

## Generalized Fermat equations (d'après Halberstadt-Kraus)

Pierre Charollois

**A**bstract. In this paper, we summarize the work of Halberstadt and Kraus on generalized Fermat equations of the shape  $ax^n + by^n = cz^n$ . In particular, we sketch the proof that, for fixed odd coprime integer coefficients  $a, b, c$ , there is a set of primes  $n$  of positive density for which only trivial solutions  $(x, y, z)$  occur.

### C

1. Introduction	83
2. Preliminary section	84
3. Proof of Theorems 1.1 and 1.2	85
4. Proof of the symplectic criterion	87
5. Limitations of the method	88
References	89

### 1. Introduction

Our purpose is to publicize the statement and the proof of the following theorem [HK02, théorème 2.1]:

**T**heorem 1.1 (Halberstadt-Kraus (2002)). *Let  $a, b, c$  be odd pairwise coprime integers. Then there is a set of primes  $\mathcal{P} = \mathcal{P}(a, b, c)$  of positive density such that if  $p \in \mathcal{P}$ , then the equation*

$$(1) \quad ax^p + by^p + cz^p = 0$$

*has only trivial rational solutions  $(x, y, z) \in \mathbb{Q}^3$ .*

A solution  $(x, y, z)$  is called trivial in our context if  $xyz = 0$ .

One must point out that before Wiles's work, even the case  $a = b = c = 1$  was unknown. Theorem 1.1 exhibits the first infinite family of generalized Fermat equations having only trivial solutions.

Note that the set of primes  $\mathcal{P}$  will be given by congruence conditions. These can be made more precise and explicit for particular choices of triples  $(a, b, c)$ . For instance, the

---

2000 *Mathematics Subject Classification*. Primary 11D41, Secondary 11F11, 11G05.

proof of Theorem 1.1 yields the following, providing a partial answer to a question raised by Serre [Ser87, p.204]:

T 1.2. *If  $p \geq 7$  is a prime number satisfying  $p \not\equiv 1 \pmod{12}$ , the equation*

$$x^p + 3y^p + 5z^p = 0$$

*has only trivial solutions over  $\mathbb{Q}$ . So does the equation*

$$x^p + y^p + 15z^p = 0.$$

The proof of these theorems relies crucially on the modularity theorem for elliptic curves from Wiles and his followers, as well as Ribet's level-lowering theorem. Another expository paper on the application of these modular techniques to Diophantine equations can be found in [Sik07].

It is a pleasure to thank Henri Darmon and Alain Kraus for their help and their support.

## 2. Preliminary section

In this section, we give some classical necessary preparation for the theorems. Namely, following the lines of the exposition in section 4 of [Dar], we attach successively three objects to a hypothetical solution  $(x, y, z)$  of (1):

1. A Frey curve  $E_0$  whose invariants can be computed.
2. A representation  $\rho$  describing the action of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  on the  $p$ -division points of  $E_0$ .
3. Corresponding to  $\rho$  is a cusp form  $f$  of weight 2 for  $\Gamma_0(N)$ , where  $N$  divides the conductor of  $E_0$ . We then reduce to the case where  $f$  has integer coefficients.

After this preparation, the point is to be able to discard all such modular forms. Halberstadt and Kraus manage to do so using their so-called "symplectic criterion" which will be explained in detail in the last section.

We proceed by contradiction and start from a hypothetical non-trivial solution

$$(x, y, z) \in \mathbb{Q}^3$$

of equation (1). Adjusting  $p^{\text{th}}$ -powers and clearing denominators, we can assume without loss of generality that  $x, y, z$  are coprime integers, and that  $a, b$  and  $c$  do not contain any  $p^{\text{th}}$ -powers.

