a 2-dimensional Galois representations.

satisfying the following conditions:

(1) The restriction of ρ to $\mathrm{Gal}_{\overline{K}(t)}$ has trivial determinant and is irreducible.

(2) Let $\overline{\rho}^{geom}$ denote the projectivization of the restriction of ρ to $\mathrm{Gal}_{\overline{K}(t)}$. Then $\overline{\rho}^{geom}$ is unramified outside $\{0,1,\infty\}$ and it maps the inertia groups at $0,1$ and ∞ to subgroups of $\mathrm{PSL}_2(\mathbb{F})$ of order p, q and r respectively.

By a result of Beckmann ([3], see also [16, Lemma 1.2]) Frey's representation ρ_t specialized at the point $t_0 = -\frac{A\alpha^q}{C\gamma^r}$ (where (α,β,γ) is a putative solution to (1)) is unramified outside the set of primes dividing $ABCpqr$ (a number which only depends on the equation, not on the solution).

The representation ρ_{t_0} should match the reduction of the representation $\rho_{\mathcal{C}}$ coming from the geometric object constructed in the first step of the modular method.

In [16] Darmon studies for each exponents (q,p,r) all irreducible Frey representations ρ_t with inertia orders q,p,r at $0,1,\infty$ respectively (the representation depends only on the exponents, not on a particular solution to the equation). However, Frey's representations are not enough to prove non-existence of solutions, mainly because of the following two problems:

(1) How can we compute all number fields fixed by the kernel of ρ_{t_0}?

(2) How to discard fields that are not related to solutions?

The standard way to solve the first problem is to relate the representation to a modular one (going back to step (II) of the modular method). This would be automatically true if Serre's conjectures are true for general number fields (or at least totally real ones). Since nowadays Serre's conjectures are only proven for the rational field, we need to construct "lifts" of Frey's representation ρ_{t_0} to fields of characteristic zero, and prove their modularity.

In [16], Darmon study some particular families of exponents and constructs for each of them a curve $\mathcal{C}$ of GL_2-type satisfying that the reduction of its Galois representation $\rho_{\mathcal{C}}$ matches ρ_{t_0}. Furthermore (under some suitable hypothesis) Darmon is able to prove modularity of the global representation $\rho_{\mathcal{C}}$, fulfilling steps (I) and (II) of the modular method for them (see [9] for results on step (III) for exponents (q,q,p)).

Hypergeometric motives (HGM for short) are useful while studying the general case of the generalized Fermat equation; they are a source of motives whose Galois representations are "reasonably" well understood. They are mentioned in Darmon's original article and in [15] Darmon proved that all representations coming from hypergeometric motives defined over totally real fields are modular. The catch is that on doing so Darmon assumed the veracity of some very strong modularity lifting results which (unfortunately) are still far from being proven.

There is a difference between our approach and Darmon's one (that allows us to prove stronger results). What Darmon calls an *hypergeometric abelian variety* (in [15]) are varieties whose existence depend on results of Belyi (Theorems 1 and 2 of [4]). Belyi's construction is not explicit, so it does not give any information on traces of Frobenius endomorphisms nor a description of the variety at primes of bad reduction of the variety. Then even when one could theoretically use Belyi construction to complete step (III) of the modular method, it will be of no use for the last one.

During the last years the theory of hypergeometric motives became a very active research area. The rational ones have nice models (as explained in [28]) and many of their expected properties are known (see [46] for a nice introduction). The purpose of the present article is to explain how the use of rank two hypergeometric motives (as studied in [29]) can be used to fulfill steps (I), (II) and (IV) of the modular method, allowing to study solutions of new families of the generalized Fermat equation (1).

Instead of presenting an hypergeometric motives as triples of monodromy matrices (as done by Darmon), we present them as pairs of rational numbers, $(a,b),(c,d)$ following the more standard convention. With this description it is easy to verify that there are finitely many rational rank 2 hypergeometric motives, corresponding to rational elliptic curves. In Table 3.1 we list all rational

rank 2 hypergeometric motives satisfying that at least one monodromy matrix has infinite order. Doing reverse engineering, we can deduce for each parameter which family of exponents of (1) can be studied with it. This recovers most of the elliptic curves appearing in the literature while studying the generalized Fermat equation (see Table 1.1).

The modular method is well suited to study solutions of (1) when the exponents lie in a line L (Fermat's last theorem corresponding to the line $q = p = r$). If we restrict to prime exponents, then there are four different types of lines (up to a relabeling of the variables):

(1) $L_1 : \{x = y = z\}$, corresponding to Fermat's last theorem of exponents (p, p, p).
(2) $L_2 : \{x = y, z = r\}$, corresponding to exponents (p, p, r).
(3) $L_3 : \{x = z = q\}$, corresponding to exponents (q, p, q).
(4) $L_4 : \{x = q, z = r\}$, corresponding to exponents (q, p, r).

The recipe for constructing an hypergeometric motive (or its parameters) defined over a totally real number field K (independent of the varying parameter p) consists on finding four rational numbers a, b, c, d satisfying the following properties:

- The numbers $a-b$, $a-d$, $c-b$ and $c-d$ are not integers (for the monodromy representation to be irreducible).
- The numbers $a+b$ and $c+d$ are integers (for the motive to be defined over a totally real number field).
- If the parameter x (respectively z) varies, then $c = d$ (respectively $a = b$) and they belong to $\{\frac{1}{2}, 1\}$. Otherwise, the denominator of c belongs to $\{x, 2x\}$ (respectively $\{z, 2z\}$).

Definition 1.1. *For each one of the previous lines define the following motives:*

(1) The motive $\mathcal{H}_1^- := \mathcal{H}((\frac{1}{2}, \frac{1}{2}), (1, 1)|t)$. *This motive is isomorphic to the elliptic curve with equation* $E : y^2 = x(x-1)(1-tx)$.
(2) The motives defined over $\mathbb{Q}(\zeta_r)^+$*:*
- $\mathcal{H}_2^+ := \mathcal{H}((\frac{1}{r}, -\frac{1}{r}), (1, 1)|t)$,
- $\mathcal{H}_2^- := \mathcal{H}((\frac{1}{2r}, -\frac{1}{2r}), (1, 1)|t)$.

(3) The two families of motives defined over $\mathbb{Q}(\zeta_q)^+$*:*
- $\mathcal{H}_{3,s}^+ := \mathcal{H}((\frac{1}{q}, -\frac{1}{q}), (\frac{s}{q}, -\frac{s}{q})|t)$, *for* $s \in \mathbb{F}_q^\times$, $s \neq \pm 1$,
- $\mathcal{H}_{3,s}^- := \mathcal{H}((\frac{1}{2q}, -\frac{1}{2q}), (\frac{s}{q}, -\frac{s}{q})|t)$, *for* $s \in \mathbb{F}_q^\times$.

(4) The two families defined over the composition of $\mathbb{Q}(\zeta_q)^+$ *and* $\mathbb{Q}(\zeta_r)^+$*:*
- $\mathcal{H}_{4,s}^+ := \mathcal{H}((\frac{1}{r}, -\frac{1}{r}), (\frac{s}{q}, -\frac{s}{q})$, *for* $s \in \mathbb{F}_q^\times$,
- $\mathcal{H}_{4,s}^- := \mathcal{H}((\frac{1}{2r}, -\frac{1}{2r}), (\frac{s}{q}, -\frac{s}{q})|t)$, *for* $s \in \mathbb{F}_q^\times$.

The notation is chosen so it is consistent with [16]; the + motives are tame at primes dividing 2, while the − motives are (a priory) wild. We will prove that these motives are suitable for the modular method. The proof's strategy can be summarized in the following diagram: to a solution (α, β, γ) to (1) one attaches the hypergeometric motive $\mathcal{H}((a, b), (c, d)|t_0)$ specialized at $t_0 = -\frac{A\alpha^p}{C\gamma^r}$. Then one studies two different types of congruences

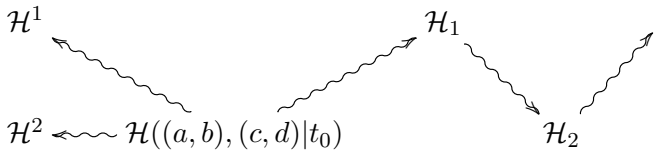

FIGURE 1. Congruences

Parameters	*Curve*	*Exponents*	*Literature*
$(1/2,1/2),(1,1)$	$y^2=x(x-1)(1-tx)$	(p,p,p)	[53]
$(1/3,2/3),(1,1)$	$y^2+xy+\frac{t}{27}y=x^3$	$(p,p,3)$	[18]
$(1/4,3/4),(1,1)$	$y^2+xy=x^3+\frac{t}{64}x$	$(p,p,2)$	[18]
$(1/6,5/6),(1,1)$	$y^2+xy=x^3-\frac{t}{432}$	$(p,p,3)$	[16]
$(1/3,2/3),(1/4,3/4)$	$y^2=x^3-12tx-16t^2$	$(2,p,3)$	[17]
$(1/6,5/6),(1/3,2/3)$	$y^2=x^3-3t^3x+t^4(t+1)$	$(3,p,3)$	[36]

TABLE 1.1. Table of rational rank 2 hypergeometric motives

The left congruences are used to prove properties of the residual representation (namely step (1) of the modular method), while the right ones are used to prove modularity (namely step (2)) via the standard "propagation of modularity" approach.

There is a catch here: to propagate modularity (using some modularity lifting theorem à la Wiles) and to lower the level we need "large residual image" (as in step (3)). Although large image results are expected to hold for geometric representations, there are few instances where unconditional results are proven (and mostly for representations coming from elliptic curves). Even when some modularity results for reducible residual representations are known (as in [48] and [43]), an absolutely irreducible image result is needed in all lowering the level results. This is probably the largest missing step needed to make Darmon's program to work in general. In some particular instances (for example when the HGM is related via a congruence to an elliptic curve) we can circumvent this issue, as will be later explained.

We must warn the reader that some properties of hypergeometric motives are still not completely understood. If we specialize the parameter t at a particular value t_0, ramification at the so called "tame" primes (primes dividing the numerator or denominator of $t_0(t_0-1)$ but not dividing N) is well understood. However, the behavior at the so called "wild" primes (primes dividing N) is not.

In order to make the modular method work, we also need a bound at the wild primes. For the motives $\mathfrak{h}_i^{\pm}$, such bounds can be obtained using the recent article [27] (build upon results of [2]). In this way, we completely fulfill the three stated steps of the modular method.

To keep the article concise, we focus on setting the bases to accomplish the stated steps of the modular method rather than proving non-existence of solutions for new families of exponents. In the article [40] we will apply the present ideas to prove non-existence of solutions to the generalized Fermat equation for exponents $(3,5,p)$.

The article is organized as follows: Section 2 consists of a user's guide to hypergeometric motives. It contains a brief presentation of the theory (including their definition) together with their main properties needed in the present article. Their proofs are mostly given in [29].

Section 3 contains the study of rational hypergeometric motives. In particular, we show how the complete list of rational HGM (listed in Table 3.1) appear in the literature while studying families of the generalized Fermat equation. Here is a summary of the results obtained in this section.

Theorem. *Table 1.1 is a complete table of all rational rank 2 hypergeometric motives with a monodromy matrix of infinite order (up to quadratic twists). The table includes the hypergeometric parameter, an equation of the corresponding elliptic curve, the exponents of the generalized Fermat equation where it can be used together with its appearance in the literature.*

Section 4 contains a detailed analysis of the ramification of the motives $\mathfrak{h}_i^{\pm}$ given in Definition 1.1 (see Theorem 4.1). It also contains the value of the residual conductor of their attached residual Galois representations (Theorem 4.2) and the "finite at p" condition (Theorem 4.3). In particular, we prove that our hypergeometric motives satisfy all the required properties of step (1) in the modular method.

Section 5 is devoted to prove modularity of our motives. Here is a summary of the results we can prove:

- the motive $\mathfrak{h}_2^+$ is modular when $r \mid \alpha\gamma$ (Theorem 5.3),
- the motive $\mathfrak{h}_2^-$ is modular if $r \geq 5$ (Theorem 5.4),
- the motives $\mathfrak{h}_{3,s}^+$ are modular if $q \mid \gamma$ (Theorem 5.5),
- the motives $\mathfrak{h}_{3,s}^-$ are modular if $q \geq 5$ (Theorem 5.6),
- the motives $\mathfrak{h}_{4,s}^+$ are modular if $q \mid \alpha$ and $r \mid \gamma$ (Theorem 5.7),
- the motives $\mod \bar{}_{4,s}$ are modular if either $r \geq 5$ and $q \mid \alpha$ or $q \geq 5$ and $r \mid \gamma$ (Theorem 5.8).

We do not expect any of the required hypothesis to be needed. There are two particular families where unconditional results can be proven (as done in Section 6): the family $(2, p, r)$ and the family $(3, r, p)$. More concretely

- The motive $\mathfrak{h}_{4,s}^+$ for the family $(2, p, r)$ is modular for $r \geq 5$ (see Theorem 6.1).
- The motive $\mathfrak{h}_{4,s}^-$ for the family $(2, p, r)$ is modular if $r \nmid A$ and $r \geq 11$ (see Theorem 6.2).
- The motive $\mathfrak{h}_{4,s}^+$ for the family $(3, p, r)$ is modular if $r \nmid A$ and $r \geq 5$ (see Theorem 6.3).
- The motive $\mathfrak{h}_{4,s}^-$ for the family $(3, p, r)$ is modular if $r \nmid A$ and $r \geq 11$ (see Theorem 6.4).

Section 7 studies the behavior of the motives $\mathfrak{h}_i^{\pm}$ at wild primes. For an odd wild prime $\mathfrak{q}$, we prove that the conductor exponent is at most 3 when $\mathfrak{q} \nmid ABC$ (see Corollary 7.5). At primes $\mathfrak{q}$ dividing 2, we can prove that the conductor is bounded by 6 when $\mathfrak{q} \nmid AC$, assuming that $p, q, r \geq 5$ (see Corollary 7.3). The explicit bounds obtained allow to fully apply the modular method to new families of generalized Fermat equations (assuming the veracity of step (3)). We are left to compute newforms of finitely many spaces of Hilbert modular forms, and prove that they are not related to solutions.

The last section (section 8) explains how to use hypergeometric motives to perform an "elimination" procedure due to Mazur (to our knowledge the unique systematic strategy to perform step (4) in the modular method approach). It is an interesting problem to decide whether other techniques (like the symplectic method) can be adapted to hypergeometric motives.

We include an appendix (due to the second named author and Fernando Rodriguez Villegas) which proves the following result.

Theorem. *Let N be a positive integer different from 1. Then the hypergeometric motive with parameter $(\frac{1}{N}, -\frac{1}{N}), (1, 1)$ is part of the middle cohomology of an explicit hyperelliptic curve.*

As a corollary (which motivated the study and proof of the result) we deduce that the Galois representation attached to the motive $\mathfrak{h}_2^{\pm}$ coincides with Darmon's ones studied in [16] (see Corollaries A.5 and A.11). Still, we believe that the result might be of independent interest.

Acknowledgments: We want to express our gratitude to Fernando Rodriguez Villegas for many helpful conversations as well as his detailed explanation of various properties satisfied by hypergeometric motives. Special thanks go to David Roberts as well, for many fruitful conversations. At last, but not least, we want to thank Nuno Freitas and Lucas Villagra Torcomian for many suggestions on an earlier version of the article.

