INTRODUCTION TO THE MODULAR METHOD

Nicolas Billerey

INTRODUCTION TO THE MODULAR METHOD

NICOLAS BILLEREY

Abstract. This article is based on the author's talk in April 2022 during the 2nd Trimester Program on *Modularity and the Generalized Fermat Equation* held online at Bhaskaracharya Pratishthana in Pune, India. We introduce the modular method for Diophantine equations, focusing on the case of Fermat's last theorem, and other variants.

1. Framework

For this section, we fix coprime non-zero integers A, B, C.

1.1. **Generalized Fermat equations.** We are interested in the following Diophantine problem: Find all sextuples (x, y, z, p, q, r) of integers such that $p, q, r \geq 2$ and

$$Ax^p + By^q = Cz^r. \tag{1.1.1}$$

This is a widely open problem, despite lots of efforts by many mathematicians starting with the old Greeks. In this article, we survey a tiny but important part of this long story focusing mainly on the case

$$A = B = C = 1 \quad \text{and/or} \quad p = q = r.$$

1.2. **Solutions and signatures.** To start with, let us introduce some terminology. Given integers $p, q, r \geq 2$, we call *solution of the generalized Fermat equation* (1.1.1) any triple (a, b, c) of integers such that

$$Aa^p + Bb^q = Cc^r.$$

We say that a solution (a, b, c) is *primitive* if $\gcd(a, b, c) = 1$. The triple (p, q, r) is called the *signature* of (1.1.1). In solving (1.1.1), the strategy is completely different according to whether

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1, \ = 1, \text{ or } \ < 1.$$

If $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$, then we have $(p, q, r) = (3, 3, 3), (2, 4, 4), (2, 3, 6)$ (up to permuting p, q, r) and we are led to the problem of determining the set of rational points on a rational elliptic curve with j-invariant $j = 0, 1728$. When $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$, the possible exponents (p, q, r) are $(2, 2, k)$ with $k \geq 2$

2010 *Mathematics Subject Classification.* 11-02, 11D41.

The author thanks Alain Kraus for his remarks on a first version of this article. He is also indebted to the referee for a very careful reading and helpful comments. This work is supported by the ANR-23-CE40-0006-01 Gaec project.

and $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ (again, up to permutation) and, by a theorem of Beukers, if (1.1.1) has at least one solution, then there exist infinitely many (see [Beu98] for a detailed account). In this article, we only discuss the case where $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$.

1.3. **Fixed signatures: general result.** For any integer $p \geq 4$, the equation

$$AX^p + BY^p = CZ^p$$

defines a smooth, projective curve of genus $\frac{(p-1)(p-2)}{2} \geq 2$. By Mordell's conjecture (proved by Faltings), it has only finitely many rational points. More generally, applying Faltings' theorem in a subtle way, Darmon and Granville proved the following theorem ([DG95]).

Theorem 1.3.1 (Darmon–Granville)**.** *Let $p,q,r \geq 2$ be integers such that $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$. Then there exist only finitely many primitive solutions to the generalized Fermat equation $Ax^p + By^q = Cz^r$.*

There are plenty of particular cases where this result is made explicit (by listing all solutions) using a variety of techniques such as linear forms in logarithms, modular Galois representations and Chabauty–Kim methods, among others.

1.4. **Varying signatures: general expectations.** For the case of varying signatures, certain important specific cases are also known (such as Fermat's last theorem!) but there is only a conjectural general answer, based on the following statement which was formulated by Masser and Oesterlé in the mid eighties.

Conjecture 1.4.1 (*abc*-conjecture)**.** *Let $\epsilon > 0$. There exists a positive constant $\kappa(\epsilon)$ such that the following property holds: for every non-zero coprime integers a,b,c such that $a+b=c$, we have*

$$\max(|a|,|b|,|c|) \leq \kappa(\epsilon)\mathrm{rad}(abc)^{1+\epsilon}.$$

Here, for a non-zero integer n, we denote by $\mathrm{rad}(n)$ the product of all distinct prime divisors of n.

The *abc*-conjecture has many consequences in arithmetic but also in geometry (e.g. on effective versions of Mordell's conjecture) and other areas of mathematics. Applied to the generalized Fermat equation, it implies the following statement.

Theorem 1.4.2. *Assume that the abc-conjecture holds. Then, there are only finitely many triples (x^p, y^q, z^r) such that x,y,z are coprime integers and p,q,r are integers ≥ 2 satisfying*

$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1 \quad \textit{and} \quad Ax^p + By^q = Cz^r.$$

Proof. Let x, y, z be coprime integers for which there exist integers $p, q, r \geq 2$ satisfying $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ and $Ax^p + By^q = Cz^r$. If $xyz = 0$, then there are only finitely many choices for x^p, y^q, z^r: if, say, $x = 0$, then y and z are coprime and thus $y^q \mid C$ and $z^r \mid B$. Let us now assume $xyz \neq 0$. The non-zero integers Ax^p, By^q and Cz^r may not be coprime. Write d for their gcd. We show that d is bounded independently of x, y, z. Let ℓ be a prime. By assumption, at least one of x, y, z is not divisible by ℓ. It then follows that

$$v_\ell(d) = \min\left(v_\ell(Ax^p), v_\ell(By^q), v_\ell(Cz^r)\right) \leq \max(v_\ell(A), v_\ell(B), v_\ell(C)).$$

Here $v_\ell(n)$ denotes the ℓ-adic valuation of $n \in \mathbb{Z}\setminus\{0\}$. This inequality shows in particuler that d divides ABC. Applying the abc-conjecture to the three non-zero coprime integers $Ax^p/d, By^q/d, Cz^r/d$, we get that for all $\epsilon > 0$, we have

$$\left|\frac{Ax^p}{d}\right|, \left|\frac{By^q}{d}\right|, \left|\frac{Cz^r}{d}\right| \leq \kappa(\epsilon)\mathrm{rad}\left(\frac{Ax^p}{d}\cdot\frac{By^q}{d}\cdot\frac{Cz^r}{d}\right)^{1+\epsilon}. \tag{1.4.3}$$