One can reorder and label the three integers  $ax^p, by^p$  and  $cz^p$  by  $A, B$  and  $C$  respectively so that  $B$  is the only even integer among them, and  $A \equiv \pm 1 \pmod{4}$ . By adjusting the signs of our solution, we are reduced to the case where  $A \equiv -1 \pmod{4}$ . To this data  $A + B + C = 0$  we attach the Frey curve over  $\mathbb{Q}$

$$E_0 : Y^2 = X(X - A)(X + B).$$

The computation of its invariants on this model using classical formulae [Sil86, p.46] leads to:

$$\tilde{c}_4 = 16(A^2 + AB + B^2) \quad \text{and} \quad \tilde{\Delta} = 16(abc)^2(xy z)^{2p} = 16(ABC)^2.$$

If  $\ell \neq 2$  is a prime dividing  $\tilde{\Delta}$ , it cannot divide  $\tilde{c}_4$ . Hence  $E_0$  is semi-stable outside 2.

To study the reduction of  $E_0$  at  $\ell = 2$ , let us change the variables to  $X' = 4X$  and  $Y' = 8Y + 4X$ . Assuming that 16 divides  $B$  (since we will assume that  $p \geq 5$ , even 32 divides  $B$ ), one obtains a global minimal Weierstrass equation for  $E_0$  over  $\mathbb{Q}$ . At this point the minimal discriminant turns out to be

$$(2) \quad \Delta(E_0) = 2^{-8}(ABC)^2,$$

and  $c_4(E_0)$  is odd. Finally,  $E_0$  is also semi-stable at  $\ell = 2$ , and thus is semi-stable. Its conductor is the radical of the discriminant, that is (because 32 divides  $B$ )

$$N_{E_0} = \prod_{\ell \text{ prime}, \ell \nmid ABC} \ell.$$

**Key observation:** Notice the factor  $2^{-8}$  involved in formula (2) for the minimal discriminant. The “minus sign” of the exponent turns out to be crucial in the proof of Theorem 1.1.

The set of  $p$ -torsion points  $E_0[p]$  of  $E_0(\bar{\mathbb{Q}})$  forms a  $\mathbb{F}_p$ -vector space of dimension 2. The absolute Galois group  $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  acts naturally on  $E_0[p]$ . Thus we obtain a representation

$$\rho : G_{\mathbb{Q}} \rightarrow \text{Aut}(E_0[p]) \simeq GL_2(\mathbb{F}_p).$$

If  $\rho$  is reducible, then  $E_0$  contains a rational subgroup of order  $p$ . This cannot be the case if  $p \geq 17$  because of the boundedness result of Mazur [Maz77, Th. 8] for the torsion of elliptic curves over  $\mathbb{Q}$ . Hence  $\rho$  is irreducible if  $p$  is large enough. Notice how our original Diophantine question has been transferred to this new Diophantine problem solved by Mazur. For more on this result, see [Reb] in this volume. This bound  $p \geq 17$  is sufficient for us to prove Theorem 1.1. Nevertheless, a more precise result is given in [Kra97, Lemma 4] showing that  $\rho$  is irreducible as soon as  $p \geq 5$ .

Serre [Ser87] associates to such a representation a conductor  $N|N_{E_0}$ . In our context we have

$$N = 2 \text{rad}(abc) := 2 \prod_{\ell \text{ prime}, \ell \nmid abc} \ell.$$

By the result of Wiles [Wil95], the semi-stable elliptic curve  $E_0$  is modular: the function on the upper half-plane  $\tau \mapsto \sum_{n \geq 1} a_n(E_0)q^n$  belongs to the space  $S_2(\Gamma_0(N_{E_0}))$  of cuspidal modular forms of weight 2 on  $\Gamma_0(N_{E_0})$ .

The “lowering the level” Theorem of Ribet [Rib90] ensures that the representation  $\rho$  is then modular: there exists a newform  $f = q + \sum_{n \geq 2} a_n q^n$  of weight 2 on  $\Gamma_0(N)$  (where  $N$  now depends only on  $abc$  and not on  $(x, y, z)$  or  $p$ ) and a place  $\mathfrak{p}$  of  $K_f = \mathbb{Q}(a_2, \dots, a_n, \dots)$  above  $p$  such that

$$(3) \quad \begin{array}{ll} i) & a_\ell \equiv a_\ell(E_0) \pmod{\mathfrak{p}} \text{ if } \ell \nmid N_{E_0} p \\ ii) & a_\ell \equiv \pm(\ell + 1) \pmod{\mathfrak{p}} \text{ if } \ell \mid N_{E_0} \text{ and } \ell \nmid pN. \end{array}$$

In the case of Fermat’s last Theorem, one could show that  $N = 2$  and the previous results were enough (!) to derive a contradiction since there is no cusp form of weight 2 and this level. In proving Theorem 1.1 and 1.2, Halberstadt and Kraus needed to refute the existence of such a form using an additional argument.