2. User's guide to Hypergeometric motives

For a nice introduction to the hypergeometric motives used in this article see [46],[7],[32],[25] and [29]. If a is a rational number, by $\exp(a)$ we denote the root of unity $e^{2\pi i a}$.

2.1. Hypergeometric motives and monodromy representations.

The input of a (rank two) hypergeometric motive is a *parameter* consisting of two pairs (a, b), (c, d) of rational numbers (up to translation by integers).

Definition 2.1. *The parameter $(a,b),(c,d)$ is called* generic *if no element of the set $\{a-c, a-d, b-c, b-d\}$ is an integer.*

From now on, we assume that all parameters are generic (the non-generic case is more subtle and will not be needed). The generic condition allows to consider the parameters a,b,c,d as elements in $\mathbb{Q}/\mathbb{Z}$. Set $\gamma = c+d-a-b$. For a parameter $(a,b),(c,d)$, define the following matrices:

$$M_0 := \begin{cases} \begin{pmatrix} \exp(-c) & 0 \\ 0 & \exp(-d) \end{pmatrix} & \text{if } c-d \notin \mathbb{Z}, \\ \exp(-c)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \text{if } c-d \in \mathbb{Z}, \end{cases} \tag{3}$$

$$M_1 := \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & \exp(\gamma) \end{pmatrix} & \text{if } \gamma \notin \mathbb{Z}, \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \text{if } \gamma \in \mathbb{Z}, \end{cases} \tag{4}$$

and

$$M_\infty = \begin{cases} \begin{pmatrix} \exp(a) & 0 \\ 0 & \exp(b) \end{pmatrix} & \text{if } a-b \notin \mathbb{Z}, \\ \exp(a)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \text{if } a-b \in \mathbb{Z}. \end{cases} \tag{5}$$

Let N be the least common denominator of a,b,c,d.

Theorem 2.2. *Let $(a,b),(c,d)$ be generic parameters, and let $x \in \mathbb{P}^1 \setminus \{0,1,\infty\}$. Then there is a monodromy representation*

$$\rho_t : \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}, x) \to \mathrm{GL}_2(\mathbb{Z}[\zeta_N]),$$

whose monodromy matrices at 0, 1 and ∞ are conjugate to M_0, M_1 and M_∞ respectively.

Proof. The result is due to Levelt, see for example [7, Theorem 3.5]. □

For $s \in \mathbb{P}^1$, denote by I_s an inertia group of $\mathrm{Gal}_{\overline{\mathbb{Q}}(t)}$ at s. For each prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_N)$, the monodromy representation extends (by continuity) to a geometric representation

$$\rho_t^{\mathrm{geom}} : \mathrm{Gal}_{\overline{\mathbb{Q}}(t)} \to \mathrm{GL}_2(\mathbb{Z}[\zeta_N]_{\mathfrak{p}}), \tag{6}$$

satisfying

(1) The representation ρ_t^{geom} is unramified outside the points $\{0,1,\infty\}$.
(2) For $s \in \{0,1,\infty\}$,

$$\rho_t^{\mathrm{geom}}(I_s) \simeq \langle M_s \rangle.$$

Remark 1. More generally, one can study representations of the projective line $\mathbb{P}^1$ (with coefficients in $\mathbb{C}$ or in a finite field) which are unramified outside finitely many points and having fixed (up to conjugation) monodromy matrices. The case of three ramified points is simpler, since this case is "rigid" (i.e. the representation is determined by the conjugacy class of the matrices M_0, M_1 and M_∞ as explained in Remark 2.10 of [29]).

The geometric representation is expected to match the (restriction to $\mathrm{Gal}_{\overline{\mathbb{Q}}(t)}$ of a) representation of a pure motive defined over a cyclotomic field (see [4]). In the rank two case the motive can be explicitly constructed: it is (up to a twist by a Hecke character) part of the new middle cohomology of the so called "Euler's curve". Explicitly, let $(a,b),(c,d)$ be a generic parameter, and let N be their least common denominator. Define the quantities:

$$A=(d-b)N,\qquad B=(b-c)N,\qquad C=(a-d)N,\qquad D=dN, \tag{7}$$

and define Euler's curve by

$$\mathcal{C}: y^N = x^A(1-x)^B(1-tx)^C t^D. \tag{8}$$

The curve $\mathcal{C}$ is geometrically irreducible precisely when $\gcd(A,B,C,N)=1$. In this case, the new part of the ζ_N-eigenspace of the first étale cohomology group of $\mathcal{C}$ is a motive $\mathcal{M}_{\mathcal{C}}$ defined over $F=\mathbb{Q}(\zeta_N)$. The hypergeometric motive $\mathcal{H}((a,b),(c,d)|t)$ is a twist of $\mathcal{M}_{\mathcal{C}}$ by a Jacobi motive that we now describe.

2.1.1. *The Jacobi motive.* Let $\mathfrak{q}$ be a prime ideal of $F=\mathbb{Q}(\zeta_N)$ not dividing N, and let $\mathbb{F}_q$ denote its residue field (so $N\mid(q-1)$). Following [52], for x an integer prime to $\mathfrak{q}$, let $\chi_{\mathfrak{q}}(x)$ denote the N-th root of unity congruent to $x^{(q-1)/N}$ modulo $\mathfrak{q}$. Extend the definition by setting $\chi_{\mathfrak{q}}(x)=0$ if $\mathfrak{q}\mid x$. This determines a character of order N

$$\chi_{\mathfrak{q}}: (\mathbb{Z}[\zeta_N]/\mathfrak{q})^\times \to \mathbb{C}^\times. \tag{9}$$

Let ψ be an additive character of $\mathbb{F}_q$

Definition 2.3. *Let $\mathbf{a}=(a_1,\dots,a_r)$ and $\mathbf{b}=(b_1,\dots,b_s)$ be two sets of rational numbers and let N be their least common denominator. The Jacobi motive attached to $\mathbf{a},\mathbf{b}$ at a prime ideal $\mathfrak{q}$ of $K=\mathbb{Q}(\zeta_N)$ not dividing N is the sum*

$$\mathbf{J}(\mathbf{a},\mathbf{b})(\mathfrak{q}) = (-1)^{r+s+1}\frac{g(\psi,\chi_{\mathfrak{q}}^{Na_1})\cdots g(\psi,\chi_{\mathfrak{q}}^{Na_r})g(\psi,\chi_{\mathfrak{q}}^{N(\sum_j b_j-\sum_i a_i)})}{g(\psi,\chi_{\mathfrak{q}}^{Nb_1})\cdots g(\psi,\chi_{\mathfrak{q}}^{Nb_s})}. \tag{10}$$

The value $\mathbf{J}(\mathbf{a},\mathbf{b})(\mathfrak{q})$ does not depend on the choice of the additive character ψ. In [52] Weil proves that a Jacobi motive is a Hecke character, i.e. there exists a character $\chi:\mathbb{A}_{\mathbb{Q}(\zeta_N)}\to\mathbb{C}^\times$ such that for all but finitely many prime ideals $\mathfrak{q}$ of K,

$$\mathbf{J}(\mathbf{a},\mathbf{b})(\mathfrak{q})=\chi(\mathfrak{q}).$$

Definition 2.4. *Suppose that Euler's curve $\mathcal{C}$ is irreducible. Then the hypergeometric motive $\mathcal{H}((a,b),(c,d)|t)$ is defined by*

$$\mathcal{H}((a,b),(c,d)|t) := \mathcal{M}_{\mathcal{C}}\otimes\mathbf{J}((-a,-b,c,d),(c-b,d-a))^{-1}(-1)^{d-b}, \tag{11}$$

where $(-1)^{d-b}$ denotes the quadratic character of $\mathbb{A}_F$, whose value at a prime ideal $\mathfrak{q}$ not dividing N equals $\varpi(-1)^{(d-b)(\mathcal{N}(q)-1)}$, for ϖ any generator of the character group of $\mathcal{O}_F/\mathfrak{q}$.

Remark 2. All hypergeometric motives considered in the present article satisfy that Euler's curve is irreducible, so the previous definition applies. When Euler's curve $\mathcal{C}$ is reducible, the hypergeometric motive is defined (see Definition 6.27 of [29]) as a twist of an irreducible Euler's curve (with parameters $(a-d,b-d),(c-d,1)$) by another Jacobi motive.

It follows from its definition that $\mathcal{H}((a,b),(c,d)|t)$ is defined over the field F.

Lemma 2.5. *Let $(a,b),(c,d)$ be a generic parameter.*

(1) If $v_2(d-b)=0$, the character $(-1)^{d-b}$ is trivial.

(2) If $v_2(d-b)=-1$, the character $(-1)^{d-b}$ matches the quadratic character $\left(\frac{-1}{\mathfrak{q}}\right)$.

Proof. Let $\mathfrak{q}$ denote a prime of F not dividing $2N$, and let $\mathbb{F}_\mathfrak{q}$ denote the finite field $\mathcal{O}_F/\mathfrak{q}$. Then $\varpi(-1)$ is 1 when -1 is a square in $\mathbb{F}_\mathfrak{q}$, or equivalently

$$\varpi(-1) = \begin{cases} 1 & \text{if } \mathcal{N}\mathfrak{q} \equiv 1 \pmod 4, \\ -1 & \text{if } \mathcal{N}\mathfrak{q} \equiv 3 \pmod 4. \end{cases}$$

When $d-b$ has odd denominator the character $(-1)^{d-b}$ is clearly trivial (since $\mathcal{N}\mathfrak{q}-1$ is even). When $d-b$ has even denominator (of valuation 1), the exponent $(d-b)(\mathcal{N}\mathfrak{q}-1)$ is odd precisely when $\mathcal{N}\mathfrak{q} \equiv 3 \pmod 4$, hence the result. □

The motives $\mathfrak{h}_i^+$, for $i = 1, 2, 3, 4$ satisfy the first hypothesis of the lemma, while the motives $\mathfrak{h}_i^-$ satisfy the second one.

Remark 3. In the present article we will consider parameters satisfying the extra condition $a+b$ and $c+d$ being integers. In this case the Jacobi motive $\mathbf{J}(-a,-b,c,d),(c-b,d-a)$ is just a Tate twist (so can be mostly be ignored).

Theorem 2.6. *The Galois representation attached to $\mathcal{H}((a,b),(c,d)|t)$ restricted to $\mathrm{Gal}_{\overline{\mathbb{Q}}(t)}$ is isomorphic to ρ_t^{geom}.*

Proof. See [29, Theorem 7.13]. □

Permuting the order of the parameters in the first or the second entries of the parameter give isomorphic motives, i.e. the motives $\mathcal{H}((a,b),(c,d)|t)$, $\mathcal{H}((b,a),(c,d)|t)$, $\mathcal{H}((a,b),(d,c)|t)$ and $\mathcal{H}((b,a),(d,c)|t)$ are all isomorphic. We will make constant use of this fact while listing hypergeometric motives.

2.2. **Field of definition.** Keeping the previous notation, let $(a,b),(c,d)$ be a generic parameter and let N denote their least common denominator. Let H be the group

$$H := \{r \in (\mathbb{Z}/N)^\times \ : \ \{a,b\} = \{ar, br\} \text{ and } \{c,d\} = \{cr, dr\}\}, \tag{12}$$

i.e. H is the set of elements that leave the sets $\{a,b\}$ and $\{c,d\}$ stable under multiplication (recall that our parameters are elements in $\mathbb{Q}/\mathbb{Z}$). By [29, Lemma 8.1], the group H is a subgroup of $\mathbb{Z}/2 \times \mathbb{Z}/2$.

The group H can be canonically identified with a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Let K be the field $\mathbb{Q}(\zeta_N)^H$ fixed by the subgroup H. The following result is proven in [29, Theorem 8.2].

Theorem 2.7. *If $a+b$ and $c+d$ are integers and $\mathcal{C}$ is irreducible, then the motive $\mathcal{H}((a,b),(c,d)|t)$ is defined over K. In particular, for every prime ideal $\mathfrak{p}$ of K, the geometric Galois representation ρ_t^{geom} extends to a representation*

$$\rho_{t,\mathfrak{p}} : \mathrm{Gal}_{K(t)} \to \mathrm{GL}_2(K_\mathfrak{p}). \tag{13}$$

Specializations of $\rho_{t,\mathfrak{p}}$ provide compatible families of Galois representations as will be explained in the next section. Although the hypothesis $a+b$ and $c+d$ being integers seems quite restrictive, most motives defined over totally real fields satisfy this condition.

2.3. **Specializations.** For $(a,b),(c,d)$ generic parameters and t_0 a rational number, $t_0 \neq 0, 1$, we can consider the specialization of the motive $\mathcal{H}((a,b),(c,d)|t)$ at t_0 (the values 0 and 1 correspond to singular values of the motive). The combinatorial nature of an hypergeometric motive allows to obtain a lot of information of the specialized motive, namely:

- *A description of the set of bad places:* it consists of prime ideals dividing the numerator/denominator of t_0 or $t_0 - 1$ but not dividing N (the so called *tame* primes) together with prime ideals dividing N (the so called *wild* primes).
- *A description of inertia at tame primes.*

- *The trace of Frobenius at good primes.*

Fix an additive character ψ on $\mathbb{F}_q$. For $\omega \in \widehat{\mathbb{F}_q^\times}$, a character of $\mathbb{F}_q^\times$, denote by $g(\psi,\omega)$ the Gauss sum

$$g(\psi,\omega) = \sum_{x\in\mathbb{F}_q^\times} \omega(x)\psi(x). \tag{14}$$

Let $\mathfrak{q}$ be a prime ideal of $F=\mathbb{Q}(\zeta_N)$ and let $\mathbb{F}_q$ be its residual field. Let $\chi_\mathfrak{q}$ be the character of $\mathbb{F}_q$ defined in (9).

Definition 2.8 (Finite hypergeometric sum)**.** *For $t_0 \in \mathbb{F}_q$, define the finite hypergeometric series $H_\mathfrak{q}((a,b),(c,d)|t_0)$ by*

$$H_\mathfrak{q}((a,b),(c,d)|t_0) = \frac{1}{1-q}\sum_{\omega\in\widehat{\mathbb{F}_q^\times}} \frac{g(\psi,\chi_\mathfrak{q}^{-aN}\omega)g(\psi,\chi_\mathfrak{q}^{cN}\omega^{-1})}{g(\psi,\chi_\mathfrak{q}^{-aN})g(\psi,\chi_\mathfrak{q}^{cN})}\frac{g(\psi,\chi_\mathfrak{q}^{-bN}\omega)g(\psi,\chi_\mathfrak{q}^{dN}\omega^{-1})}{g(\psi,\chi_\mathfrak{q}^{-bN})g(\psi,\chi_\mathfrak{q}^{dN})}\omega(t_0).$$

The value $H_\mathfrak{q}((a,b),(c,d)|t_0)$ does not depend on the choice of the additive character ψ. If $\mathfrak{p}$ is a prime ideal of F, denote by $I_\mathfrak{p}$ an inertia group of Gal_F at $\mathfrak{p}$.