On the other hand, we have

$$\begin{aligned}\mathrm{rad}\left(\frac{Ax^p}{d}\cdot\frac{By^q}{d}\cdot\frac{Cz^r}{d}\right) &\leq \mathrm{rad}\left(\frac{ABC}{d}x^py^qz^r\right)\\ &\leq \mathrm{rad}\left(\frac{ABC}{d}\right)\mathrm{rad}\left(x^py^qz^r\right) \quad \text{as } d \text{ divides } ABC\\ &\leq \left|\frac{ABCxyz}{d}\right|.\end{aligned}$$

It then follows from (1.4.3) that we have

$$|x|^p \leq \kappa(\epsilon)\frac{|A|^\epsilon|BC|^{1+\epsilon}}{d^\epsilon}|xyz|^{1+\epsilon}, \qquad |y|^q \leq \kappa(\epsilon)\frac{|B|^\epsilon|AC|^{1+\epsilon}}{d^\epsilon}|xyz|^{1+\epsilon},$$
$$|z|^r \leq \kappa(\epsilon)\frac{|C|^\epsilon|AB|^{1+\epsilon}}{d^\epsilon}|xyz|^{1+\epsilon}$$

and hence

$$|x|^p, |y|^q, |z|^r \leq \kappa(\epsilon)\,|ABC|^{1+\epsilon}\,|xyz|^{1+\epsilon}. \tag{1.4.4}$$

Therefore we have

$$\begin{aligned}|xyz| = (|x|^p)^{\frac{1}{p}}(|y|^q)^{\frac{1}{q}}(|z|^r)^{\frac{1}{r}} &\leq \kappa(\epsilon)^{\chi_{p,q,r}}|ABC|^{\chi_{p,q,r}\cdot(1+\epsilon)}|xyz|^{\chi_{p,q,r}\cdot(1+\epsilon)}\\ &\leq \kappa(\epsilon)^{\frac{41}{42}}|ABC|^{\frac{41}{42}(1+\epsilon)}|xyz|^{\frac{41}{42}(1+\epsilon)}\end{aligned}$$

since $\chi_{p,q,r} \coloneqq \frac{1}{p}+\frac{1}{q}+\frac{1}{r} \leq \frac{1}{2}+\frac{1}{3}+\frac{1}{7} = \frac{41}{42}$. Choosing $\epsilon < \frac{1}{41}$, we have

$$1 - \frac{41}{42}(1+\epsilon) > 0 \quad \text{and} \quad |xyz|^{1-\frac{41}{42}(1+\epsilon)} \leq \kappa(\epsilon)^{\frac{41}{42}}|ABC|.$$

Therefore $|xyz|$ is bounded and so are $|x|^p, |y|^q$ and $|z|^r$ by (1.4.4). □

Based on computational investigations (partly due to Beukers and Zagier), the following conjecture has been formulated in the case $A = B = C = 1$.

Conjecture 1.4.5. *The only primitive solutions in non-zero integers of the generalized Fermat equation*

$$x^p + y^q = z^r, \quad \text{with } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

correspond to the following identities:

$$1^p + 2^3 = 3^2 \,(p > 6), \qquad 2^5 + 7^2 = 3^4,$$

$$7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2, \qquad 3^5 + 11^4 = 122^2$$

and

$$17^7 + 76271^3 = 21063928^2, \qquad 1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7, \qquad 43^8 + 96222^3 = 30042907^2,$$

$$33^8 + 1549034^2 = 15613^3.$$

In all identities listed above, Beal noticed that the smallest exponent is 2. This led him to the following statement (also known as the Tijdeman–Zagier conjecture) whose proof is awarded $1 million by the American Mathematical Society.

Conjecture 1.4.6 (Beal Prize conjecture)**.** *If, for integers $p, q, r \geq 2$ such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, the equation $x^p + y^q = z^r$ has a solution in non-zero integers, then one of the exponents p, q, and r is equal to 2.*

1.5. **Trivial solutions.** As a consequence of Theorem 1.4.2 (and hence of the *abc*-conjecture), if (x, y, z) is a primitive solution in non-zero integers of a generalized Fermat equation, then for large enough p and fixed $r \geq 3$, we have

$$\begin{cases} |xyz| = 1 & \text{for signature } (p, p, p); \\ |xy| = 1 & \text{for signature } (p, p, r); \\ |z| = 1 & \text{for signature } (r, r, p). \end{cases}$$

Definition 1.5.1. For these signatures, we call such triples the *trivial solutions* together with solutions (x, y, z) such that $xyz = 0$.

As we shall explain later, these 'trivial solutions' will be the main obstruction in solving the corresponding generalized Fermat equation.

2. Background

In this section, we recall some background on Galois representations, modular forms and elliptic curves which will be useful when discussing the modular method.

2.1. **Galois representations.** Let us denote by $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the absolute Galois group of $\mathbb{Q}$, that is the automorphism group of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The group $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is profinite, and hence compact.

Let p be a prime number. Write $\overline{\mathbb{F}}_p$ for an algebraic closure of $\mathbb{F}_p$. The following definition is quite restrictive (there are plenty of other 'types' of Galois representations!) but will be enough for what we are concerned with in the present article.

Definition 2.1.1. A *mod p Galois representation* is defined to be a group homomorphism

$$\overline{\rho} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{F}}_p)$$

which is continuous with respect to the profinite topology on the left and the discrete topology on the right.

We shall see in the next subsections that there are Galois representations attached to classical eigenforms and to rational elliptic curves but we first recall the following useful definition.

Definition 2.1.2. A mod p Galois representation $\overline{\rho} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{F}}_p)$ is *unramified at a prime ℓ* if $\overline{\rho}(I_\ell) = \{1\}$, where I_ℓ is an inertia group at ℓ in $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Otherwise, it is *ramified at ℓ*.