### 3. Proof of Theorems 1.1 and 1.2

Let  $f$  be the modular form of level  $N$  given by the previous construction. Both  $f$  and  $N$  do not depend on the solution  $(x, y, z)$  nor on  $p$ . We first reduce to the case where the modular form  $f$  has coefficients in  $\mathbb{Z}$ . Otherwise, the finite extension  $K = K_f$  of  $\mathbb{Q}$  has degree bounded by  $g = \dim_{\mathbb{Q}}(S_2^{\text{new}}(\Gamma_0(N)))$ . Let  $a_\ell \notin \mathbb{Z}$  for the smallest possible prime  $\ell$ . Both  $g$  and  $\ell$  do not depend on  $p$ . We can assume that  $\ell$  does not divide  $pN$  because  $a_\ell$  would be 0,  $\pm 1$ . Thus in the previous case  $i)$   $p$  divides  $N_{K/\mathbb{Q}}(a_\ell - a_\ell(E_0))$ , while in case  $ii)$   $p$  divides  $N_{K/\mathbb{Q}}(a_\ell \pm (\ell + 1))$ . The Hasse bound gives  $|a_\ell(E_0)| \leq 2\sqrt{\ell}$ , while Weil-Deligne’s bound shows that  $|\sigma(a_\ell)| \leq 2\sqrt{\ell}$  for each real embedding  $\sigma$  of  $K$ .

In any case  $p$  is bounded by a number depending only on  $a, b, c$ . Therefore, choosing large enough  $p$  we can make sure that  $f$  has integer coefficients. Under this hypothesis, the Eichler-Shimura theory provides an elliptic curve  $E'$  over  $\mathbb{Q}$  of conductor  $N$  such that the Hasse-Weil function of  $E'$  is  $\sum a_n n^{-s}$ .

For almost all primes  $\ell$ , the congruence relations (3) impose that  $a_\ell \equiv a_\ell(E_0) \pmod{p}$ . This is enough to show that the Galois modules  $E[p]$  and  $E'[p]$  are isomorphic. For, if  $\ell \nmid pN_{E_0}$  the Frobenius element  $\text{Frob}_\ell$  in  $\text{Aut}(E[p])$  has trace (resp. determinant)  $a_\ell \pmod{p}$  (resp.  $\ell \pmod{p}$ ). The same occurs with  $E'$ . By the Chebotarev density theorem, this implies that an element  $g \in G_{\mathbb{Q}}$  has the same characteristic polynomial when it acts on  $E[p]$  or  $E'[p]$ . Thus the two representations of  $G_{\mathbb{Q}}$  in the  $p$ -division points of  $E$  and  $E'$  have isomorphic semi-simplifications. Our assertion follows since  $E[p]$  is irreducible.

At this point, the following key proposition is in order:

**P** 3.1 ([KO92], Prop. 2). *Let  $E$  and  $E'$  be two elliptic curves over  $\mathbb{Q}$  with minimal discriminants  $\Delta$  and  $\Delta'$ , and let  $p$  be a prime number.*

*Assume that the groups of  $p$ -torsion points  $E[p]$  and  $E'[p]$  are isomorphic as  $G_{\mathbb{Q}}$ -modules. Assume also that  $E$  and  $E'$  have multiplicative reduction at a common prime  $\ell \neq p$  such that  $p$  does not divide the valuation  $v_\ell(\Delta)$ . Then we have*

- a) *The prime  $p$  does not divide  $v_\ell(\Delta')$ .*
- b) *The following conditions are equivalent:*
  - (i) *there is a symplectic (viz. compatible with the Weil pairing on  $E[p]$  and  $E'[p]$ ) isomorphism between these two representations.*
  - (ii) *the quotient  $v_\ell(\Delta)/v_\ell(\Delta')$  is a square in  $(\mathbb{Z}/p\mathbb{Z})^*$ .*

We postpone the proof of this ‘‘symplectic criterion’’ to the last section. The way it implies Theorems 1.1 and 1.2 is a bit tricky. Up to isogeny, there is only a finite number of elliptic curves over  $\mathbb{Q}$  of conductor  $N$ , say  $E_1, \dots, E_h$ . We label our previous curve  $E' = E_j$  among them, and we want to apply the criterion to the pair  $(E_0, E_j)$ .