Theorem 2.9. *Let $(a,b),(c,d)$ be a generic parameter satisfying that $a+b$ and $c+d$ are integers. Let $t_0\in\mathbb{Q}$ be a rational number and let $K=\mathbb{Q}(\zeta_N)^H$. Then $\mathcal{H}((a,b),(c,d)|t_0)$ provides a compatible system of irreducible Galois representations*

$$\{\rho_{t_0,\mathfrak{p}} : \mathrm{Gal}_{\mathbb{Q}(\zeta_N)} \to \mathrm{GL}_2(\mathbb{Q}(\zeta_N)_\mathfrak{p})\}_\mathfrak{p},$$

where $\mathfrak{p}$ ranges over primes ideals of $\mathbb{Q}(\zeta_N)$. The family satisfies the following properties:

1. *Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Q}(\zeta_N)$ not dividing N nor the norm of $\mathfrak{p}$. Let $\mathrm{Frob}_\mathfrak{q}$ be a Frobenius element. Then if $v_\mathfrak{q}(t_0(t_0-1))=0$, the representation $\rho_{t_0,\mathfrak{p}}$ is unramified at $\mathfrak{q}$ and*
$$\mathrm{Tr}\,\rho_{t_0,\mathfrak{p}}(\mathrm{Frob}_\mathfrak{q}) = H_\mathfrak{q}((a,b),(c,d)|t_0).$$
2. *If $\mathfrak{q}\nmid\mathfrak{p}N$ and $r=v_\mathfrak{q}(t_0)>0$, then $\rho_{t_0,\mathfrak{p}}(I_\mathfrak{q})\simeq\langle M_0^r\rangle$ (up to conjugation).*
3. *If If $\mathfrak{q}\nmid\mathfrak{p}N$ and $r=v_\mathfrak{q}(t_0)<0$, then $\rho_{t_0,\mathfrak{p}}(I_\mathfrak{q})\simeq\langle M_\infty^r\rangle$ (up to conjugation).*
4. *If If $\mathfrak{q}\nmid\mathfrak{p}N$ and $r=v_\mathfrak{q}(t_0-1)>0$, then $\rho_{t_0,\mathfrak{p}}(I_\mathfrak{q})\simeq\langle M_1^r\rangle$ (up to conjugation).*
5. *The family extends to a family $\{\widetilde{\rho}_{t_0,\mathfrak{p}} : \mathrm{Gal}_K \to \mathrm{GL}_2(K_\mathfrak{p})\}$, where $\mathfrak{p}$ ranges over prime ideals of K.*

Proof. The first statement is proved in [29, Theorems 4.8 and 7.23]; the three statements regarding inertia groups are proved in [29, Appendix A] when M_i^r is the identity and in general in [26]. The last statement is proved in [29, Corollary 8.19]. □

Remark 4. A script written by Fernando Ridriguez Villegas to compute p-adically $H_\mathfrak{q}((a,b),(c,d)|t_0)$ in terms of the p-adic Gamma function is available at the github repository

https://github.com/frvillegas/frvmath.

As mentioned in the introduction, the result does not provide any information at wild primes. There is a caveat in the statement: the motive is defined over $K=F^H$, but the formula relating the trace of a Frobenius element to an hypergeometric motive is only proved over F (although it is expected to hold over K as well).

Remark 5. The last result implies that even when $v_\mathfrak{q}(t_0)$ is positive, the motive $\mathcal{H}((a,b),(c,d)|t_0)$ might have good reduction at $\mathfrak{q}$ (precisely when the matrix M_0 has finite order dividing $v_\mathfrak{q}(t_0)$). In this case, one can still give a formula to compute the trace of a Frobenius endomorphism at $\mathfrak{q}$ (assuming $\mathfrak{q}\nmid N$), as described in [29, Appendix A].

Remark 6. The normalization of the motive $\mathcal{H}((a,b),(c,d)|t_0)$ given in [29] is useful to work with any rank 2 hypergeometric motive, but while working over totally real fields it might be a Tate twist of the expected Hilbert modular form (when the motive happens to be modular). It is the case that when $a+b$ and $c+d$ are integers:

- if $c,d \in \mathbb{Z}$ (or $a,b \in \mathbb{Z}$), then no twist is needed,
- otherwise the motive $\mathcal{H}((a,b),(c,d)|t_0)(1)$ has Hodge-Tate weights $\{0,1\}$.

We will disregard this subtlety, but the reader should keep it in mind while matching the motive to an automorphic form.

There is an isomorphism of motives (whose veracity follows from a simple manipulation of the finite hypergeometric sum definition)

$$\mathcal{H}((a,b),(c,d)|t_0) \simeq \mathcal{H}((c,d),(a,b)|t_0^{-1}). \tag{15}$$

This justifies the ambiguity while choosing the order of the pairs of parameters.

2.4. **Congruences.** Let p be a rational prime. For a,b rational numbers, denote by $a \sim_p b$ the relation defined by the condition that the denominator of $a-b$ is a p-th power, extended naturally to vectors component-wise.

Theorem 2.10. *Let p be a prime number, and let $(a,b),(c,d)$ and $(a',b'),(c',d')$ be generic parameters. Let F be the composite of the cyclomotic fields where both motives are defined. If $(a,b) \sim_p (a',b')$ and $(c,d) \sim_p (c',d')$ then both motives over F are congruent modulo $\mathfrak{p}$, for $\mathfrak{p}$ any prime ideal of their coefficient field dividing p.*

Proof. See [29, Theorem 10.3]. □

2.5. **Galois action.** Keeping the previous notation, let $(a,b),(c,d)$ be a generic rational parameter with common denominator N. Let $t_0 \in \mathbb{Q}$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ with $\sigma(\zeta_N) = \zeta_N^j$ for some j coprime with N. Then

$$\mathcal{H}((a,b),(c,d)|t_0)^\sigma = \mathcal{H}((ja,jb),(jc,jd)|t_0). \tag{16}$$

The result follows from [29, Proposition 6.3]. This allows to chose the parameters so that (up to Galois conjugation) the numerator of a equals 1.

2.6. **Quadratic Twists.** Let $(a,b),(c,d)$ be generic parameters such that $a+b$ and $c+d$ are integers.

Proposition 2.11. *Under the previous hypothesis, the motive $\mathcal{H}((a+1/2,b+1/2),(c+1/2,d+1/2)|t_0)$ is (up to a Tate twist) a quadratic twist by $\sqrt{t_0}$ of the motive $\mathcal{H}((a,b),(c,d)|t_0)$.*

Proof. By Theorem 2.9 it is enough to prove the stated relation for the finite hypergeometric sums $H_q((a,b),(c,d)|t_0)$ and $H_q((a+1/2,b+1/2),(c+1/2,d+1/2)|t_0)$. It follows from [29, Proposition 6.3] that

$$H_q((a+1/2,b+1/2),(c+1/2,d+1/2)|t_0) = \omega(t_0)^{\frac{q-1}{2}} H_q((a,b),(c,d)|t_0)\kappa,$$

where ω is a generator of $\mathbb{F}_q^\times$ (so $\omega^{\frac{q-1}{2}}$ equals the quadratic character of $\mathbb{F}_q^\times$) and

$$\kappa = \frac{g(\psi,\omega^{(a+1/2)(q-1)})g(\psi,\omega^{(b+1/2)(q-1)})g(\psi,\omega^{-(c+1/2)(q-1)})g(\psi,\omega^{-(d+1/2)(q-1)})}{g(\psi,\omega^{a(q-1)})g(\psi,\omega^{b(q-1)})g(\psi,\omega^{-c(q-1)})g(\psi,\omega^{-d(q-1)})}.$$

Since $a+b \in \mathbb{Z}$, $\omega^{a(q-1)} = (\omega^{b(q-1)})^{-1}$. Recall that

$$g(\psi,\omega)g(\psi,\omega^{-1}) = \begin{cases} \omega(-1)q & \text{if } \omega \text{ is non-trivial,} \\ 1 & \text{if } \omega \text{ is trivial.} \end{cases}$$

Parameters	Order at 0	Order at 1	Order at ∞	Equation
$(1/2,1/2),(1,1)$	∞	∞	∞	(p,p,p)
$(1/3,2/3),(1,1)$	∞	∞	3	$(p,p,3)$
$(1/4,3/4),(1,1)$	∞	∞	4	$(p,p,2)$
$(1/6,5/6),(1,1)$	∞	∞	6	$(p,p,3)$
$(1/3,2/3),(1/4,3/4)$	3	∞	4	$(2,p,3)$
$(1/6,5/6),(1/3,2/3)$	3	∞	6	$(3,p,3)$
$(1/6,5/6),(1/2,1/2)$	∞	∞	6	$(p,p,3)$
$(1/4,3/4),(1/2,1/2)$	∞	∞	4	$(p,p,2)$
$(1/3,2/3),(1/2,1/2)$	∞	∞	3	$(p,p,3)$
$(1/6,5/6),(1/4,3/4)$	4	∞	6	$(2,p,3)$

TABLE 3.1. Rational HGM with a not-finite order monodromy matrix

Then if neither a,b,c,d are integers nor half integers, $\kappa=1$. Otherwise, if two are integers or half integers, $\kappa=q^{\pm 1}$. □

3. Rational rank 2 hypergeometric motives

The combinatorial nature of hypergeometric motives makes it clear that there are only finitely many rank 2 rational ones: let N denote the least common multiple of the denominators of the parameter $(a,b),(c,d)$. If the motive is rational then H (a subgroup of $\mathbb{Z}/2\times\mathbb{Z}/2$) must equal the group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, so $N\in\{1,2,3,4,6,8,12\}$ (but it is not hard to verify that N cannot be 8). A small computer search gives a complete list of rational hypergeometric motives with at least one monodromy matrix of infinite order as given in Table 3.1. The table includes the order of inertia at the three ramified points and the exponents of the generalized Fermat equation it allows to study (each case will be studied in detail).

Note that the seventh HGM (the one after the horizontal line) is a quadratic twist of the second one (obtained by adding 1/2 to all parameters), the eighth is a quadratic twist of the third one and so on, hence only the first six HGM give different elliptic curves (up to isomorphism). The explicit equation we use for the elliptic curve attached to the listed HGM were found by Cohen in [31] (see also [30]).

3.1. **The motive $\mathcal{H}((1/2,1/2),(1,1)|t)$:** corresponds to the family of elliptic curves in Legendre equation

$$E_t : y^2 = x(x-1)(1-tx), \tag{17}$$

or equivalently the equation

$$E : y^2 = x(x+1)(x+t).$$

The curve has full 2-torsion. Its invariants are

$$\Delta(E_t) = 2^4t^2(t-1)^2, \qquad j(E_t) = \frac{2^8(t^2-t+1)^3}{t^2(t-1)^2}.$$

All odd primes dividing the numerator of $t(t-1)$ are primes of multiplicative reduction, while the odd primes dividing the denominator of t have inertial type a ramified quadratic twist of a multiplicative reduction type (i.e. are quadratic twist of a Steinberg representation). The reduction type at 2 is a little more complicated to describe.

Lemma 3.1. *Let $t_0\in\mathbb{Q}$ be a rational number with $t_0\neq 0,1$. The conductor exponent s of E_{t_0} at the prime 2 is given by:*

- *If* $v_2(t_0) \geq 0$, *then*

$$s = \begin{cases} 5 & \text{if } t_0 \equiv 2,3 \pmod 4, \\ 4 & \text{if } t_0 \equiv 1 \pmod 4, \\ 3 & \text{if } v_2(t_0) = 2,3, \\ 0 & \text{if } v_2(t_0) = 4, \\ 1 & \text{if } v_2(t_0) \geq 5. \end{cases}$$

- *If* $v_2(t_0) < 0$, *then*

$$s = \begin{cases} 6 & \text{if } 2 \nmid v_2(t_0), \\ 4 & \text{if } 2 \mid v_2(t_0) \text{ and } t_0/2^{v_2(t_0)} \equiv 3 \pmod 4, \\ 3 & \text{if } v_2(t_0) = -2 \text{ and } 4t_0 \equiv 1 \pmod 4, \\ 0 & \text{if } v_2(t_0) = -4 \text{ and } 16t_0 \equiv 1 \pmod 4, \\ 1 & \text{if } 2 \mid v_2(t_0) < -4 \text{ and } t_0/2^{v_2(t_0)} \equiv 1 \pmod 4. \end{cases}$$

Proof. Follows from applying Tate's algorithm [49] to the different cases. □

If (α, β, γ) is a solution to the generalized Fermat equation $Ax^p + By^p + Cz^p = 0$, set $t_0 = -\frac{A\alpha^p}{C\gamma^p}$, and consider the twisted curve

$$E : C\gamma^p y^2 = x(x-1)\left(1 + \frac{A\alpha^p}{C\gamma^p}x\right).$$

The twist is needed because the monodromy matrix at ∞ equals $(-1)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence we need to cancel the extra -1. After a change of variables we obtain the famous Frey elliptic curve ([53])

$$y^2 = x(x - A\alpha^p)(x + C\gamma^p).$$

3.2. **The motive $\mathcal{H}((1/3, 2/3), (1, 1)|t)$:** corresponds to the elliptic curve with equation

$$E_t : y^2 + xy + \frac{t}{27}y = x^3. \tag{18}$$

The point $P = (0, 0)$ is a 3-torsion point of E_t. The curve invariants are

$$\Delta(E_t) = -3^{-9}t^3(t-1), \qquad j(E_t) = \frac{3^3(8t-9)^3}{t^3(t-1)}.$$

To a putative solution (α, β, γ) of the equation $Ax^p + By^p + Cz^3 = 0$ corresponds the specialization $t_0 = -\frac{A\alpha^p}{C\gamma^3}$, giving the elliptic curve

$$E : y^2 - 3C\gamma xy + A\alpha^p C^2 y = x^3,$$

with

$$\Delta(E) = 3^3 A^3 BC^8 \alpha^{3p}\beta^p, \qquad j(E) = -\frac{3^9 C\gamma^3(8A\alpha^p + 9C\gamma^3)}{A^3 B\alpha^{3p}\beta^p}.$$

The curve has multiplicative reduction at primes dividing A and B, and its local type at primes dividing C is a Principal Series given by a character of order 3. The ramification at the prime 3 can be obtained running Tate's algorithm to the equation. When $A = B = C = 1$ the curve matches the one studied by Darmon and Merel in [18].

3.3. **The motive $\mathcal{H}((1/4,3/4),(1,1)|t)$:** corresponds to the elliptic curve with equation

$$E_t : y^2 + xy = x^3 + \frac{t}{64}x. \tag{19}$$

The point $P = (0,0)$ is a 2-torsion point of E_t. Its invariants are

$$\Delta(E_t) = -2^{12}t^2(t-1), \qquad j(E_t) = \frac{2^6(3t-4)^3}{t^2(t-1)}. \tag{20}$$

Since the monodromy matrix at the point ∞ has order 4 (instead of 2), we need to take a quadratic twist of the equation. To a putative solution (α,β,γ) of equation $Ax^p+By^p+Cz^2=0$ one attaches the elliptic curve

$$E : y^2 = x^3 - \frac{2^2 3^3(3A\alpha^p + 4C\gamma^2)}{C}x + \frac{2^4 3^3(9A\alpha^p + 8C\gamma^2)\gamma}{C},$$

with invariants

$$\Delta(E) = -\frac{2^{12}3^{12}A^2B\alpha^{2p}\beta^p}{C^3}, \qquad j(E) = \frac{2^6(3A\alpha^p + 4C\gamma^2)^3}{A^2B\alpha^{2p}\beta^p}.$$

Primes dividing A and B are of multiplicative reduction, while primes dividing C have inertial type that of a Principal series given by an order 4 character. Special care needs to be taken at primes dividing 2 and 3. When $A=B=C=1$, the curve matches the one studied by Darmon and Merel in [18].