2.2. **Modular forms.** Let $f = \sum_{n\geq 1} a_n(f)q^n$ be a weight-2 (cuspidal) newform of level $\Gamma_0(N)$ with $N \geq 1$ (that is, f has trivial Nebentypus character). Denote by $K = \mathbb{Q}(\{a_n(f); n \geq 1\})$ the field generated by the Fourier coefficients of f (which are also its Hecke eigenvalues since f is normalized: $a_1(f) = 1$) and recall that K is a number field (which is viewed as a subfield of a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$) such that $a_n(f)$ is an integral element in K for every $n \geq 1$.

Let p be a prime number. We fix a place of $\overline{\mathbb{Q}}$ above p and consider the reduction of integral elements in $\overline{\mathbb{Q}}$ with respect to this choice. Its residue field is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

The following result was proved by Eichler and Shimura – and later generalized to arbitrary weights ≥ 2 by Deligne.

Theorem 2.2.1 (Eichler–Shimura, Deligne)**.** *Up to isomorphism, there is a unique semisimple mod p Galois representation*

$$\overline{\rho}_{f,p} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{F}}_p)$$

satisfying the following properties: it is unramified outside Np and for every prime $\ell \nmid Np$, the characteristic polynomial of $\overline{\rho}_{f,p}(\mathrm{Frob}_\ell)$ is the reduction of

$$X^2 - a_\ell(f)X + \ell. \tag{2.2.2}$$

Here Frob_ℓ *denotes a choice of a Frobenius element at ℓ in* $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

This result motivates the following definition.

Definition 2.2.3. A mod p Galois representation

$$\overline{\rho} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{F}}_p)$$

is said to be *modular of level* $N \geq 1$ if there exists a weight-2 newform f of level $\Gamma_0(N)$ such that $\overline{\rho} \simeq \overline{\rho}_{f,p}$. In that case, we also say that $\overline{\rho}$ *arises from* f.

It may happen that a mod p Galois representation which is modular of some level N is also modular of a smaller level. This phenomenon is intimately related to congruences between modular forms and is the subject of the following deep result, known as *Ribet's level-lowering theorem*.

Theorem 2.2.4 (Ribet, [Rib90])**.** *Let $\overline{\rho} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{F}}_p)$ be irreducible and modular of level N, with $p \geq 3$. Let ℓ be a prime dividing N precisely once. When $\ell \neq p$, assume further that N is coprime to p. If $\overline{\rho}$ is finite at ℓ, then $\overline{\rho}$ is modular of level N/ℓ.*

Remark 2.2.5. At a prime $\ell \neq p$, the condition that $\overline{\rho}$ is finite merely means that $\overline{\rho}$ is unramified. At $\ell = p$, the condition is more technical but we shall rephrase it more simply in the special case of interest to us in the next subsection.

2.3. **Elliptic curves.** Let E be an elliptic curve defined over $\mathbb{Q}$ and let p be a prime number. Denote by $E[p]$ the set of p-torsion points on E. Then, $E[p]$ is a 2-dimensional vector space over $\mathbb{F}_p$. The absolute Galois group $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$ acts linearly on $E[p]$. Hence, after choosing a basis for the p-torsion, this gives rise to a mod p Galois representation

$$\overline{\rho}_{E,p} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \simeq \mathbf{GL}_2(\mathbb{F}_p),$$

known as *the mod p representation associated with E*.

Lemma 2.3.1. *Assume that p is odd. The representation $\overline{\rho}_{E,p}$ is irreducible if and only if it is absolutely irreducible (i.e., it is irreducible when we extend the scalars to $\overline{\mathbb{F}}_p$).*

Proof. If $\overline{\rho}_{E,p}$ is absolutely irreducible, then it is irreducible. Let us now show the reverse implication. Recall from the properties of the Weil pairing that $\det(\overline{\rho}_{E,p}) = \chi_p$ where χ_p denotes the mod p cyclotomic character and assume, by the contrapositive, that $\overline{\rho}_{E,p}$ is absolutely reducible, i.e. that there exists $P \in \overline{\mathbb{F}}_p^2$ which is a common eigenvector for every $\overline{\rho}_{E,p}(\sigma)$ with $\sigma \in \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let c denote the complex conjugation in $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since p is odd, we have that $\det \overline{\rho}_{E,p}(c) = \chi_p(c) = -1 \neq 1$. Therefore, $\overline{\rho}_{E,p}(c)$ has order 2 and is conjugate in $\mathbf{GL}_2(\mathbb{F}_p)$ to the diagonal matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In particular, up to multiplication by a scalar in $\overline{\mathbb{F}}_p$, we have that P actually lies in $\mathbb{F}_p^2$, hence proving that the representation $\overline{\rho}_{E,p} : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F}_p)$ is already reducible.

□

Remark 2.3.2. Let $\overline{\rho}$ be a Galois representation with values in $\mathbf{GL}_2(\mathbb{F})$ where $\mathbb{F}$ is a subfield of $\overline{\mathbb{F}}_p$. Assume that $p > 2$ and that $\overline{\rho}$ is *odd* in the sense that $\det \overline{\rho}(c) = -1$, where c denotes the complex conjugation in $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (with respect to an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$). Then, the previous proof shows more generally that $\overline{\rho}$ is irreducible if and only if it is absolutely irreducible.

Recall that the conductor of E is a certain integer N_E whose prime divisors are precisely the primes of bad reduction for E. By the criterion of Néron–Ogg–Shafarevich, the representation $\overline{\rho}_{E,p}$ is unramified outside $N_E p$. If $\ell \neq p$ is a prime of good reduction, then the characteristic polynomial of $\overline{\rho}_{E,p}(\mathrm{Frob}_\ell)$ is the reduction of

$$X^2 - a_\ell(E)X + \ell. \tag{2.3.3}$$

Moreover, E has (bad) multiplicative reduction at a prime ℓ if and only if $v_\ell(N_E) = 1$. In that case, we have the following result of Tate describing the ramification of $\overline{\rho}_{E,p}$, where we denote by j_E the j-invariant of E and by v_ℓ the ℓ-adic valuation.