Recall that  $E_0$  has minimal discriminant

$$\Delta(E_0) = 2^{-8}(abc)^2(xyz)^{2p}.$$

We can assume that  $|abc| > 2$  by Fermat’s last theorem. Now we choose a first prime  $\ell_1$  dividing the odd integer  $abc$ , and  $\ell_2 = 2$ . If  $p$  is large enough,  $p$  divides neither  $v_{\ell_1}(\Delta(E_0))$  nor  $v_2(\Delta(E_0))$ .

Let us emphasise that we are not going to decide whether or not  $E_j$  and  $E_0$  are symplectically isomorphic. But in both cases, Proposition 3.1.b implies that *the product of the two terms*

$$\frac{v_{\ell_1}(\Delta(E_0))}{v_{\ell_1}(\Delta(E_j))} \pmod{p} \quad \text{and} \quad \frac{v_2(\Delta(E_0))}{v_2(\Delta(E_j))} \pmod{p}$$

*is a square mod  $p$  because both terms are simultaneously squares or non-squares.*

Equality (2) shows that the numerator of this product is

$$\begin{aligned} v_{\ell_1}(\Delta(E_0))v_2(\Delta(E_0)) &\equiv 2 v_{\ell_1}(abc)(-8) \pmod{p} \\ &\equiv -16 v_{\ell_1}(abc) \pmod{p}. \end{aligned}$$

Therefore the symplectic criterion implies that the integer  $n_j$  defined by

$$n_j = -v_{\ell_1}(abc)v_{\ell_1}(\Delta(E_j))v_2(\Delta(E_j))$$

has to be a square mod  $p$ .

Hence if  $p \gg_{a,b,c} 0$  is a prime satisfying

$$(4) \quad \left(\frac{n_j}{p}\right) = -1 \quad \text{for all } j = 1, \dots, h,$$

the equation  $ax^p + by^p + cz^p = 0$  has no non-trivial solution. It remains to show that these conditions are simultaneously satisfied on a set of positive density. To do this, let  $p$  be a prime such that

- i)  $-1$  is a non-square mod  $p$ ;
- ii) each prime divisor of  $n_j$  ( $j = 1, \dots, h$ ) is a square mod  $p$ .

The previous two conditions define a subset of  $\mathcal{P}$  which has positive density by Chebotarev's Theorem. Theorem 1.1 follows.  $\square$

*Proof of Theorem 1.2 (sketch):*

Both equations  $x^p + 3y^p + 5z^p = 0$  and  $x^p + y^p + 15z^p = 0$  have coefficients  $a, b, c$  satisfying  $abc = 15$ . The existence of a putative non-trivial rational solution with  $p \geq 7$  leads to cusp forms of level  $N = 30$ . There is only one such newform of weight 2. Thus the Galois module  $E_0[p]$  has to be isomorphic to  $E_1[p]$ , where  $E_1$  is an elliptic curve of conductor 30, say 30A1 in Cremona's tables. The minimal discriminant of  $E_1$  is

$$\Delta(E_1) = -2^4 3^3 5.$$

Then we choose  $\ell_1 = 2$  and  $\ell_2 = 5$  to deduce that  $n_1 = -1$  must be a square mod  $p$ . But we could also use  $\ell_2 = 3$  and obtain that  $-3$  must be a square mod  $p$ .

The only primes  $p$  satisfying both conditions are those congruent to 1 mod 12. If we avoid such primes, there can be no non-trivial solutions. Therefore we obtain the conclusion of Theorem 1.2, at least for  $p$  large enough. The lower bound for  $p$  can be made precise using the explicit formulations of [Kra97].  $\square$

#### 4. Proof of the symplectic criterion

We conclude this paper by proving the key Proposition 3.1, following closely the lines of [KO92]. The proof consists of a local study of  $E$  and  $E'$  at the place  $\ell$ , for which the Tate curve model can be used to make the computations explicit.