3.4. **The motive $\mathcal{H}((1/6,5/6),(1,1)|t)$:** corresponds to the elliptic curve with equation

$$E_t : y^2 + xy = x^3 - \frac{t}{432}. \tag{21}$$

It has invariants

$$\Delta(E_t) = \frac{-t(t-1)}{2^4 3^3}, \qquad j(E_t) = \frac{-2^4 3^3}{t(t-1)}.$$

One again, to a putative solution (α,β,γ) of the equation $Ax^p + By^p + Cz^3 = 0$, one attaches the elliptic curve obtained by specialization at $t_0 = -\frac{A\alpha^p}{C\gamma^3}$ twisted by γ, i.e.

$$E : y^2 = x^3 - 27C^4\gamma^2 x - 54(2A\alpha^p + C\gamma^3)C^5,$$

with invariants

$$\Delta(E) = 2^8 3^9 ABC^{10}\alpha^p\beta^p, \qquad j(E) = \frac{2^4 3^3 C^2\gamma^6}{AB\alpha^p\beta^p}.$$

Primes dividing A and B (but not dividing 6) have multiplicative reduction, while primes dividing C are primes with inertial type a Principal series given by an order 6 character. The reduction type at the primes 2 and 3 can be determined using Tate's algorithm. This elliptic curve matches the hyperelliptic curve C^- of [16] for $q=3$.

3.5. **The motive $\mathcal{H}((1/3,2/3),(1/4,3/4)|t)$:** corresponds to the elliptic curve with equation

$$E_t : y^2 = x^3 - 12tx + 16t^2, \tag{22}$$

with invariants

$$\Delta(E_t) = -2^{12}3^3t^3(t-1), \qquad j(E_t) = \frac{-2^6 3^3}{(t-1)}.$$

Historically, one studies the equation $Ax^2 + By^3 = Cz^p$ (i.e. the equation for exponents $(2,3,p)$) instead of the equation with exponents $(2,p,3)$. If (α,β,γ) is a putative solution to $Ax^2 + By^3 =$

Cz^p, then (α,γ,β) is a solution to $Ax^2+(-C)z^p+By^3=0$. Specializing (22) at $t_0=-\frac{A\alpha^2}{B\beta^3}$ and twisting by α gives the curve

$$E: y^2 = x^3 + 12AB^3\beta x + 16A^2B^4\alpha,$$

with invariants

$$\Delta(E) = -2^{12}3^3A^3B^8C\gamma^p, \qquad j(E) = \frac{1728B\beta^3}{C\gamma^p}.$$

This curve is the quadratic twist by $\sqrt{2B}$ of the elliptic curve associated to the equation $Ax^2+By^3=Cz^p$ by Darmon and Granville in [17].

3.6. **The motive $\mathcal{H}((1/6,5/6),(1/3,2/3)|t)$:** corresponds to the elliptic curve with equation

$$E_t: y^2 = x^3 - 3t^3x + t^4(t+1), \tag{23}$$

with invariants

$$\Delta(E_t) = -2^4 3^3 t^8(t-1)^2, \qquad j(E_t) = \frac{-2^8 3^3 t}{(t-1)^2}.$$

Once again, instead of studying the equation $Ax^3+By^3=Cz^p$, we consider the equation $Ax^3+(-C)z^p+By^3=0$. Let (α,β,γ) be a putative solution of $Ax^3+By^3=Cz^p$. Specializing (23) at $t_0=-\frac{A\alpha^3}{B\beta^3}$ and twisting by β (to lower the order of the monodromy matrix from 6 to 3) we obtain the elliptic curve

$$E: y^2 = x^3 + 3A^3B\alpha\beta x + A^4B(B\beta^3 - A\alpha^3),$$

with invariants

$$\Delta(E) = -432A^8B^2C^2\gamma^{2p}, \qquad j(E) = \frac{6912AB\alpha^3\beta^3}{C^2\gamma^{2p}}.$$

When $A=B=C=1$, this curve matches the one studied by Kraus in [36] (see equation (4−3)).

4. The generalized Fermat equation

The goal of this section is to prove that the hypergeometric motives of Definition 1.1 are suitable for the modular method. Keeping the introduction's notation, let (q,p,r) be the exponents of (1) lying in one of the four lines $L_1,\dots,L_4$. To give unified statements, denote by $\mathcal{H}_i^{\pm}(t)$ the motive (or family of motives) attached to the line L_i as given in Definition 1.1 (although they might depend of an extra parameter s, their conductor will not). Let $K=F^H$ denote its field of definition.

For d an integer, let θ_d be the quadratic character attached to the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. By abuse of notation, we use the same symbol to denote the quadratic character of $\mathrm{Gal}_{\mathbb{Q}}$ (from class field theory) and its restriction to any subgroup Gal_L for L a number field. Let (α,β,γ) be a primitive solution of the equation and set $t_0:=-\frac{A\alpha^q}{C\gamma^r}$. To ease notation, we introduce

$$\mathfrak{h}_i^+ := \mathcal{H}_i^+(t_0), \qquad \mathfrak{h}_i^- := \mathcal{H}_i^-(t_0)\otimes\theta_\gamma. \tag{24}$$

Theorem 4.1. *Let ℓ be a prime ideal of K. Then*

- *If $\ell\nmid 2ABCp\alpha\beta\gamma$ then $\mathfrak{h}_1^-$ is unramified at ℓ.*
- *If $\ell\nmid ABCpr\alpha\beta$ then $\mathfrak{h}_2^+$ is unramified at ℓ.*
- *If $\ell\nmid 2ABCpr\alpha\beta$ then $\mathfrak{h}_2^-$ is unramified at ℓ.*
- *If $\ell\nmid ABCpq\beta$ then $\mathfrak{h}_3^+$ is unramified at ℓ.*
- *If $\ell\nmid 2ABCpq\beta$ then $\mathfrak{h}_3^-$ is unramified at ℓ.*
- *If $\ell\nmid ABCpqr\beta$ then $\mathfrak{h}_4^+$ is unramified at ℓ.*
- *If $\ell\nmid 2ABCpqr\beta$ then $\mathfrak{h}_4^-$ is unramified at ℓ.*

Proof. Let ℓ be a prime number. If $v_\ell(t_0(t_0-1))=0$ and $\ell \nmid pqr$ (or equivalently $\ell \nmid ABCpqr\alpha\beta\gamma$) then $\mathcal{H}_i^+(t_0)$ is unramified at ℓ by Theorem 2.9. The same is true for $\mathcal{H}_i^-(t_0)$ if we furthermore assume that $\ell \nmid 2$.

Suppose then that $\ell \mid \alpha$, but $\ell \nmid Apqr$, so $q \mid v_\ell(t_0)$. The parameter given in Definition 1.1 makes (by construction) the monodromy matrix M_0 (as defined in (3)) of the motive $\mathcal{H}_i^\pm(t_0)$ to have order q if $q \neq p$ and order ∞ if $q=p$. Then the second statement of Theorem 2.9 implies that $\mathcal{H}_i^\pm(t_0)$ is unramified at primes dividing α when $q \neq p$ (proving the last four cases).

When $\ell \mid \gamma$ the situation is similar, but the matrix M_∞ has order:

- p for the motive $H_i^+(t_0)$ when $r \neq p$,
- $2p$ for the motive $H_i^-(t_0)$ when $r \neq p$,
- ∞ when $r=p$.

The same proof as before implies that the motive $\mathcal{H}_i^+(t_0)$ is unramified at primes dividing γ for $i=2,3,4$. The monodromy matrix M_∞ of the motive $\mathcal{H}_i^-$ has order $2p$, so the quadratic twist $\mathcal{H}_i^-(t_0)\otimes\theta_\gamma$ has order p (as occurs in the proof of Fermat's last theorem). Then the motive $\mathcal{H}_i^-(t_0)\otimes\theta_\gamma$ is also unramified at primes dividing γ for $i=2,3,4$.

The matrix M_1 always has infinite order, so the representation is ramified at all prime ideals dividing β but not dividing pqr. □

Let $\mathfrak{p}$ be a prime ideal of K dividing p. Then the $\mathfrak{p}$-th residual representation attached to the motive $\mathfrak{h}_i^\pm$ has the expected ramification.

Theorem 4.2. *Let $\rho_\mathfrak{p}^\pm : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be the $\mathfrak{p}$-th Galois representation attached to the motive $\mathfrak{h}_i^\pm$ respectively. Let ℓ be a prime ideal of K not dividing $2ABCpqr$. Then the residual representation $\overline{\rho_\mathfrak{p}^\pm}$ is unramified at ℓ. Furthermore, if $\ell \mid 2$, the representation $\overline{\rho_\mathfrak{p}+}$ is also unramified at ℓ.*

Proof. The last theorem implies that we only need to prove the result for primes ℓ of K dividing $\alpha\beta\gamma$ but not dividing $2ABCpqr$. Suppose that $\ell \mid \alpha$, and consider the motive $\mathfrak{h}_1^-$. Define the motive $\mathfrak{h} := \mathcal{H}((\frac{1}{2}+\frac{1}{p},\frac{1}{2}),(1,1)|t_0)\otimes\theta_\gamma$. Theorem 2.10 implies that over the field $\mathbb{Q}(\zeta_p)$, the motives $\mathfrak{h}$ and $\mathfrak{h}_1^-$ are congruent modulo $\mathfrak{p}$. Since $v_\ell(\alpha)\equiv 0 \pmod p$, the motive $\mathfrak{h}$ is unramified at ℓ (by Theorem 2.9), hence $\overline{\rho_\mathfrak{p}^-}$ is unramified at ℓ while restricted to $\mathrm{Gal}_{K(\zeta_p)}$. Since the extension $K(\zeta_p)/K$ is unramified at ℓ, the same is true for $\overline{\rho_\mathfrak{p}^-}$. The same argument proves that the residual representation is unramified at primes dividing β (since $\mathfrak{h}$ has monodromy matrix of order $2p$ at 1). To prove the result for primes dividing γ, one considers the motive $\mathfrak{h} := \mathcal{H}((\frac{1}{2},\frac{1}{2}),(\frac{1}{p},1)|t_0)$.

The same proof works for all other motives $\mathfrak{h}_i^\pm$: consider the hypergeometric motive obtained by adding $\frac{1}{p}$ to one of the first two coordinates. This new motive will be unramified at primes dividing β and also at primes dividing α when $i=2$. □

At last, we need a similar result for primes dividing p. Assume that $p \neq 2$.

Theorem 4.3. *Let $\mathfrak{p}$ be a prime ideal of K dividing p, such that $\mathfrak{p} \nmid 2ABC$. Then $\overline{\rho_\mathfrak{p}^\pm}$ arises from a finite flat group scheme.*

Proof. The result for $i=1$ follows from [47, Proposition 5] while for $i=2$ it follows from [16, Proposition 1.15]. We focus on the case $i=4$ (the novelty of the present article). If $\mathfrak{p} \nmid \alpha\beta\gamma$, then t_0 reduces modulo $\mathfrak{p}$ to a point in $\mathbb{P}^1\setminus\{0,1,\infty\}$, so the reduction of (a non-singular model of) Euler's curve (8) is non-singular (and so is the quadratic twist by γ). If $\mathfrak{p} \mid \alpha\gamma$ a similar result holds by Theorem 2.9 (recall that $N=qr$ or $2qr$).

The proof when $\mathfrak{p} \mid \beta$ depends on the theory of Mumford curves (as in Darmon's proof). Consider Euler's curve attached to $\mathfrak{h}_{4,s}^+$ at t_0, given with equation

$$\mathcal{C} : y^{qr} = x^A(1-x)^B(1-t_0x)^C t_0^{-sr},$$

for $A = q - sr$, $B = -q - sr$ and $C = q + rs$. Let $v = v_{\mathfrak{p}}(\beta)$ and write $t_0 = 1 + u_0$, so that $u_0 = \pi^{vp}\widetilde{u_0}$, for $\widetilde{u_0}$ a unit in $\mathcal{O}_{\mathfrak{p}}^{\times}$. Consider the curve (in the variable u) with equation

$$\mathcal{C} : y^{qr} = x^A(1-x)^B(1-x(u+1))^C t_0^{-sr}, \tag{25}$$

The stable model of its special fiber (see [11] and [42]) consists of two curves $\mathcal{C}_1$ and $\mathcal{C}_2$ intersecting at a point, given by the equations

$$\mathcal{C}_1 : y^{qr} = x^A(1-x)^{B+C} t_0^{-rs},$$

and

$$\mathcal{C}_2 : y_2^{qr} = x_2^B(x_2 - \widetilde{u_0})^C t_0^{-rs}.$$

The second curve is obtained via the change of variables $1 - x = \pi^{vp}x_2$ and $y_2 = y$ (noting that $B+C = 0$). Both curves have genus zero (since $B+C = 0$) and their intersection points are defined over the extension $K_{\mathfrak{p}}(\sqrt[qr]{t_0})$, an unramified extension of $K_{\mathfrak{p}}$, so the reduction type of $\mathrm{Jac}(\mathcal{C})$ is that of multiplicative reduction and $\mathcal{C}$ is a Mumford curve. The result follows from the fact that its p-torsion points are defined over the extension $K[\sqrt[p]{u_0}]$ (as in the proof of Proposition 1.15 in [16]). The proof for $\mathfrak{h}_{4,s}^-$ follows from a similar computation.

The proof for $\mathfrak{h}_{3,s}^{\pm}$ is similar, if $\mathfrak{p} \nmid \beta$, the motive has good reduction. When $\mathfrak{p} \mid \beta$, the semistable model of Euler's curve with parameters $(\frac{1}{q}, -\frac{1}{q}), (\frac{s}{q}, -\frac{s}{q})$ is the intersection of the two genus 0 curves

$$\mathcal{C}_1 : y^q = x^A(1-x)^{B+C} t_0^{-s},$$

and

$$\mathcal{C}_2 : y_2^q = x_2^B(x_2 - \widetilde{u_0})^C t_0^{-s}.$$

□

Remark 7. The motive attached to the parameters $(a/q, -a/q), (1,1)$ gives the same motive as the hyperelliptic curve $C_r^+(\alpha, \beta, \gamma)$ studied in [16], as proven in Corollary A.5.