Proposition 2.3.4 (Tate)**.** *Let $\ell \neq p$ be a prime such that E has multiplicative reduction at ℓ. Then, the representation $\overline{\rho}_{E,p}$ is unramified at ℓ if and only if we have $v_\ell(j_E) \equiv 0 \pmod{p}$.*

When E has multiplicative reduction at p, the condition that $\overline{\rho}_{E,p}$ is finite at p is equivalent to $v_p(j_E) \equiv 0 \pmod{p}$ ([DDT97, Proposition 2.12]). Therefore, according to Remark 2.2.5 and Tate's result, for any prime ℓ of multiplicative reduction, we have that the representation $\overline{\rho}_{E,p}$ is finite at ℓ if and only if $v_\ell(j_E) \equiv 0 \pmod{p}$.

The following important result was conjectured by Ogg and proved by Mazur in 1977.

Theorem 2.3.5 (Mazur, [Maz77, Theorem 8])**.** *The only possible torsion subgroups of $E(\mathbb{Q})$ are*

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \leq n \leq 10 \text{ and } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} & \text{for } 1 \leq n \leq 4. \end{array}$$

We finally state the following crucial result which was historically the last missing ingredient in the proof of Fermat's last theorem.

Theorem 2.3.6 (Wiles [Wil95], Taylor–Wiles [TW95])**.** *Assume $E/\mathbb{Q}$ is semistable and for $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 3/2$, let*

$$L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p(E)p^{-s} + \mathbf{1}_{N_E}(p)p^{1-2s}} = \sum_{n \geq 1} \frac{a_n(E)}{n^s}$$

be the L-function of E. Here, $\mathbf{1}_{N_E}(p)$ is 0 or 1 according to whether p divides N_E or not, respectively. Then, $f_E = \sum_{n \geq 1} a_n(E)q^n$ is a weight-2 newform of level $\Gamma_0(N_E)$.

3. Fermat's last theorem

3.1. **Statement and first reductions.** In this section, we summarize the main steps in the proof of Fermat's last theorem whose statement is recalled below.

Theorem 3.1.1 (Fermat's last theorem)**.** *For every integer $n \geq 3$, there are no non-trivial solutions to the equation $x^n + y^n = z^n$.*

The proof is by contradiction assuming the existence of a non-trivial solution (a, b, c) for some $n \geq 3$. Without loss of generality, we can assume that a, b, c are pairwise coprime integers.

Euler proved the case $n = 3$ and Fermat the case $n = 4$ using a famous descent argument. Hence, we may assume that $n = p \geq 5$ is prime. Switching a, b, c if necessary, we may further suppose that

$$a^p \equiv -1 \pmod 4 \quad \text{and} \quad b^p \equiv 0 \pmod{32}. \tag{3.1.2}$$

We now proceed in five main steps. The whole strategy is known as *the modular method*.

3.2. **The (original) modular method.** The strategy presented here follows the original approach of Hellegouarch, Frey, Mazur, Ribet, and Wiles – among others. In particular, we do not appeal to (but sometimes mention) more recent results that could be used to weaken some assumptions or shorten certain proofs.

Step 1: Construction. Following an idea of Hellegouarch and Frey, we consider the cubic curve given by the following Weierstrass equation

$$E : y^2 = x(x - a^p)(x + b^p). \tag{3.2.1}$$

Its discriminant

$$\Delta = 16(abc)^{2p}$$

is non-zero since (a, b, c) is non-trivial and hence (3.2.1) defines an elliptic curve over $\mathbb{Q}$. Incidentally, we note that E has all of its 2-torsion which is defined over $\mathbb{Q}$. The standard c_4 and j coefficients of this model are computed to be

$$c_4 = 16\left(a^{2p} + (ab)^p + b^{2p}\right) \quad \text{and} \quad j = \frac{c_4^3}{\Delta}.$$

Since a, b and c are pairwise coprime, the formulas for Δ and c_4 show that (3.2.1) defines a minimal model for $E/\mathbb{Q}$ away from 2. Moreover, the curve E has bad reduction at an odd prime ℓ if and only if $\ell \mid abc$.

Under our assumption (3.1.2), the change of variables

$$x = 4X \quad \text{and} \quad y = 8Y + 4X$$

gives the following integral model for $E/\mathbb{Q}$:

$$Y^2 + XY = X^3 + \frac{b^p - a^p - 1}{4}X^2 - \frac{(ab)^p}{16}X. \tag{3.2.2}$$

For this model we have

$$c_4 = a^{2p} + (ab)^p + b^{2p} \quad \text{and} \quad \Delta = \frac{(abc)^{2p}}{2^8}.$$

In particular, these coefficients c_4 and Δ are coprime, and hence (3.2.2) defines a (global) minimal model for $E/\mathbb{Q}$. In particular, the elliptic curve E is *semistable* and its minimal discriminant is $\Delta_{\min}(E) = \frac{(abc)^{2p}}{2^8}$.

We summarize the main properties of $E/\mathbb{Q}$ we have proved so far in the following statement.

Proposition 3.2.3. *The elliptic curve E has all of its 2-torsion points which are defined over $\mathbb{Q}$. Moreover, E is semistable and has bad reduction precisely at the primes dividing abc. If ℓ is such a bad prime, then we have*

$$v_\ell(j_E) = -v_\ell(\Delta_{\min}) = \begin{cases} -2pv_\ell(abc) & \equiv 0 \pmod{p} \quad \text{if } \ell \text{ odd;} \\ 8 - 2pv_2(abc) & \not\equiv 0 \pmod{p} \quad \text{if } \ell = 2. \end{cases}$$

Step 2: Modularity. Write $\overline{\rho}_{E,p}$ for the mod p Galois representation attached to E and p as constructed in §2.3. Applying Wiles' modularity theorem, we obtain the following result using the terminology introduced in §2.2.