Let  $K = \mathbb{Q}_\ell^{\text{nr}}$  denote the maximal unramified extension of  $\mathbb{Q}_\ell$ . Both  $E$  and  $E'$  having multiplicative reduction over  $\mathbb{Q}$  at  $\ell$ , their  $j$ -invariant is not an integer in  $K$ . We deduce from [Sil94, Th. V.5.3] that  $E$  is uniformized over  $K$  by a Tate curve  $\mathbb{G}_m/q^{\mathbb{Z}}$ , where  $q$  in  $K$  has valuation  $e = -v_\ell(j(E)) = v_\ell(\Delta)$ . The same is true for  $E'$ , with a  $q' \in K$  of valuation  $e' = v_\ell(\Delta')$ .

The given isomorphism and the previous uniformizations combine to provide a  $\text{Gal}(\bar{K}/K)$ -module isomorphism  $\Psi$  between the  $p$ -division points  $E[p]$  of  $\bar{K}^*/q^{\mathbb{Z}}$  and those  $E'[p]$  of  $\bar{K}^*/q'^{\mathbb{Z}}$ .

Let us describe the effect of  $G_K = \text{Gal}(\bar{K}/K)$  and  $\Psi$  on a basis of  $E[p]$ , following [Sil94, Prop. 5.6.1]. First note that  $K$  contains the  $p^{\text{th}}$ -roots of unity, and let us fix  $\zeta$  a primitive one. Fix also  $\gamma \in \bar{K}$ , a  $p^{\text{th}}$ -root of  $q$ . Then  $\{\zeta^j q^{\mathbb{Z}}, \gamma q^{\mathbb{Z}}\}$  forms a basis for  $E[p]$ . The Galois group  $G_K$  acts transitively on the  $p$  conjugates  $\{\zeta^j \gamma, 1 \leq j \leq p\}$ . Hence there is a distinguished element  $\sigma \in G_K$  which satisfies  $\sigma(\zeta) = \zeta \gamma$ , i.e. whose matrix is  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .

As  $G_K$  fixes  $\zeta$ , it acts trivially on  $E[p]$  iff  $\gamma$  is in  $K$ , that is, iff  $p$  divides  $e = v_\ell(q)$ . The same assertion holds for  $E'[p]$  and  $e'$ . These two Galois modules are isomorphic and  $p$

does not divide  $e$  by assumption, so we conclude that  $p$  cannot divide  $e'$ , which is assertion  $a$ ). Hence there are integers  $m$  and  $n$  such that

$$e' = ne + mp.$$

We detail how  $\Psi$  acts on our basis. Since  $q'/(q^{nlmp})$  is a unit in  $K$ , it has a  $p^{\text{th}}$ -root  $\alpha \in K$ . We obtain a  $p^{\text{th}}$ -root of  $q'$  by setting  $\gamma' = \gamma^{nlm}\alpha$ , completing a basis  $\{\zeta q'^{\mathbb{Z}}, \gamma' q'^{\mathbb{Z}}\}$  of  $E'[p]$ .

Observe that for all  $g \in G_K$ , we have  $\Psi(\zeta q'^{\mathbb{Z}})^g = \Psi((\zeta q'^{\mathbb{Z}})^g) = \Psi(\zeta q'^{\mathbb{Z}})$  because  $\Psi$  is compatible with  $G_K$ . Therefore the matrix of  $\Psi$  with respect to the previous basis is upper triangular, say of the form  $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ .

The very definitions of  $\sigma$  and  $\gamma'$  lead to the identity  $\sigma(\gamma') = \sigma(\gamma)^n \sigma(l^m \alpha) = \zeta^n \gamma'$ . Compatibility between  $\Psi$  and  $\sigma$  can be written in matrix terms as follows:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Identification of upper right entries shows the intermediate identity

$$(5) \quad a = nd.$$

Now we turn to the Weil pairing. It is a bilinear alternate pairing satisfying the following identities on  $E[p]$  and  $E'[p]$  respectively:

$$B(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}}) = \zeta, \quad B'(\gamma q'^{\mathbb{Z}}, \zeta q'^{\mathbb{Z}}) = \zeta.$$

Assuming that  $\Psi$  is a symplectic isomorphism, we obtain

$$\zeta = B(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}}) = B'(\Psi(\gamma q^{\mathbb{Z}}), \Psi(\zeta q^{\mathbb{Z}})) = B'(\zeta^b \gamma^d q'^{\mathbb{Z}}, \zeta^a q'^{\mathbb{Z}}) = \zeta^{ad}.$$

It follows that  $ad \equiv 1 \pmod{p}$ , or  $nd^2 \equiv 1 \pmod{p}$  by (5) and  $n$  is a square modulo  $p$ .

Reciprocally, if  $n$  is a square modulo  $p$ , there is an integer  $r$  such that  $r^2 nd^2 = 1 \pmod{p}$ . It can be easily checked that the  $r^{\text{th}}$ -power  $\Psi^r$  defines the required *symplectic* isomorphism between the Tate curves, hence  $E$  and  $E'$  are symplectically isomorphic.  $\square$

## 5. Limitations of the method

The paper [HK02] presents the symplectic method and two others (called the reduction method and the decomposition method) to handle the case of different generalized Fermat equations. Even if Theorem 1.1 is successful, as it solves an infinite family of Fermat equations, many questions are still open.

For instance, the remaining case  $p = 1 \pmod{12}$  in Theorem 1.2 cannot be settled using the methods of Halberstadt and Kraus. This would provide a complete answer to the question raised by Serre.

The authors also mention (Exemple 2.12) the case of the curve

$$16x^7 + 87y^7 + 625z^7 = 0.$$

Denote by  $E_0$  the corresponding Frey curve and by  $E_1$  the elliptic curve 435C2. The symplectic criterion cannot ensure that  $\rho_7^{E_0}$  and  $\rho_7^{E_1}$  are not isomorphic since  $E_0$  and  $E_1$  have discriminants  $3^2 5^8 29^2 (xyz)^{14}$  and  $3^4 5^2 29^2$  respectively.

Moreover, the aim of their three methods is to show that the set of solutions of some generalized Fermat equation is trivial. Thus the case of the Diophantine equation  $ax^p + by^p + cz^p = 0$  with  $a + b + c = 0$  falls out of their scope because the non-trivial solution  $(1, 1, 1)$  has to be considered.

Nevertheless, a result in this setting has been obtained in [DM97], providing an optimistic conclusion to this section and to this note:

**T** 5.1 (Darmon-Merel (1997) [DM97]). *Let  $n \geq 3$  be an arbitrary integer. Then the equation*

$$x^n + y^n - 2z^n = 0$$

*has no integer solutions  $(x, y, z) \in \mathbb{Z}^3$  with  $|xyz| > 1$ .*

### References

- [Dar] H. Darmon, *Rational points on curves*, in this volume.
- [DM97] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100. MR 1468926 (98h:11076)
- [HK02] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. MR 1915212 (2003h:11068)
- [KO92] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), no. 2, 259–275. MR 1166121 (93e:11074)
- [Kra97] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161. MR 1611640 (99g:11039)
- [Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR 488287 (80c:14015)
- [Reb] M. Rebolledo, *Merel's theorem for the boundedness of the torsion of elliptic curves*, in this volume.
- [Rib90] K. A. Ribet, *On modular representations of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476. MR 1047143 (91g:11066)
- [Ser87] J.-P. Serre, *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$* , Duke Math. J. **54** (1987), no. 1, 179–230. MR 885783 (88g:11022)
- [Sik07] S. Siksek, *The modular approach to Diophantine equations*, Graduate Texts in Mathematics, vol. 240, ch. 15, pp. xxiv+596, Springer, New York, 2007, a book by H. Cohen. MR 2312338 (2008e:11002)
- [Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210 (87g:11070)
- [Sil94] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368 (96b:11074)
- [Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035 (96d:11071)

I { J }, U { P } 6, E { C } 247 - 4,  
 J - 75252 P C F  
 E-mail address: charollois@math.jussieu.fr