5. Modularity

Let us denote by $\mathfrak{h}_1^+$ the hypergeometric motive attached to the parameters $(1,1), (1,1)$. It is not generic, corresponding to the Eisenstein series of weight 2 (see Proposition 6.3 of [29]). Theorem 2.10 implies the following "congruences" (up to Galois conjugation and quadratic twists)

$$\mathfrak{h}_1^+ \equiv \mathfrak{h}_2^+ \pmod{\mathfrak{r}}, \qquad \mathfrak{h}_1^+ \equiv \mathfrak{h}_3^+ \pmod{\mathfrak{q}}, \qquad \mathfrak{h}_{4,s}^+ \equiv \mathfrak{h}_2^+ \pmod{\mathfrak{q}},$$

for any prime ideal $\mathfrak{r} \mid r$ (respectively $\mathfrak{q} \mid q$). There is a subtlety here: the motive $\mathfrak{h}_1^+$ is defined over $\mathbb{Q}$, the motive $\mathfrak{h}_2^+$ is defined over $K = \mathbb{Q}(\zeta_r)^+$ and they become congruent while restricted to Gal_F, for $F = \mathbb{Q}(\zeta_r)$. Since the extension F/K is cyclic, the motive $\mathfrak{h}_2^+$ is isomorphic (up to a quadratic twist) to $\mathfrak{h}_1^+$ restricted to Gal_K. Since modularity is preserved under quadratic twists, by abuse of notation, we will "assume" that the congruences to hold over K (the same applies to the motives $\mathfrak{h}_i^-$).

Formula (15) gives the extra isomorphism

$$\mathfrak{h}_{4,s}^+ \equiv \mathcal{H}\left(\left(\frac{s}{q}, -\frac{s}{q}\right), (1,1) | t_0^{-1}\right) \pmod{r}. \tag{26}$$

Similar congruences hold for the family $\mathfrak{h}_i^-$. General modularity lifting theorems allow (with appropriate hypothesis) to propagate modularity from one motive to another. When the residual representations are irreducible, no hypothesis is needed, thanks to general results of Kisin ([35]). When the residual representation is reducible the theory is not complete and extra hypotheses appear (for example the main result of [48] requires the representations to be ordinary at the congruence prime). In [43] the author proves a stronger version for abelian totally real extensions $K/\mathbb{Q}$

(which is our case). However, there are still some technical hypothesis in his main result that we now recall. Let p be the residual characteristic, then the following must hold

(1) The prime p splits completely in K.
(2) The global representation is either ordinary at all primes of K dividing p (Corollary 6.6.11 of [43]) or
(3) The global representation is irreducible while restricted at the decomposition subgroup $D_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of K dividing p (Theorem 7.1.1 of loc. cit).

It is not clear how to verify whether our motives satisfy one of the last two conditions. A more general result (including mixed cases) would imply modularity of all our motives. Still, we can prove some partial results for our motives.

Lemma 5.1. *Let $p \geq 5$ be a prime number and let E be Legendre's elliptic curve (17) specialized at any rational point $t_0 \in \mathbb{Q} \setminus \{0, 1\}$. Then the residual representation $\overline{\rho_{E,p}}$ is irreducible.*

Proof. An elliptic curve whose residual Galois representation modulo p is reducible has an isogeny of degree p. Since the elliptic curve has full 2-torsion, the result follows from Mazur's work ([37]) when the curve is semistable. In general, a curve with full 2-torsion and a degree p isogeny gives a curve with an isogeny of degree $4p$, and there are no such rational elliptic curves when $p \geq 5$ by Kenku's result (see [33]). □

Lemma 5.2. *Let $p \geq 5$ be a prime number, and let $F = \mathbb{Q}(\zeta_p)$. Then the Galois representation of the residual representation of Legendre's elliptic curve E specialized at any rational point $t_0 \in \mathbb{Q} \setminus \{0, 1\}$ restricted to Gal_F is irreducible.*

Proof. The previous lemma implies that the residual representation $\overline{\rho_{E,p}}$ is irreducible. By [22, Lemma 1.13] the restriction to Gal_F is reducible if and only if the restriction to $\mathrm{Gal}_{\mathbb{Q}(\sqrt{p^\star})}$ is reducible, where $p^\star = \left(\frac{-1}{p}\right) p$. When the restriction is reducible, we are in what is usually called a *bad dihedral* prime. Let k be Serre's weight of the (irreducible) representation $\overline{\rho_{E,p}}$. If p does not divide the denominator of t_0, the curve E has either good or multiplicative reduction at p. When p does divide the denominator, the same is true for the quadratic ramified twist of E (twisting preserves irreducibility). So we can assume (up to a quadratic twist) that $k = 2$ or $k = p + 1$. On the other hand, by [22, Lemma 1.14] either $p = 2k - 3$ or $p = 2k - 1$. These conditions are not compatible when $p \geq 5$. □

Theorem 5.3. *If $r \mid \alpha\gamma$ then $\mathfrak{h}_2^+$ is modular.*

Proof. The result if proven in [16, Theorem 2.9]. Let $\mathfrak{r}$ be a prime ideal dividing r. As noticed in [16], the hypothesis $r \mid \alpha\gamma$ implies that the representation $\rho_{\mathfrak{r}}$ is ordinary at all primes dividing r, hence the result follows from [48]. □

Theorem 5.4. *If $r \geq 5$, the motive $\mathfrak{h}_2^-$ is modular.*

Proof. The proof follows the argument given in [16, Theorem 2.9]: let $\mathfrak{r}$ be a prime ideal of K dividing r. Let $\rho_{\mathfrak{r}}^-$ be the $\mathfrak{r}$-adic representation attached to $\mathfrak{h}_2^-$. Its residual representation is isomorphic to the residual representation attached to the motive $\mathfrak{h}_1^-$ restricted to Gal_K (corresponding to the elliptic curve E_{t_0} of (17)). By the Shimura-Taniyama conjecture (proved in [53] and [12]) E_{t_0} is modular, i.e. there exists a weight 2 modular form f_{t_0} for the group $\Gamma_0(N)$ (for an appropriate N) whose L-series matches that of E_{t_0}. Let F_{t_0} be the Hilbert modular form (of parallel weight 2) corresponding to the base change of f_{t_0} to K (whose existence is proven in [20]). Then the representation $\rho_{\mathfrak{r}}^-$ is congruent modulo $\mathfrak{r}$ to the Galois representation attached to F_{t_0}. By Lemma 5.2 the residual Galois representation $\overline{\rho_{E_{t_0},r}}$ restricted to Gal_K is absolutely irreducible, so by [35] $\mathfrak{h}_2^-$ is modular. □

Remark 8. In Darmon's article, there is an extra requirement (that $p \mid \alpha\beta$). This was a technical hypothesis that modularity lifting theorems had at the time (like ordinariness of the residual representation). These hypotheses have been removed since Darmon's article (see section §4 of [9]).

Theorem 5.5. *If $q \mid \gamma$ then the motive $\mathfrak{h}^+_{3,s}$ is modular for all s.*

Proof. Follows the same argument given in the proof of Theorem 5.3 (see [16, Theorem 2.9]). □

Theorem 5.6. *If $q \geq 5$, the motive $\mathfrak{h}^-_{3,s}$ is modular for all s.*

Proof. Follows the same argument of Theorem 5.4. See also [16, Theorem 2.9]. □

Theorem 5.7. *If $q \mid \alpha$ and $r \mid \gamma$ then $\mathfrak{h}^+_{4,s}$ is modular.*

Proof. Let $\mathfrak{q}$ be a prime ideal of K dividing q and let $\rho_{\mathfrak{q}}$ denote the $\mathfrak{q}$-th Galois representation attached to the motive $\mathfrak{h}^+_{4,s}$. The reduction of $\rho_{\mathfrak{q}}$ is isomorphic to the reduction of the $\mathfrak{q}$-th representation $\widetilde{\rho}_{\mathfrak{q}}$ of the motive $\mathfrak{h}^+_2$ restricted to Gal_K (there is an abuse of notation here, since the motive $\mathcal{H}^+_2$ is specialized at $t_0 = -\frac{A\alpha^q}{C\gamma^r}$). If $\overline{\rho_{\mathfrak{q}}}$ is reducible, then the hypothesis $q \mid \alpha$ implies that the reduction is ordinary at all prime ideals dividing q, hence by [48] the representation $\rho_{\mathfrak{q}}$ is modular.

Otherwise, $\overline{\rho_{\mathfrak{q}}}$ is absolutely irreducible and by [35] it is enough to prove that $\mathfrak{h}^+_2$ (specialized at $t_0 = -\frac{A\alpha^q}{C\gamma^r}$) is modular. Let $\mathfrak{r}$ be the prime ideal of $\mathbb{Q}(\zeta_r)^+$ dividing r. The reduction of $\widetilde{\rho}_{\mathfrak{r}}$ is reducible, hence modular when $r \mid \gamma$ by Theorem 5.3. □

Remark 9. In the previous result we do not expect the hypothesis $r \mid \gamma$ to be needed, as in general, the residual representation of $\widetilde{\rho}_{\mathfrak{r}}$ should be irreducible (if r is large enough).

Theorem 5.8. *If either $r \geq 5$ and $q \mid \alpha$ or $q \geq 5$ and $r \mid \gamma$ then $\mathfrak{h}^-_{4,s}$ is modular.*

Proof. Let $\mathfrak{q}$ be a prime ideal of K dividing q and let $\rho_{\mathfrak{q}}$ be the $\mathfrak{q}$-th Galois representation attached to $\mathfrak{h}^-_{4,s}$. If the residual representation $\overline{\rho_{\mathfrak{q}}}$ is reducible, then it is modular by [48] (because $q \mid \alpha$). Otherwise, it is congruent to $\mathfrak{h}^-_2$ restricted to Gal_K (specialized at $t_0 = -\frac{A\alpha^q}{C\gamma^r}$). The later motive is modular over $\mathbb{Q}(\zeta_r)^+$ by Theorem 5.4 and also over K by cyclic base change. Then $\mathfrak{h}^-_{4,s}$ is modular by [35]. The proof in the second case hypothesis follows from a similar argument using (26). □

Remark 10. As in the previous results, we do not expect the conditions $q \mid \alpha$ or $r \mid \gamma$ to be needed as long as the primes are large enough (so that the residual representations are absolutely irreducible).

6. Some special families

Let us consider the particular families $(2, p, r)$ and $(3, p, r)$. In these two cases we can prove modularity of the involved motives for r larger than an explicit small constant. The proof depends on the rational cases studied in section 3.

6.1. The family $(2, p, r)$.

We can assume that $r \geq 5$, since the case $(2, p, 3)$ has already been studied in the literature. Let $\mathcal{H}^+_2 := \mathcal{H}((\frac{1}{r}, -\frac{1}{r}), (\frac{1}{2}, \frac{1}{2})|t)$, a motive defined over the totally real field $K := \mathbb{Q}(\zeta_r)^+$. Its monodromy matrices have order $\{r, \infty, 2\}$ at $\{0, 1, \infty\}$ respectively.

Theorem 6.1. *The motive $\mathcal{H}^+_2(t)$ is modular for all specialization of the parameter t.*

Proof. The motive $\mathcal{H}^+_2(t)$ is congruent modulo $\mathfrak{r}$ (the unique prime ideal of K dividing r) to the motive $\mathcal{H}^-_2$ (specialized at t^{-1} by (15)) corresponding (as mentioned before) to Legendre's elliptic curve (17). By Lemma 5.2 its residual image restricted to Gal_K is absolutely irreducible modulo r for all primes $r \geq 5$. The result then follows from [35] (since E_t is modular). □

To a putative solution (α, β, γ) of the equation

$$Ax^2 + By^p + Cz^r = 0,$$

one can also attach the hypergeometric motive $\mathcal{H}_2^- := \mathcal{H}\left(\left(\frac{1}{r}, -\frac{1}{r}\right), \left(\frac{1}{4}, -\frac{1}{4}\right) | t\right)$. As before, let $\mathfrak{h}_2^-$ denote the specialization of $\mathcal{H}_2^-$ at $t_0 := -\frac{A\alpha^2}{C\gamma^r}$, twisted by the character θ_α. If $\mathfrak{p}$ denotes a prime ideal of $K = \mathbb{Q}(\zeta_r)^+$ dividing p, then the $\mathfrak{p}$-th residual representation attached to $\mathfrak{h}_2^-$ is unramified outside $2r$.

Theorem 6.2. *Suppose that $r \nmid A$. If $r \geq 11$ or if $r = 7$ and $2 \mid v_7(B)$, the motive $\mathfrak{h}_2^-$ is modular.*

Proof. Let $\mathfrak{r}$ denote the prime ideal of K dividing r. The $\mathfrak{r}$-th Galois representation attached to $\mathfrak{h}_2^-$ is congruent to the quadratic twist by θ_α of the motive $\mathcal{H}((\frac{1}{4}, -\frac{1}{4}), (1, 1)|t_0^{-1})$ of §3.3. It corresponds to the elliptic curve

$$E_t : y^2 + xy = x^3 + \frac{t}{64}x.$$

The curve E_t has a rational 2-torsion point, hence Kenku's result ([33]) implies that the residual image of E_t is absolutely irreducible for all primes $r > 7$ (for all specializations of the parameter). The case $r = 7$ is also irreducible, since the curve $X_0(14)$ has only two points corresponding to the j-invariants -3375 and 16581375. They correspond to the values $t_0 = \frac{64}{63}$ and $t_0 = -\frac{1}{63}$, but note that $63 = 9 \cdot 7$, which is not a square if $v_7(AB) = v_7(B)$ is even, hence it does not come from any solution of the equation $Ax^2 + By^p + Cz^r = 0$ with $r \geq 2$. Irreducibility of the residual representation restricted to Gal_K follows from the same argument used in Lemma 5.2: the curve has additive or multiplicative reduction at r. The reduction of $E_{t_0^{-1}}$ at a prime $r > 3$ is either good (if $v_r(t_0^{-1}(t_0^{-1} - 1)) = 0$ by (20)) or multiplicative when $v_r(t_0^{-1}(t_0^{-1} - 1)) > 0$. When $v_r(t_0) > 0$, since $t_0^{-1} = -\frac{C\gamma^r}{A\alpha^2}$ and $r \nmid A$, the motive $\mathfrak{h}_2^-$ has good reduction at r by Theorem 2.9. □

Remark 11. It seems plausible that the residual image modulo 5 at points coming from solutions is also irreducible, but we did not study this problem in detail (this is just a speculation based on some numerical experiments). Although this second motive could be used to run a multi-Frey approach, the problem is that the conductor exponent at 2 is larger than the previous one.

6.2. **The family $(3, p, r)$.** Assume that $r \geq 5$, since the case $(3, 3, r)$ has already been studied in the literature. Let $\mathcal{H}_4^+ := \mathcal{H}((\frac{1}{r}, -\frac{1}{r}), (\frac{1}{3}, -\frac{1}{3})|t)$, an hypergeometric motive also defined over $K := \mathbb{Q}(\zeta_r)^+$. Its monodromy matrices at the points $\{0, 1, \infty\}$ have order $\{3, \infty, r\}$ respectively. Let (α, β, γ) be a solution to

$$Ax^3 + By^p + Cz^r = 0,$$

and set $t_0 := -\frac{A\alpha^3}{C\gamma^r}$.

Theorem 6.3. *If $r \nmid A$, the motive $\mathcal{H}_4^+(t_0)$ is modular.*

Proof. Let $\mathfrak{r}$ be a prime ideal of K dividing r. The motive $\mathcal{H}_4^+(t_0)$ is congruent modulo $\mathfrak{r}$ to the hypergeometric motive $\mathcal{H}((\frac{1}{3}, -\frac{1}{3}), (1, 1)|t_0^{-1})$ corresponding (as described in §3.2) to the elliptic curve with equation

$$E_t : y^2 + xy + \frac{t_0}{27}y = x^3. \tag{27}$$

The point $P = (0, 0)$ belongs to E and has order 3. By Kenku's result [33] (based in Mazur's result [37]) there are no rational elliptic curves with a cyclic isogeny of order $3p$ for $p \geq 11$. Furthermore, there are finitely many curves (up to quadratic twists) with an isogeny of order 15 and 21 (see [10] page 79 and Table 4).