Theorem 3.2.4. *The mod p representation $\overline{\rho}_{E,p}$ is modular of level*

$$N_E = \operatorname{rad}\left(\frac{(abc)^p}{16}\right) = \prod_{\ell \mid abc} \ell.$$

Here, the product runs over all prime divisors ℓ of abc.

Proof. Since E is semistable, then $N_E = \operatorname{rad}(\Delta_{\min}(E)) = \operatorname{rad}\left(\frac{(abc)^p}{16}\right)$ is the conductor of E. Consider the weight-2 newform f_E of level N_E associated to E by Wiles' modularity theorem 2.3.6. Let ℓ be a prime not dividing pN_E. Then, we have $a_\ell(f_E) = a_\ell(E)$ and $\overline{\rho}_{f_E,p}(\mathrm{Frob}_\ell)$ and $\overline{\rho}_{E,p}(\mathrm{Frob}_\ell)$ have the same characteristic polynomials by equations (2.2.2) and (2.3.3). It follows that $\overline{\rho}_{E,p} \simeq \overline{\rho}_{f_E,p}$ ([DS74, Lemme 3.2]). □

Remark 3.2.5. Note that Wiles' proof of the modularity of all semistable rational elliptic curves followed from the modularity of either their mod 3 or their mod 5 representation.

Step 3: Irreducibility. As a consequence of Tate's result (Proposition 2.3.4) and Proposition 3.2.3, we have the following statement.

Proposition 3.2.6. *The representation $\overline{\rho}_{E,p}$ is unramified away from $\{2, p\}$.*

Proof. Let ℓ be a prime, $\ell \neq p$. If $\ell \nmid abc$, then E has good reduction at ℓ and hence $\overline{\rho}_{E,p}$ is unramified at ℓ. Assume now that $\ell \mid abc$ and $\ell > 2$. According to Proposition 3.2.3, we have $v_\ell(j_E) \equiv 0 \pmod{p}$, and hence by Proposition 2.3.4, the representation $\overline{\rho}_{E,p}$ is unramified at ℓ. □

The following theorem is the main result of the third step. It follows from Mazur's theorem 2.3.5 and from the local description of the mod p representation associated with E.

Theorem 3.2.7. *The representation $\overline{\rho}_{E,p}$ is absolutely irreducible, i.e., it is irreducible when we extend the scalars to $\overline{\mathbb{F}}_p$.*

Proof. According to Lemma 2.3.1, the representation $\overline{\rho}_{E,p}$ is absolutely irreducible if and only if it is irreducible. Therefore, assume for a contradiction that $\overline{\rho}_{E,p}$ is reducible. Write D for a rational subgroup of order p in $E[p]$ and denote by $\chi : \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ the character giving the action of $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on D. Since E is semistable by Step 1, one has either $\chi = \chi_p$ or χ is trivial ([Ser72, p. 307]). Here χ_p denotes the mod p cyclotomic character. In the latter case, the curve E has a rational point of order p. Moreover, E also has all of its 2-torsion which is defined over $\mathbb{Q}$. Therefore, the order of the torsion subgroup of $E(\mathbb{Q})$ is $\geq 4p \geq 20$, hence contradicting Mazur's theorem. In the former case, the elliptic curve $E' = E/D$ has a rational subgroup D' of order p and the action of $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on D' is given by $\chi_p\chi^{-1}$ which is trivial by assumption. We conclude as before. □

Remark 3.2.8. Alternatively, one may also invoke Mazur's isogeny theorem from 1978 ([Maz78, Theorem 1]) and its later generalizations; see the article *Mazur's isogeny theorem* by Philippe Michaud-Jacobs in this volume. Note also that the previous proof requires only that $E/\mathbb{Q}$ is semistable and has all of its 2-torsion which is defined over $\mathbb{Q}$.

Step 4: Level lowering. The proof of the following statement uses Ribet's level-lowering theorem from §2.2 and the results from the previous steps.

Theorem 3.2.9. *The representation $\overline{\rho}_{E,p}$ is modular of level 2.*

Proof. By Step 2, the representation $\overline{\rho}_{E,p}$ is modular of level N_E and by Step 3, it is absolutely irreducible. Let N'_E be the prime-to-p part of N_E. Let us first show that $\overline{\rho}_{E,p}$ is modular of level N'_E. If $p \nmid N_E$ (that is $p \nmid abc$), then $N'_E = N_E$ and there is nothing to say. Else, if $p \mid N_E$, then $\overline{\rho}_{E,p}$ is finite at p by the discussion after Proposition 2.3.4 and Proposition 3.2.3. According to Ribet's level-lowering theorem 2.2.4, we conclude that $\overline{\rho}_{E,p}$ is modular of level N'_E, as desired.

Write $N'_E = 2m$ where m is the squarefree product of all odd prime numbers $\neq p$ dividing abc. Let ℓ be a prime dividing m (in particular, ℓ is different from p and odd). According to Proposition 3.2.6, the representation $\overline{\rho}_{E,p}$ is unramified at ℓ, and hence finite. Applying Ribet's theorem repeatedly to such primes ℓ, we obtain that $\overline{\rho}_{E,p}$ is modular of level $N'_E/m = 2$. □

Step 5: Contradiction. Contrary to other Diophantine equations – as we shall see in the next section – this last step is particularly easy in the case of Fermat's last theorem. Indeed, it is well-known that there are no nonzero cusp forms of weight 2 and level 2.

This gives the desired contradiction with Theorem 3.2.9 and concludes the proof of Fermat's last theorem.

4. Extending the modular method

In this section, we discuss some obstacles that arise when applying the modular method to tackle other Diophantine equations of Fermat type. For simplicity, we focus on some specific examples which are representative of these difficulties.

4.1. **An example of Ribet–Darmon–Merel.**

We deal here with the equation

$$x^p + y^p = 2z^p \tag{4.1.1}$$

for a prime exponent ≥ 7 which was studied independently by Ribet ([Rib97]) and Darmon–Merel ([DM97]) in 1997.