Any curve with an isogeny of order 15 has the same j-invariant as a curve in the isogeny graph of curves of level $50.b$ (with LMFDB label 50.b1, 50.b2, 50.b3 and 50.b4), while any curve with an

isogeny of order 21 has the same j-invariant as a curve in the isogeny graph 162b, with LMFDB labels 162.b1, 162.b2, 162.b3 and 162.b4. It is easy to verify that $j(E_t)$ does not match any of these 8 values for any rational value of t. In particular, the curve E_t has absolutely irreducible residual image for $q \geq 5$. Its restriction to Gal_K is also absolutely irreducible (by the same argument given in Lemma 5.2 and Theorem 6.2 under the assumption $r \nmid A$). The result then follows from [35]. □

Remark 12. One can obtain a bound for the conductor exponent of $\mathcal{H}_3^+(t)$ at primes dividing 3 by studying the conductor exponent of the curve (27) as done in Lemma 3.1 for the prime 2.

A similar result holds for the motive $\mathcal{H}_4^-(t)$ corresponding to the parameters $\left(\frac{1}{r}, -\frac{1}{r}\right), \left(\frac{1}{6}, -\frac{1}{6}\right)$ (this is a quadratic twist of the motive $\mathcal{H}\left(\left(\frac{1}{2r}, -\frac{1}{2r}\right), \left(\frac{1}{3}, -\frac{1}{3}\right)|t\right)$ as explained in §2.6).

Theorem 6.4. *Suppose that $r \nmid A$. Then if $r \geq 11$ the motive $\mathcal{H}_4^-(t_0)$ is modular.*

Proof. Let $\mathfrak{r}$ be a prime ideal of K dividing r. Then for any specialization of the parameter, the motive $\mathcal{H}_4^-(t)$ is congruent modulo $\mathfrak{r}$ to the restriction to Gal_K of motive $\mathcal{H}\left(\left(\frac{1}{6}, -\frac{1}{6}\right), (1,1)|t\right)$. As studied in §3, the later corresponds to the elliptic curve

$$E_t : y^2 + xy = x^3 - \frac{t}{432}.$$

The curve E_t does not have any torsion point, hence proving that its residual image modulo r is irreducible seems more challenging. By Mazur's result on isogenies of prime degrees ([37]) this is the case if r does not belong to the set $\{5, 7, 11, 17, 19, 37, 43, 67, 163\}$. The result holds when $r \geq 11$ because for each of these values there are finitely many j-invariants of elliptic curves with reducible image modulo r (see for example [10]), namely:

- Any elliptic curve with a rational 11-isogeny either has CM, or is a quadratic twist of one of the curves 121.a1, 121.a2 or 121.b1, i.e. its j-invariant equals -121, -32768 or -24729001. Only the first j-invariant corresponds to the values $t_0 = \frac{27}{11}$ or $t_0 = \frac{-16}{11}$, whose denominator is a prime number (so does not come from a solution).
- Any elliptic curve with a rational 17-isogeny is a quadratic twist of either the curve 14450.b1 or 14450.b2 (using the LMFDB label), with j-invariants $-\frac{882216989}{131072}$ and $-\frac{297756989}{2}$. None of them are j-invariants of E_t for a rational value of t.
- Any rational curves having a rational 19, 37, 43, 67 or 163 isogeny has CM. Then its j-invariant must be (respectively) -884736, -12288000, -884736000, -147197952000 and -262537412640768000. None of them belong to the family E_t.

Then modularity follows from Kisin's result. □

We do not know whether the last large image result holds for $r = 5$ or $r = 7$ (but it is an interesting problem to study).

7. Bounds at wilds primes

As mentioned in the introduction, it seems like a very hard problem to determine the conductor exponents of an hypergeometric motive at a wild prime $\mathfrak{p}$ dividing a rational prime p. However we can give an explicit bound under the following assumption:

Assumption 1. *The parameters $(a, b), (c, d)$ are generic and satisfy the following properties:*

- *$a + b$ and $c + d$ are integers,*
- *if p is a prime dividing N, then either $v_p(a) = v_p(b) = -1$ and $v_p(c) = v_p(d) = 0$ or vice-versa.*

Sometimes we will impose an extra hypothesis on the specialization t_0 in order to lower the number of cases to consider, but the same approach applies to the general case.

Recall that if $\rho : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{K_\lambda})$ is a Galois representation and $\mathfrak{q}$ is a prime ideal whose residual characteristic is prime to that of λ, then the $\mathfrak{q}$-th valuation of the Artin conductor of ρ at $\mathfrak{q}$ is computed by

$$\mathfrak{n}_\mathfrak{q}(\rho) = \mathfrak{n}_{\mathfrak{q},tame}(\rho) + \mathfrak{n}_{\mathfrak{q},wild}(\rho),$$

where $\mathfrak{n}_{\mathfrak{q},tame}(\rho)$ is the codimension of the subspace fixed by the inertia group $I_\mathfrak{q}$ while $\mathfrak{n}_{\mathfrak{q},wild}(\rho)$, the *Swan* conductor, is the sum of the codimensions over higher ramification groups.

Our bound depends on the fact that two $\mathfrak{q}$-adic Galois representations which are residually isomorphic have the same Swan conductor at any prime ideal $\mathfrak{p}$ not dividing $\mathcal{N}\mathfrak{q}$ (the norm of $\mathfrak{q}$).

Lemma 7.1. *Under Assumption 1, if $\mathfrak{q}$ is a prime ideal of K dividing N with residual characteristic q and $t_0 \in \mathbb{Q}$ then there exists $s \in \mathbb{F}_q^\times$ such that*

$$\mathfrak{n}_{\mathfrak{q},wild}(\mathcal{H}((a,b),(c,d)|t_0)) = \begin{cases} \mathfrak{n}_{\mathfrak{q},wild}\left(\mathcal{H}\left(\left(\frac{s}{q},-\frac{s}{q}\right),(1,1)\,|t_0\right)\right) & \text{if } v_q(a) = -1, \\ \mathfrak{n}_{\mathfrak{q},wild}\left(\mathcal{H}\left(\left(\frac{s}{q},-\frac{s}{q}\right),(1,1)\,|\frac{1}{t_0}\right)\right) & \text{if } v_q(c) = -1. \end{cases}$$

Proof. The isomorphism (15) implies that the second case follows from the first one. Since $a+b$ and $c+d$ are integers we can assume that $b=-a$ and $d=-c$.

Let p be a rational prime different from q such that $v_p(a) = -1$. Then we can write $a = \frac{r}{p} + \frac{\alpha}{\beta}$ with $v_p(\beta) = 0$ and $v_q(\beta) = 1$. Let $\mathfrak{p}$ be a prime ideal of K dividing p. By Theorem 2.10, we have a congruence between $\mathcal{H}((a,b),(c,d)|t_0)$ and $\mathcal{H}((\frac{\alpha}{\beta},-\frac{\alpha}{\beta}),(c,d)|t_0)$ over $K(\zeta_p)$ modulo a prime ideal of $K(\zeta_p)$ dividing $\mathfrak{p}$, so both motives have the same Swan conductor at $\mathfrak{q}$. Since the extension $K(\zeta_p)/K$ is unramified at $\mathfrak{q}$, they both have the same Swan conductor over K. Applying the same procedure for each rational prime dividing β different from q it follows that

$$\mathfrak{n}_{\mathfrak{q},wild}(\mathcal{H}((a,b),(c,d)|t_0)) = \mathfrak{n}_{\mathfrak{q},wild}\left(\mathcal{H}\left(\left(\frac{s}{q},-\frac{s}{q}\right),(c,d)|t_0\right)\right).$$

Since the denominator of c is prime to q, a similar argument proves the result. □

Remark 13. By (16), the motives $\mathcal{H}\left(\left(\frac{1}{q},-\frac{1}{q}\right),(1,1)|t_0\right)$ and $\mathcal{H}\left(\left(\frac{s}{q},-\frac{s}{q}\right),(1,1)|t_0\right)$ are Galois conjugate and both appear in the same superelliptic curve (which is defined over $\mathbb{Q}$), so their conductor exponent at a prime ideal $\mathfrak{p}$ are the same.

The lemma implies that under Assumption 1, the Swan conductor of our motive is the same as the Swan conductor of the motive $\mathcal{H}\left(\left(\frac{1}{q},-\frac{1}{q}\right),(1,1)|t_0\right)$ (or its specialization at t_0^{-1}), which appears in the Jacobian of an hyperelliptic curve (as proved in Appendix A), so one can use the theory of cluster pictures to compute its Swan conductor at odd primes (as done in [27]).

Computing the local type of an hyperelliptic curve at 2 is also quite challenging, but for $q=2$ the motive is actually an elliptic curve whose conductor was computed in Lemma 3.1. This approach allows us to give upper bounds for the conductor exponents at odd wild primes for the motives $\mathfrak{h}_2^\pm$ and $\mathfrak{h}_4^\pm$ and at primes dividing 2 for all motives $\mathfrak{h}_i^-$.

A prime ideal $\mathfrak{q}$ is called *wild* if $\mathfrak{n}_{\mathfrak{q},wild}(\rho) \neq 0$. In the case of 2-dimensional representations we have that

$$\mathfrak{n}_{\mathfrak{q},tame}(\rho) \in \begin{cases} \{1,2\} & \text{if } \mathfrak{q} \text{ is wild,} \\ \{0,1,2\} & \text{otherwise.} \end{cases} \tag{28}$$

The wild primes of an hypergeometric motive always divides N.

Remark 14. If $\mathfrak{q}$ is an odd prime (i.e. $\mathfrak{q} \nmid 2$) then the Swan conductor of ρ at $\mathfrak{q}$ is invariant under quadratic twists. This fact plays a crucial role in our computations.

7.1. **Primes dividing 2.** Let $\mathfrak{q}$ be a prime ideal of K dividing 2.

Theorem 7.2. *Let $(a,b),(c,d)$ be parameters satisfying Assumption 1, with $v_2(a)=-1$. Let s be the valuation at $\mathfrak{q}$ of the conductor of $\mathcal{H}((a,b),(c,d)|t_0)$. Then:*

- *If $v_2(t_0)\geq 0$,*

$$s=\begin{cases}5 & \text{if } t_0\equiv 3 \pmod 4,\\ 4 & \text{if } t_0\equiv 1 \pmod 4,\\ 0,1,2 & \text{if } v_2(t_0)\geq 5.\end{cases}$$

- *If $v_2(t_0)<0$,*

$$s=\begin{cases}6 & \text{if } 2\nmid v_2(t_0),\\ 4 & \text{if } 2\mid v_2(t_0) \text{ and } t_0/2^{v_2(t_0)}\equiv 3 \pmod 4,\\ 0,1,2 & \text{if } 2\mid v_2(t_0)<-4 \text{ and } t_0/2^{v_2(t_0)}\equiv 1 \pmod 4.\end{cases}$$

Proof. By the proof of Lemma 7.1, our motive is related under a finite number of congruences (modulo odd prime ideals) and base extensions (unramified at 2) to the motive $\mathcal{H}((\frac{1}{2},\frac{1}{2})(1,1)|t_0)$.

Let k be the conductor exponent at 2 of E_{t_0} given in Lemma 3.1. If $t_0\equiv 3 \pmod 4$, then $k=5$. Looking at Table 1 of [19] we see that the Weil-Deligne type of E_{t_0} is supercuspidal, and the extension where the curve attains good reduction has ramification degree 8. Equivalently, our local type corresponds to the induction from $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$ of a character of conductor $\sqrt{-1}^3$ and order 4 (see [38, Corollary 4.1] and [21, Theorem 2.10]). In particular, the Swan part is 3 and its tame part 2. By Lemma 7.1 the Swan conductor of $\mathcal{H}((a,b),(c,d)|t_0)$ is also 3. More can be said on the tame conductor: since all congruences involve odd primes, and our base extensions are unramified at 2, the local type of the residual representations involved in the congruences is also supercuspidal, hence their residual tame conductor is 2, so $s=5$ as claimed. The other cases follow from a similar argument, via the following observations:

- If $k=4$, it follows from Table 1 of [19] that the Weil-Deligne type of E_{t_0} is either:
  (1) A twist (by the quadratic character ε_{-1} corresponding to $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$) of the Steinberg representation.
  (2) A principal series, twist by ε_{-1} of an unramified representation.
  (3) Supercuspidal, induced from the unramified extension $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ of a character of conductor 2^2 and order 6 (which is the same as taking the twist by ε_{-1} of the induction of the character of order 3 and conductor 2 as described in Table 1 of [19]).
  (4) Exceptional supercuspidal representation, twist by ε_{-1} of the exceptional supercuspidal of conductor 2^3.
  In all cases, the residual tame conductor exponent is 2, hence $\mathcal{H}((a,b),(c,d)|t_0)$ has the same conductor at $\mathfrak{q}$ as E_{t_0}.
- If $k=1$, the Swan conductor is 0, hence $\mathcal{H}((a,b),(c,d)|t_0)$ has conductor exponent $s=0,1,2$ at $\mathfrak{q}$.
- If $k=6$, the Weil-Deligne type of E_{t_0} is either:
  (1) A quadratic twist by $\varepsilon_{\pm 2}$ (the character attached to the extension $\mathbb{Q}_2(\sqrt{\pm 2})/\mathbb{Q}_2$) of a Steinberg representation.
  (2) A principal series, twist by $\varepsilon_{\pm 2}$ of an unramified one.
  (3) Supercuspidal, induced from either: a character of $\mathbb{Q}_2(\sqrt{5})$ of conductor 2^3 and order 6, a character of $\mathbb{Q}_2(\sqrt{-1})$ or $\mathbb{Q}_2(\sqrt{-5})$ of conductor 2^2 (of valuation 4) and order 4.
  (4) Exceptional supercuspidal.
  In all cases, the residual tame conductor exponent is 2.

□

Corollary 7.3. *Let $\mathfrak{q}$ be a prime ideal of K dividing 2 and suppose $2 \nmid AC$. Then, for $p, q, r \geq 5$, $\mathfrak{n}_{\mathfrak{q}}(\mathfrak{h}_i^-) \leq 6$ for all i.*

Proof. Recall that $t_0 = -\frac{A\alpha^q}{C\gamma^r}$. The assumption $2 \nmid AC$ implies that either $v_2(t_0) = 0$, $v_2(t_0) \geq 5$ or $v_2(t_0) < -4$. In all cases, the last theorem implies that the conductor exponent of the motive $\mathcal{H}((a,b),(c,d)|t_0)$ is at most 6. The quadratic character θ_γ has conductor valuation at most 3 at 2, hence the quadratic twist $\mathfrak{h}_i^-$ also has conductor exponent at most 6 at $\mathfrak{q}$. □

7.2. **Odd primes.** Let $\mathfrak{q}$ be an odd prime of K dividing N of residual characteristic q.

Theorem 7.4. *Let $(a,b),(c,d)$ be parameters satisfying Assumption 1. Let s be its conductor exponent at $\mathfrak{q}$. Then*

$$s \leq \begin{cases} \frac{q+5}{2} & \text{if } v_{\mathfrak{q}}(t_0(t_0-1)) = 1, \\ q+2 & \text{if } q \nmid v_q(t_0) < 0, \\ 3 & \text{otherwise.} \end{cases}$$

Proof. Recall that if $\mathcal{C}$ is Euler's curve attached to the parameters $(a,b),(c,d)$, then the motive $\mathcal{H}((a,b),(c,d)|t_0)$ is defined by $\mathcal{M}_{\mathcal{C}} \otimes \mathbf{J}((-a,-b,c,d),(c-b,d-a))^{-1}(-1)^{d-b}$. When $a+b$ and $c+d$ are integers, the Jacobi motive is at most a Tate twist (hence it does not affect the action of inertia groups). Under Assumption 1, Lemma 2.5 implies that the character $(-1)^{d-b}$ is unramified outside 2, so the conductor of the motive matches the conductor of (a 2-dimensional part of) Euler's curve.

By Lemma 7.1 it is enough to understand the Swan conductor of $\mathcal{H}\left(\left(\frac{1}{q}, -\frac{1}{q}\right), (1,1)|t_0^{\pm 1}\right)$, whose Euler's curve is isomorphic (by Theorem A.5) to an hyperelliptic curve. Its Swan conductor is given in [27] (see formula (36)): it is either equal to 0, or it equals 1 when $v_{\mathfrak{q}}(t_0(t_0-1)) \in \{0, 2\}$, $\frac{q+1}{2}$ if $v_{\mathfrak{q}}(t_0(t_0-1)) = 1$ and q if $v_q(t_0) < 0$ and $q \nmid v_q(t_0)$. □

Corollary 7.5. *Let $\mathfrak{q}$ be an odd prime dividing N with residual characteristic q. Let s_i be the conductor exponent of the motive $\mathfrak{h}_i^{\pm}$, for $i = 2, 4$. Then*

$$s_i \leq \begin{cases} 3 & \text{if } \mathfrak{q} \nmid ABC, \\ q+2 & \text{otherwise.} \end{cases}$$

8. Eliminating modular forms using HGMs

Let us focus in the case of general exponents (q,p,r). Suppose that the first three steps of the modular method succeed, so we have attached to a putative primitive solution (α,β,γ) of equation (1) a Hilbert newform $g \in S_2(\Gamma_0(\mathfrak{n}))$ over a totally real base field K (contained in $\mathbb{Q}(\zeta_N)$), where the level $\mathfrak{n}$ is only divisible by primes dividing $ABCpq$. The form g satisfies that it is congruent modulo $\mathfrak{p}$ (a prime ideal of K dividing the exponent p) to $\mathcal{H}((a,b),(c,d)|t_0)$ while restricted to F.

After computing the space $S_2(\Gamma_0(\mathfrak{n}))$ and its newforms, we aim to discard newforms not related to the solution (α,β,γ) (at least for large values of the prime r). If we can discard them all then no solution can exist.

Let us explain an algorithm based on an idea of Mazur, which in practice allows to discard most newforms when the exponent p is larger than a computable constant. Keeping the previous notation, let N be the least common multiple of the denominators of a,b,c,d and let $F = \mathbb{Q}(\zeta_N)$. Let g be any newform in $S_2(\Gamma_0(\mathfrak{n}))$, and denote by the same letter its base change to F. For $\mathfrak{l}$ a prime ideal of F, denote by $a_{\mathfrak{l}}(g)$ the $\mathfrak{l}$-th Fourier coefficient of g.

The algorithm consists on studying solutions to (1) modulo ℓ (for ℓ a rational prime not dividing $ABCpqr$), in order to get information on the Fourier coefficient $a_{\mathfrak{l}}(F)$ for primes $\mathfrak{l}$ of F dividing ℓ. More concretely, let

$$S_\ell = \{(\tilde{\alpha},\tilde{\beta},\tilde{\gamma}) \in \mathbb{F}_\ell^3 \setminus \{(0,0,0)\} \ : \ A\tilde{\alpha}^q + B\tilde{\beta}^p + C\tilde{\gamma}^r = 0\}.$$

Then any primitive solution (α, β, γ) of (1) reduces modulo ℓ to an element in S_ℓ. In practice, since the prime p is going to be larger than ℓ, raising to the p-th power is a bijection of $\mathbb{F}_\ell$, so we can parametrize S_ℓ by elements $(\tilde{\alpha}, \tilde{\gamma}) \in \mathbb{F}_\ell^2 \setminus \{(0,0)\}$, which determine $\tilde{\beta}$ uniquely. Denote by $S_\ell^\times$ the subset of S_ℓ made of elements where none of their entries are zero. Consider the following three distinct cases:

(1) The value $\tilde{\alpha}\tilde{\beta}\tilde{\gamma} \neq 0$ (i.e. $(\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}) \in S_\ell^\times$).
(2) Either $\tilde{\alpha} = 0$ or $\tilde{\gamma} = 0$, but $\tilde{\beta} \neq 0$.
(3) The number $\tilde{\beta}$ equals 0.

In the first case, we set $t_0 = -\frac{A\tilde{\alpha}^q}{C\tilde{\gamma}^r}$, and compute the value $H_{\mathfrak{l}}((a,b),(c,d)|t_0)$ (using Definition 2.8), whose value depends only t_0 modulo $\mathfrak{l}$. By part (2) of Theorem 2.9 the following congruence holds

$$a_{\mathfrak{l}}(F) \equiv H_{\mathfrak{l}}((a,b),(c,d)|t_0) \pmod{\mathfrak{p}}, \tag{29}$$

where $\mathfrak{p}$ is a prime ideal dividing p in the composition of the coefficient field of g and F.

Assumption 1: Suppose that both sides of (29) are different for all values t_0 obtained from elements of $S_\ell^\times$.

Then for each element t_0, the difference between the left and the right hand side of (29) is non-zero and p must divide (the norm) of their difference. This gives for each value of t_0 a finite list of possibilities for p, so we can take their union and get a bound for p in case (1).

Suppose then that we are in case (2) with $\tilde{\alpha} = 0$ (so $\ell \mid \alpha$). Since $\ell \nmid A$, $v_\ell(A\alpha^q)$ is divisible by q. The condition $\ell \nmid ABCpqr$ implies that ℓ is not a wild prime so part (3) of Theorem 2.9 implies that the image of inertia at $\mathfrak{l}$ is trivial (i.e. $\mathcal{H}((a,b),(c,d)|t_0)$ is unramified at $\mathfrak{l}$). Write the parameter t_0 in the form $t_0 = \ell^{qv_\ell(\alpha)}\tilde{t_0}$, where $\ell \nmid \tilde{t_0}$. Then, by [29, Theorem A.1], the trace of $\mathrm{Frob}_{\mathfrak{l}}$ for $\mathcal{H}((a,b),(c,d)|t_0)$ equals

$$-\chi_{\mathfrak{l}}(-1)^{(d-b)(\mathcal{N}(\mathfrak{l})-1)}\mathbf{J}((-a,-b,c,d),(c-b,d-a))(\mathfrak{l})^{-1}\cdot \tag{30}$$
$$\cdot\left(\chi_{\mathfrak{l}}(\tilde{t_0})^{dN}J(\chi_{\mathfrak{l}}(\tilde{t_0})^{(d-b)N},\chi_{\mathfrak{l}}(\tilde{t_0})^{(b-c)N}) + \chi_{\mathfrak{l}}(\tilde{t_0})(-1)^{(b-c)N}\chi_{\mathfrak{l}}(\tilde{t_0})^{cN}J(\chi_{\mathfrak{l}}(\tilde{t_0})^{(d-c)N},\chi_{\mathfrak{l}}(\tilde{t_0})^{(a-d)N})\right),$$

where $J(\psi,\chi)$ is the usual Jacobi sum.

Assumption 2: Suppose that $a_{\mathfrak{l}}(g)$ does not match (30) for any value $\widetilde{t_0} \in \mathbb{F}_\ell^\times$.

Then once again, for each t_0 of type (2) the difference between (30) and $a_{\mathfrak{l}}(g)$ is non-zero and p must divide its norm.

When $\tilde{\gamma} = 0$ the strategy follows analogously: replacing (using [29, Theorem A.2]) (30) by

$$-\chi_{\mathfrak{l}}(-1)^{(d-b)(\mathcal{N}(\mathfrak{l})-1)}\mathbf{J}((-a,-b,c,d),(c-b,d-a))(\mathfrak{l})^{-1}\cdot \tag{31}$$
$$\cdot\left(\chi_{\mathfrak{l}}(\tilde{t_0})^{bN}J(\chi_{\mathfrak{l}}(\tilde{t_0})^{(d-b)N},\chi_{\mathfrak{l}}(\tilde{t_0})^{(a-d)N}) + \chi_{\mathfrak{l}}(\tilde{t_0})(-1)^{(a-d)N}\chi_{\mathfrak{l}}(\tilde{t_0})^{aN}J(\chi_{\mathfrak{l}}(\tilde{t_0})^{(a-b)N},\chi_{\mathfrak{l}}(\tilde{t_0})^{(b-c)N})\right).$$

Case (3) (when $\mathfrak{l} \mid \beta$) lies in the so called "lowering the level" situation: by construction the hypergeometric motive has multiplicative reduction at primes dividing β (which do not divide B), but $\mathfrak{l}$ does not divide $\mathfrak{n}$. Then the well known lowering the level condition must hold, namely

$$a_{\mathfrak{l}}(g) \equiv \pm(\mathcal{N}(\mathfrak{l}) + 1) \pmod{\mathfrak{p}}. \tag{32}$$

Note that $a_{\mathfrak{l}}(g)$ cannot be equal to $\pm(\mathcal{N}(\mathfrak{l}) + 1)$ for ℓ large enough (as it contradicts Weil's bound on the number of points of a curve over a finite field), so there are finitely many possibilities for p.

In each case both sides of the expected congruence can be computed. If the values happen to be different (i.e. Assumption 1, Assumption 2 and the analogous assumption for $\tilde{\gamma} = 0$ are true), we get a finite list of candidates for the prime p dividing the norm of their difference. In practice, one varies ℓ over a small set of primes and take the greatest common divisor of the different bounds

to reduce the possible values of p. This method is very powerful, and succeeds to discard most newforms of $S_2(\Gamma_0(\mathfrak{n}))$. Sometimes it is the case that no newforms (except for example some with complex multiplication) pass the test, proving non-existence of solutions to (1) for all primes p but a few small ones. However in many instances, there are a few newforms which systematically pass the test and other ideas are needed to discard them.

Appendix A. Motives coming from hyperelliptic curves

by Ariel Pacetti and Fernando Rodriguez-Villegas

The results of the present appendix follow the ideas of [50]. Let $N > 1$ be an odd positive integer, ζ_N an N-th primitive root of unity and $F = \mathbb{Q}(\zeta_N)$ the cyclotomic field. For $a \in \mathbb{Q}$, $a \neq \pm 2$, define the hyperelliptic curve

$$\mathcal{C}'_N : y^2 = x^{2N} + ax^N + 1. \tag{33}$$

The curve $\mathcal{C}'_N$ has two involutions, the canonical one $\tau : \mathcal{C}'_N \to \mathcal{C}'_N$ given by $\tau(x, y) = (x, -y)$ and a second involution $\iota_N : \mathcal{C}'_N \to \mathcal{C}'_N$ given by $\iota_N(x, y) = \left(\frac{1}{x}, \frac{y}{x^N}\right)$. A simple computation proves that both involutions commute, so the group $\mathbb{Z}/2 \times \mathbb{Z}/2$ is a subgroup of the automorphisms of $\mathcal{C}'_N$.

Let $g(x)$ denote the monic polynomial whose zeros are all the numbers $\xi + \xi^{-1}$, for $\xi \in \overline{\mathbb{Q}} \setminus \{-1\}$ satisfying $\xi^N = -1$ (which matches the minimal polynomial of $-(\zeta_N + \zeta_N^{-1})$ when N is odd). Let $\mathcal{D}_N$ denote the hyperelliptic curve

$$\mathcal{D}_N : y^2 = (x + 2)(xg(x^2 - 2) + a). \tag{34}$$

Lemma A.1. *The quotient of $\mathcal{C}'_N$ by the involution ι_N is isomorphic to $\mathcal{D}_N$.*

Proof. See Proposition 3 of [50]. The idea is that $\xi = x + \frac{1}{x}$ and $\eta = \frac{y(1+1/x)}{x^{(N-1)/2}}$ generate the field of functions fixed by the involution, and the given equation is the relation they both satisfy (setting $y = \eta$ and $x = \xi$). □

Lemma A.2. *The quotient of $\mathcal{C}'_N$ by the involution $\iota \circ \tau$ is given by the equation*

$$\mathcal{D}'_N : y^2 = (x - 2)(xg(x^2 - 2) + a). \tag{35}$$

Proof. Mimics the previous one, noting that the field of invariant functions is now generated by the functions $\xi = x + \frac{1}{x}$ and $\eta = \frac{y(1-1/x)}{x^{(N-1)/2}}$. The two variables satisfy the stated relation (setting $y = \eta$ and $x = \xi$). □

Since the quotient of $\mathcal{C}'_N$ by $\langle \tau, \iota_N \rangle$ has genus 0, up to isogeny

$$\mathrm{Jac}(\mathcal{C}'_N) \sim \mathrm{Jac}(\mathcal{D}_N) \times \mathrm{Jac}(\mathcal{D}'_N).$$

If $d \mid N$, there is a natural map $\pi_d : \mathcal{C}'_N \to \mathcal{C}'_d$ sending $(x, y) \to (x^{N/d}, y)$. It is easy to verify that the following diagram is commutative

$$\begin{array}{ccc} \mathcal{C}'_N & \xrightarrow{\iota_N} & \mathcal{C}'_N \\ {\scriptstyle \pi_d}\downarrow & & \downarrow{\scriptstyle \pi_d} \\ \mathcal{C}'_d & \xrightarrow{\iota_d} & \mathcal{C}'_d \end{array}$$

so the map π_d also induces a map $\pi_d : \mathcal{D}_N \to \mathcal{D}_d$. The pullback under π_d of the Jacobian of $\mathcal{D}_d$ is a subvariety of $\mathrm{Jac}(\mathcal{D}_N)$ (belonging to its *old* part). Define the *new* part of $\mathrm{Jac}(\mathcal{D}_N)$ to be a complement to the contribution from all of its old parts. Clearly

$$\mathrm{Jac}(\mathcal{C}'_N)^{\mathrm{new}} \sim \mathrm{Jac}(\mathcal{D}_N)^{\mathrm{new}} \times \mathrm{Jac}(\mathcal{D}'_N)^{\mathrm{new}}.$$

Lemma A.3. *The dimension of $\mathrm{Jac}(\mathcal{D}_N)^{new}$ equals $\frac{\phi(N)}{2}$.*

Proof. The polynomial $g(x)$ has degree $\frac{N-1}{2}$, so the right hand side of (34) has degree $N+1$ and the genus of $\mathcal{D}_N$ equals $\frac{N-1}{2}$. If N is a prime number, then the result follows. Otherwise, by an inductive argument, we can assume that the result holds for all divisors of N, hence

$$\frac{N-1}{2} = g(\mathcal{D}_N) = \dim(\mathrm{Jac}(\mathcal{D}_N)^{\mathrm{new}}) + \sum_{\substack{d|N \\ 1<d<N}} \frac{\phi(d)}{2},$$

and the result follows from Möbius inversion formula. □

An analogue result holds for $\mathrm{Jac}(\mathcal{D}'_N)^{\mathrm{new}}$. The group μ_N of N-th roots of unity acts on the curve $\mathcal{C}'_N$ via $\zeta_N \cdot (x,y) = (\zeta_N x, y)$ (this endomorphism is defined over F). The action does not commute with ι_N, but satisfies the relation

$$\zeta_N \circ \iota = \iota \circ \zeta_N^{-1}.$$

Then over $K = \mathbb{Q}(\zeta_N)^+$, the ring $\mathbb{Z}[\zeta_N + \zeta_N^{-1}]$ acts on $\mathrm{Jac}(\mathcal{D}_N)$.