We briefly explain how we can proceed with Steps 1–4 of the modular method in this situation and then discuss in more detail the fifth step.

Step 1. Let (a, b, c) be a non-trivial primitive solution to equation (4.1.1). Recall that primitive means $\gcd(a, b, c) = 1$ and non-trivial means abc is neither 0 nor ± 1. Then a and b are odd, and without loss of generality, one may assume that $a^p \equiv -1 \pmod 4$. Associated with such a solution (a, b, c) is the following rational elliptic curve $E = E_{a,b,c}$ given by

$$E : y^2 = x(x - a^p)(x - 2c^p).$$

We note that E is a quadratic twist (by -1) of the elliptic curve given by the equation $y^2 = x(x - a^p)(x + b^p)$.

Its c_4- and Δ-coefficients are

$$c_4 = 2^4 \left(a^{2p} - 2a^p c^p + 4c^{2p}\right) \quad \text{and} \quad \Delta = 2^6 (abc)^{2p}. \tag{4.1.2}$$

The elliptic curve $E/\mathbb{Q}$ is semistable away from 2. Moreover, E has multiplicative reduction at each odd prime $\ell \mid abc$ and $v_\ell(j_E) \equiv 0 \pmod p$, where $j_E = \frac{c_4^3}{\Delta}$ denotes the j-invariant of E.

More precisely, the conductor N_E of E satisfies

$$N_E = \begin{cases} \mathrm{rad}(abc) & \text{if } abc \text{ is even} \\ 2^5 \mathrm{rad}(abc) & \text{if } abc \text{ is odd.} \end{cases} \tag{4.1.3}$$

This finishes Step 1 of the modular method for this equation.

Step 2. Since we no longer have the semistability condition, Wiles' original modularity theorem 2.3.6 does not apply. Fortunately, this result has been generalized by Breuil, Conrad, Diamond and Taylor who proved in 2001 that *every* elliptic curve over $\mathbb{Q}$ is modular ([BCDT01]), hence concluding Step 2.

Step 3. Similarly, the proof of Theorem 3.2.7 does not apply anymore as E is not semistable in general. A key observation is that E has a prime $\neq 2$ of multiplicative reduction though. This follows from (4.1.3) and the fact that, if abc is a power of 2, then (a, b, c) is trivial.

Fortunately again, at least for $p \geq 17$, Mazur's work mentioned in Remark 3.2.8 together with the previous observation imply that the mod p representation $\overline{\rho}_{E,p}$ associated with E is absolutely irreducible ([Maz78, Corollary 4.4]). This completes Step 3.

Step 4. Combining the arithmetic properties of E listed above with modularity and irreducibility results for E and $\overline{\rho}_{E,p}$ respectively, Ribet's level-lowering theorem 2.2.4 implies that, at least for $p \geq 17$, the representation $\overline{\rho}_{E,p}$ arises from a weight-2 newform f of level M which is explicitly given by:

$$M = \begin{cases} 2 & \text{if } abc \text{ is even} \\ 32 & \text{if } abc \text{ is odd.} \end{cases}$$

This completes Step 4.

Step 5. We now turn our attention to the last step of the modular method for equation (4.1.1).

In the case abc is even, we reach a contradiction exactly as in Fermat's last theorem.

From now on, assume that abc is odd. This case is much more difficult! The reason is that the space of weight-2 newforms of level 32 is non-trivial. More precisely, it is a one-dimensional vector space over $\mathbb{C}$ generated by a form f whose first Fourier coefficients are given by

$$f = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} + \dots$$

It turns out that f corresponds (by modularity or more simply via the Eichler–Shimura correspondence which associates a rational elliptic curve to every weight-2 newform of trivial Nebentypus character with *integral* Fourier expansion) to (the isogeny class of) the elliptic curve $F/\mathbb{Q}$ given by the following minimal equation:

$$F : y^2 = x^3 - x. \tag{4.1.4}$$

At this point it is worth noting that F is isomorphic to the elliptic curve $E_{1,1,1}$ corresponding to the trivial solution $(1, 1, 1)$, hence showing that it is actually the main obstacle in solving this equation. Therefore, we are led to the problem of contradicting the following isomorphism between two mod p elliptic Galois representations:

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{F,p}. \tag{4.1.5}$$

This problem, in general, only has a conjectural answer, given by the following.

Conjecture 4.1.6 (Frey–Mazur)**.** *There exists a constant $C > 0$ such that the following holds: for all elliptic curves E and F defined over $\mathbb{Q}$ and for all prime numbers $p > C$, if $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$ are isomorphic, then E and F are isogenous over $\mathbb{Q}$.*

Remark 4.1.7.

(1) The *abc*-conjecture implies the following weaker (non-uniform) statement in the direction of the Frey–Mazur conjecture. Fix an elliptic curve $E/\mathbb{Q}$. Then, there exists a constant $C_E > 0$ (depending on E) such that for all elliptic curves $F/\mathbb{Q}$ and for all prime numbers $p > C_E$, if $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$ are isomorphic, then E and F are isogenous over $\mathbb{Q}$ (see for instance [Bil08, Appendice B] for a proof of this assertion).

(2) If it exists, the constant C in Conjecture 4.1.6 is > 17 since (as it was first observed by Cremona) the two elliptic curves

$$E : y^2 + xy = x^3 - 8x + 27$$

and

$$F : y^2 + xy = x^3 + 8124402x - 11887136703,$$

labelled [LMF23, 3675.g1] and [LMF23, 47775.be1] in LMFDB respectively, have isomorphic mod 17 representations ([Bil16]). For values of $p < 17$, examples (or even infinite families of examples) of pairs of 'congruent elliptic curves' can be found in the literature. Such congruences play a crucial role in Wiles' proof of his famous '3-5 trick' for instance.

(3) It is worth noting that given an elliptic curve $E/\mathbb{Q}$ and a prime p such that $\overline{\rho}_{E,p}$ is absolutely irreducible, there are *infinitely many* weight-2 newforms f whose mod p representation $\overline{\rho}_{f,p}$ (coming from Theorem 2.2.1, suitably generalized to take into account that f need not be of trivial Nebentypus character) is isomorphic to $\overline{\rho}_{E,p}$. See [DT94] for a precise statement in this direction. Rephrased in these terms, Conjecture 4.1.6 then implies that only *finitely many* of these forms f correspond (via the aforementioned Eichler–Shimura correspondence) to rational elliptic curves. More generally, one may wonder for instance whether there are only finitely of the forms f for which the degree of their coefficient field is bounded by a given constant?

Applying this conjecture to the isomorphism (4.1.5) gives the desired conclusion. Indeed, isogenous elliptic curves have the same conductor, and hence

$$2^5 \mathrm{rad}(abc) = N_E = M = 2^5,$$

that is $abc = \pm 1$, in contradiction with the assumption that (a, b, c) is non-trivial.

Remarkably, Darmon and Merel manage to reach a contradiction in the fifth step of the modular method for equation (4.1.1) without appealing to any conjecture.

Fundamental to their approach is the fact that the elliptic curve F given by (4.1.4) has complex multiplication by $\mathbb{Q}(i)$. This allows for a precise understanding of the image G in $\mathbf{GL}_2(\mathbb{F}_p)$ of the Galois representation $\overline{\rho}_{F,p}$. In particular, we have that G is the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbb{F}_p)$ which is split or non-split according to whether $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$, respectively.

Assume first that $p \equiv 1 \pmod 4$. By the theory of complex multiplication and the isomorphism (4.1.5), the curve E gives rise to a rational point on the modular curve $X_{\mathrm{split}}(p)$ parametrizing elliptic curves with a mod p representation whose image is contained in the normalizer of a split Cartan subgroup.

For $p \geq 17$, a result of Momose ([Mom84]) then implies that E has potentially good reduction at all primes $\neq 2$, contradicting the key observation made in Step 3. This finishes the proof of the main result for (large enough) $p \equiv 1 \pmod 4$. We note that this case was already known to Ribet ([Rib97]).

Remark 4.1.8. Results by Bilu–Parent–Rebolledo ([BPR13]) for $p \geq 17$ and Balakrishnan–Dogra–Müller–Tuitman–Vonk ([BDM$^+$19]) for $p = 13$ show that $X_{\mathrm{split}}(p)(\mathbb{Q})$ consists only of cusps and complex multiplication points. A sledge-hammer argument for this case!

Assume now that $p \equiv -1 \pmod 4$. Using basic arguments from complex multiplication and Tate's theory, Darmon and Merel first show that p does not divide abc. Their main contribution is then an integrality result (analogous to that of Momose mentioned above) for the j-invariant of E which we state below in the general form given in their article.

Theorem 4.1.9 (Darmon–Merel, [DM97, Theorem 8.1])**.** *Suppose that E is an elliptic curve over $\mathbb{Q}$ such that the following conditions hold:*

1. *The curve E has a $\mathbb{Q}$-rational subgroup of order r, with $r = 2$ or 3.*
2. *We have $p \geq 5$, and the image in $\mathbf{GL}_2(\mathbb{F}_p)$ of the mod p representation associated with E is isomorphic to the normalizer of a non-split Cartan subgroup.*

Then the j-invariant of E belongs to $\mathbb{Z}[\frac{1}{p}]$.

The Frey elliptic curve E has all of its 2-torsion points which are defined over $\mathbb{Q}$. In particular, it has a $\mathbb{Q}$-rational subgroup of order 2. Moreover, since $p \equiv -1 \pmod 4$, its mod p representation has image isomorphic to the normalizer of a non-split Cartan subgroup by the isomorphism (4.1.5) and the theory of complex multiplication. Applying Darmon–Merel's result then gives the desired contradiction thanks to formula (4.1.2) and the fact

that $p \nmid abc$. This finishes Step 5 of the modular method in the case $p \equiv -1 \pmod 4$.

Remark 4.1.10. In the non-split Cartan case, there are no results analogous to those mentioned in Remark 4.1.8, but Lemos ([Lem19, Proposition 2.1]) has improved on Darmon–Merel's Theorem 4.1.9 by showing that if E has a $\mathbb{Q}$-rational isogeny of degree $r \in \Sigma := \{2, 3, 5, 7, 13\}$ and a mod p representation for some prime $p \notin \Sigma$ which has image contained in the normalizer of a non-split Cartan subgroup, then its j-invariant is integral.

Combining the previous arguments (for $p \geq 17$) with work of Dénes from 1952 (for the smaller exponents) yields the following result.

Theorem 4.1.11 (Ribet, Darmon–Merel)**.** *For every integer $n \geq 3$, the Fermat equation $x^n + y^n = 2z^n$ has no non-trivial primitive solution.*

4.2. **Other signatures, other problems.** Frey curves associated with generalized Fermat equations have been constructed by various authors for a few signatures including $(p, p, 2)$, $(p, p, 3)$ and (r, r, p) for $r = 3, 5, 7$ (see the survey articles [Kra99] and [BCDY15] for a more complete list).

For a non-trivial primitive solution (a, b, c) of $x^3+y^3 = z^p$, this Frey curve reads as follows:

$$E_{a,b} : y^2 = x^3 + 3abx + b^3 - a^3.$$

It has discriminant $-2^4 3^3 (a^3 + b^3)^2$.

Solutions with $c \neq 0$ give rise to elliptic curves, which luckily have complex multiplication when (a, b, c) is trivial, that is $abc = 0$. Since the curve $E_{a,b}$ has a rational 2-torsion point (namely the point $(a-b, 0)$), Darmon–Merel's arguments mentioned in the previous subsection apply to eliminate the newforms corresponding to trivial solutions.