Theorem A.4. *For any $t_0 \in \mathbb{Q}$, $t_0 \neq 0, 1$, $\mathcal{H}((\frac{1}{N}, -\frac{1}{N}), (1,1)|t_0)$ is up to a quadratic twist by F/K part of the new part of the hyperelliptic curve $\mathcal{D}_N$ for $a = 2(1-2t_0)$.*

Proof. Since N is odd, the motive $\mathcal{H}((\frac{1}{N}, -\frac{1}{N}), (1,1)|t_0)$ is realized in the new part of the Jacobian of (the desingularization of) Euler's curve

$$\mathcal{C}_N : y^N = x(1-x)^{N-1}(1-t_0 x). \tag{36}$$

A trivial change of variables translates this equation into

$$(1-x)y^N = x(1-t_0 x).$$

Then the function field of $\mathbb{Q}(\mathcal{C}_N)$ is a quadratic extension of $\mathbb{Q}(y)$. Computing the discriminant (with respect to the variable x) of the last equation, we get the alternate definition

$$\mathcal{C}'_N : z^2 = y^{2N} + 2(1-2t_0)y^N + 1,$$

matching the curve (33) (changing variables $z = y$, $y = x$) for the value $a = 2(1-2t_0)$. The result follows from the previous considerations. □

Corollary A.5. *Let p be a prime number and let $t_0 \in \mathbb{Q} \setminus \{0,1\}$. The hypergeometric motive $\mathcal{H}((\frac{1}{p}, -\frac{1}{p}), (1,1)|t_0)$ matches the hypergeometric curve denoted by C_p^+ in [16].*

Remark 15. Theorem 2.9 states a precise formula for Frobenii elements of $\mathcal{H}((\frac{1}{p}, -\frac{1}{p}), (1,1)|t_0)$ over F (not over K). Then a priori the numerical value $H_{\mathfrak{q}}(\frac{1}{p}, -\frac{1}{p}), (1,1)|t_0)$ of might differ from Darmon's curve by the quadratic twist corresponding to the extension F/K.

Proof. The curve C_p^+ matches the hypergeometric curve $\mathcal{D}_N$ of (34). □

The picture for N even is more interesting. In this case the curve $\mathcal{C}'_N$ has an extra involution $\sigma : \mathcal{C}'_N \to \mathcal{C}'_N$ given by $\sigma(x,y) = (-x,y)$. The three involutions commute with each other, providing an action of the group $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ on $\mathcal{C}'_N$. The following result is elementary.

Lemma A.6. *The quotient of $\mathcal{C}'_N$ by the involution σ is given by*

$$\mathcal{C}'_{N/2} : y^2 = x^N + ax^{N/2} + 1.$$

Lemma A.7. *The quotient of $\mathcal{C}'_N$ by the involution $\sigma \circ \tau$ is given by*

$$\mathcal{D}_N : y^2 = x(x^N + ax^{N/2} + 1).$$

Proof. The involution $\sigma \circ \tau$ send $(x, y) \to (-x, -y)$. The field of functions on $\mathcal{C}'_N$ fixed by it is generated by $\xi = x^2$ and $\eta = xy$, which satisfy the stated relation

$$\eta^2 = \xi(\xi^N + a\xi^{N/2} + 1).$$

□

Since $\tau \in \langle \sigma \circ \tau, \sigma \rangle$, and the quotient of $\mathcal{C}'_N$ by τ has genus zero, the varieties $\mathrm{Jac}(\mathcal{C}'_{N/2})$ (of dimension $\frac{N}{2} - 1$) and $\mathrm{Jac}(\mathcal{D}_N)$ (of dimension $\frac{N}{2}$), seen as subvarieties of $\mathrm{Jac}(\mathcal{C}'_N)$ under the pullback of the quotient map, have finite intersection. Since the sum of their dimensions match the dimension of $\mathrm{Jac}(\mathcal{C}'_N)$, it follows that

$$\mathrm{Jac}(\mathcal{C}'_N) \sim \mathrm{Jac}(\mathcal{C}'_{N/2}) \times \mathrm{Jac}(\mathcal{D}_N). \tag{37}$$

Note that the *old* part of $\mathrm{Jac}(\mathcal{D}_N)$ comes from divisors d satisfying that N/d is odd (the other divisors contribute to $\mathrm{Jac}(\mathcal{C}'_{N/2})$). Explicitly, if $d \mid N$ and N/d is odd, the map

$$\pi_d(x, y) = (x^{\frac{N}{d}}, x^{\left(\frac{N}{d}-1\right)\frac{1}{2}} y),$$

maps the curve $\mathcal{D}_N$ to the curve $\mathcal{D}_d$.

Lemma A.8. *The new part of* $\mathrm{Jac}(\mathcal{D}_N)$ *has dimension* $\phi(N)$.

Proof. Follows from an easy computation as the one done in Lemma A.3, using that the old contribution comes from divisors d satisfying that N/d is odd. □

The action of the group of N-th roots of unity on $\mathcal{C}'_N$ commutes with $\sigma \circ \tau$, hence it induces an action on $\mathcal{D}_N$ given explicitly by

$$\zeta_N \cdot (x, y) = (\zeta_N^2 x, \zeta_N y).$$

In particular, the compatible systems of Galois representations attached to $\mathrm{Jac}(\mathcal{D}_N)^{\mathrm{new}}$ (viewed as $\mathbb{Z}[\zeta_N]$-module) are the ones corresponding to $\mathcal{H}((1/N, -1/N), (1, 1)|t_0)$, for $a = 2 - 4t_0$.

In order to get a representation over the field $\mathbb{Q}[\zeta_N + \zeta_N^{-1}]$, we need to get an extra splitting of the Jacobian. The curve $\mathcal{D}_N$ has once again two different involutions, namely the canonical involution τ and the involution $\iota_N : (x, y) \to \left(\frac{1}{x}, \frac{y}{x^{N+1}}\right)$. Both involutions commute with each other; τ commutes with the action of the N-th roots of unity, but ι does not, they satisfy the relation

$$\iota \circ \zeta_N = \zeta_N^{-1} \circ \iota.$$

Let $g(x)$ denote the monic polynomial whose zeroes are all the numbers $\xi + \xi^{-1}$, for $\xi \in \overline{\mathbb{Q}} \setminus \{-1\}$ satisfying $\xi^{N/2} = -1$. Clearly

$$\deg(g(x)) = \begin{cases} (N/2 - 1)/2 & \text{if } 4 \nmid N, \\ N/4 & \text{if } 4 \mid N. \end{cases}$$

Lemma A.9. *The quotient of the curve* $\mathcal{D}_N$ *by the involution* ι_N *is given by the curve*

$$\mathcal{C}_N : y^2 = xg(x^2 - 2) + a, \tag{38}$$

when $N/2$ *is odd, and by the equation*

$$\mathcal{C}_N : y^2 = (x + 2)(xg(x^2 - 2) + a), \tag{39}$$

when $N/2$ *is even. The Jacobian of both curves contain* $\mathbb{Z}[\zeta_N + \zeta_N^{-1}]$ *in their endomorphism ring.*

Proof. See [50, Proposition 3] for the first statement. The second one is clear. □

Just for completeness, we compute the quotient of $\mathcal{D}_N$ by the involution $\iota \circ \tau$.

Lemma A.10. *The quotient of the curve $\mathcal{D}_N$ by the involution $\iota_N \circ \tau$ is given by the curve*

$$y^2 = x(x^2-4)(g(x^2-2)+a),$$

when $N/2$ is odd, and by the equation

$$y^2 = (x-2)(xg(x^2-2)+a),$$

when $N/2$ is even. The Jacobian of both curves contain $\mathbb{Z}[\zeta_N + \zeta_N^{-1}]$ in their endomorphism ring.

Proof. Follows from a similar computation as the previous ones. In the first case, the functions on $\mathcal{D}_N$ fixed by the involution are generated by $\xi = x + \frac{1}{x}$ and $\eta = y(1-\frac{1}{x^2})x^{-(N/2-1)/2}$ while in the second case, they are generated by $\xi = x + \frac{1}{x}$ and $\eta = y(1-\frac{1}{x})x^{-N/4}$. □

Corollary A.11. *Let p be a prime number and let $t_0 \in \mathbb{Q} \setminus \{0,1\}$. The hypergeometric motive $\mathcal{H}((\frac{1}{2p}, -\frac{1}{2p}), (1,1)|t_0)$ matches the quadratic twist by (-1) of the hypergeometric curve denoted C_p^- in [16].*

Proof. Lemma 2.5 implies that the motive $\mathcal{H}((\frac{1}{2p}, -\frac{1}{2p}), (1,1)|t_0)$ is a quadratic twist by (-1) of Euler's curve. The curve $\mathcal{C}_{2p}$ matches the curve C_p^- of (38) with parameter $a = 2 - 4t_0$. □

References

[1] Natália Archinard. Hypergeometric abelian varieties. *Canad. J. Math.*, 55(5):897–932, 2003.

[2] Martin Azon, Mar Curcó-Iranzo, Maleeha Khawaja, Céline Maistret, and Diana Mocanu. Conductor exponents for families of hyperelliptic curves, 2024. arXiv:2410.21134.

[3] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.

[4] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979.

[5] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. Generalized Fermat equations: a miscellany. *Int. J. Number Theory*, 11(1):1–28, 2015.

[6] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng. The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. *Int. J. Number Theory*, 6(2):311–338, 2010.

[7] F. Beukers and G. Heckman. Monodromy for the hypergeometric function ${}_nF_{n-1}$. *Invent. Math.*, 95(2):325–354, 1989.

[8] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Mathematical Journal*, 91(1):61 – 88, 1998.

[9] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. On darmon's program for the generalized fermat equation, i, 2022.

[10] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV*, volume Vol. 476 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1975.

[11] Irene I. Bouw and Stefan Wewers. Computing L-functions and semistable reduction of superelliptic curves. *Glasg. Math. J.*, 59(1):77–108, 2017.

[12] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[13] Christophe Breuil and Fred Diamond. Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens. *Ann. Sci. Éc. Norm. Supér. (4)*, 47(5):905–974, 2014.

[14] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008.

[15] Henri Darmon. Modularity of fibres in rigid local systems. *Ann. of Math. (2)*, 149(3):1079–1086, 1999.

[16] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Mathematical Journal*, 102(3):413 – 449, 2000.

[17] Henri Darmon and Andrew Granville. On the equations $z^m = f(x,y)$ and $ax^p + by^q = cz^r$. *Bulletin of the London Mathematical Society*, 27(6):513–543, 11 1995.

[18] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[19] Lassina Dembélé, Nuno Freitas, and John Voight. On galois inertial types of elliptic curves over $\mathbb{Q}_\ell$, 2022. arXiv:2203.07787.

[20] Luis Dieulefait. Langlands base change for GL(2). *Ann. of Math. (2)*, 176(2):1015–1038, 2012.
[21] Luis Victor Dieulefait, Ariel Pacetti, and Panagiotis Tsaknias. On the number of Galois orbits of newforms. *J. Eur. Math. Soc. (JEMS)*, 23(8):2833–2860, 2021.
[22] Luis Victor Dieulefait and Ariel Martín Pacetti. A simplified proof of Serre's conjecture. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 117(4):Paper No. 153, 17, 2023.
[23] Johnny Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$. *J. Reine Angew. Math.*, 571:213–236, 2004.
[24] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4+B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.
[25] Jenny Fuselier, Ling Long, Ravi Ramakrishna, Holly Swisher, and Fang-Ting Tu. Hypergeometric functions over finite fields. *Mem. Amer. Math. Soc.*, 280(1382):vii+124, 2022.
[26] Elisa Lorenzo García and Ariel Pacetti. Galois representations of superelliptic curves ii: the new part. *In preparation*, 2024.
[27] Pedro-JosÃ© Cazorla GarcÃa and Lucas Villagra Torcomian. On the conductor of a family of frey hyperelliptic curves, 2025. arXiv:2503.21568.
[28] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2008. Reprint of the 1994 edition.
[29] Franco Golfieri, Ariel Pacetti, and Fernando Rodriguez Villegas. On rank 2 hypergeometric motives. *A draft is available at https://sweet.ua.pt/apacetti/*, 2025.
[30] Giulia Gugiatti, Martin Mereb, and Fernando Rodriguez-Villegas. In Preparation.
[31] Cohen Henri. L-functions of hypergeometric motives. https://www.math.u-bordeaux.fr/~hecohen/ow.pdf, 2011. Oberwolfach Talk.
[32] Nicholas M. Katz. *Exponential Sums and Differential Equations. (AM-124)*. Princeton University Press, 1990.
[33] M. A. Kenku. On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc. (2)*, 23(3):415–427, 1981.
[34] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.
[35] Mark Kisin. Moduli of finite flat group schemes, and modularity. *Ann. of Math. (2)*, 170(3):1085–1180, 2009.
[36] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.
[37] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
[38] Ariel Pacetti. On the change of root numbers under twisting and applications. *Proc. Amer. Math. Soc.*, 141(8):2615–2628, 2013.
[39] Ariel Pacetti. On transformation properties of hypergeometric motives and diophantine equations. *In preparation*, 2025.
[40] Ariel Pacetti and Lucas Villagra Torcomian. The generalized fermat equation with exponents $(3, 5, p)$, 2025. In preparation.
[41] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations. *Math. Comp.*, 91(338):2817–2865, 2022.
[42] Ariel Pacetti and Angel Villanueva. Galois representations of superelliptic curves. *Glasg. Math. J.*, 65(2):356–382, 2023.
[43] Lue Pan. The Fontaine-Mazur conjecture in the residually reducible case. *J. Amer. Math. Soc.*, 35(4):1031–1169, 2022.
[44] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
[45] Kenneth A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.
[46] David P. Roberts and Fernando Rodriguez Villegas. Hypergeometric motives. *Notices Amer. Math. Soc.*, 69(6):914–929, 2022.
[47] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.
[48] C. M. Skinner and A. J. Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, (89):5–126 (2000), 1999.
[49] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975.
[50] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

[51] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
[52] André Weil. Jacobi sums as "Grössencharaktere". *Trans. Amer. Math. Soc.*, 73:487–495, 1952.
[53] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
Email address: francogolfieri@ua.pt

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
Email address: apacetti@ua.pt

(Villegas) The Abdus Salam International Centre for Theoretical Physics, Strada Costiera 11, 34151 Trieste, Italy
Email address: villegas@ictp.it