Unfortunately, another issue arises in the contradiction step due to the existence of an 'almost solution' (or 'pseudo-solution') corresponding to the Catalan identity $2^3+1^3 = 3^2$. More precisely, we do not know how to discard the isomorphism

$$\overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{E_{2,1},p}, \quad \text{with} \quad E_{2,1} : y^2 = x^3 + 6x - 7,$$

for an arbitrary non-trivial solution (a, b, c), hence preventing us from completely solving the equation $x^3 + y^3 = z^p$. Despite this, it has been solved for various values of the exponent p using a great variety of techniques. The following statement combines work of Euler, Darmon–Granville ([DG95]), Kraus ([Kra98b]), Bruin ([Bru00]), Dahmen ([Dah08]), Chen–Siksek ([CS09]) and Freitas ([Fre16]).

Theorem 4.2.1. *The generalized Fermat equation $x^3+y^3 = z^p$ has no non-trivial primitive solution for $p \geq 3$ in a set of primes P of density ≈ 0.844. For instance, P contains the primes $p \geq 3$ such that*

$$p < 10^9, \quad \text{or } p \equiv 51, 103, 105 \pmod{106}, \quad \text{or } p \equiv 2 \pmod 3.$$

4.3. **Frey curves over totally real fields and Frey varieties.** Let $r \geq 7$ be a prime. In [Fre15], Freitas associates several explicit Frey curves with the equation $x^r + y^r = Cz^p$ which are defined over totally real subfields of $\mathbb{Q}(\zeta_r)$. Here, ζ_r denotes a primitive r-th root of unity in $\mathbb{C}$. In addition, a construction of Kraus attaches a hyperelliptic curve with nice arithmetic properties to any non-trivial primitive solution.

For the case $r = 7$, we therefore have the following three different Frey objects associated with a non-trivial primitive solution (a, b, c) of the equation $x^7 + y^7 = Cz^p$:

- (Darmon, [Kra99, §4.5.1.3]) A Frey curve over $\mathbb{Q}$:
$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$
where
$$\begin{aligned} a_2 &= -(a-b)^2, \\ a_4 &= -2a^4 + a^3b - 5a^2b^2 + ab^3 - 2b^4, \\ a_6 &= a^6 - 6a^5b + 8a^4b^2 - 13a^3b^3 + 8a^2b^4 - 6ab^5 + b^6. \end{aligned}$$
See also [Fre15, p. 629] where the curve $E_{(a,b)}$ is isomorphic to this curve via the change of variables given by $x = X/6^2 - a_2/3$ and $y = Y/6^3$.
- (Freitas, [Fre15, p. 619]) A Frey curve over the totally real cubic field $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$:
$$y^2 = x(x - A_{a,b})(x + B_{a,b}),$$
where for $i = 1, 2$, we have $\omega_i = \zeta_7^i + \zeta_7^{-i}$ and
$$\begin{aligned} A_{a,b} &= (\omega_2 - \omega_1)(a+b)^2 \\ B_{a,b} &= (2 - \omega_2)(a^2 + \omega_1 ab + b^2). \end{aligned}$$
- (Kraus, [Kra98a]; see also [BCDF23a]) A Frey hyperelliptic curve over $\mathbb{Q}$:
$$y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7.$$

This is a very rich situation! How the modular method extends to deal with it is the topic of current research (see [BCDF23a, BCDF23b]) and of the article *Darmon's Program: A survey* by Imin Chen and Angelos Koutsianas in this volume.

References

[BCDF23a] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. On Darmon's program for the generalized Fermat equation, I. ArXiv preprint, arxiv.org/abs/2205.15861, 2023.

[BCDF23b] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. On Darmon's program for the generalized Fermat equation, II. ArXiv preprint, arxiv.org/abs/2308.07062, 2023.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BCDY15] 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.

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[Beu98] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[Bil08] Nicolas Billerey. Formes homogènes de degré 3 et puissances p-ièmes. *J. Number Theory*, 128(5):1272–1294, 2008.

[Bil16] Nicolas Billerey. On some remarkable congruences between two elliptic curves. ArXiv preprint, arxiv.org/abs/1605.09205, 2016.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[Bru00] Nils Bruin. On powers as sums of two cubes. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 169–184. Springer, Berlin, 2000.

[CS09] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322(3):638–656, 2009.

[Dah08] Sander R. Dahmen. *Classical and modular methods applied to Diophantine equations*. PhD thesis, University of Utrecht, 2008.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[DT94] Fred Diamond and Richard Taylor. Nonoptimal levels of mod l modular representations. *Invent. Math.*, 115(3):435–462, 1994.

[Fre15] Nuno Freitas. Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$. *Math. Z.*, 279(3-4):605–639, 2015.

[Fre16] Nuno Freitas. On the Fermat-type equation $x^3 + y^3 = z^p$. *Comment. Math. Helv.*, 91(2):295–304, 2016.

[Kra98a] Alain Kraus. On the equation $x^r + y^r = z^p$. Notes for a talk given at IEM, Universität Duisburg-Essen, 1998.

[Kra98b] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[Kra99] Alain Kraus. On the equation $x^p + y^q = z^r$: a survey. *Ramanujan J.*, 3(3):315–333, 1999.

[Lem19] Pedro Lemos. Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. *Trans. Amer. Math. Soc.*, 371(1):137–146, 2019.

[LMF23] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2023. [Online; accessed 23 April 2023].

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mom84] Fumiyuki Momose. Rational points on the modular curves $X_{\mathrm{split}}(p)$. *Compositio Math.*, 52(1):115–137, 1984.

[Rib90] Kenneth A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Rib97] Kenneth A. Ribet. On the equation $a^p+2^\alpha b^p+c^p = 0$. *Acta Arith.*, 79(1):7–16, 1997.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Laboratoire de Mathématiques Blaise Pascal, Université Clermont Auvergne et CNRS, Campus universitaire des Cézeaux, 3, place Vasarely, 63178 Aubière Cedex, France

Email address: nicolas.billerey@uca.fr