HAL
open science

Le théorème de Fermat sur certains corps de nombres totalement réels

Alain Kraus

To cite this version:

Alain Kraus. Le théorème de Fermat sur certains corps de nombres totalement réels. Algebra & Number Theory, 2019, 13 (2), pp.301-332. 10.2140/ant.2019.13.301 . hal-02089717

HAL Id: hal-02089717

https://hal.sorbonne-universite.fr/hal-02089717v1

Submitted on 8 Apr 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Algebra & Number Theory

Volume 13
2019
No. 2

Le théorème de Fermat sur certains corps de nombres totalement réels

Alain Kraus

msp

ALGEBRA AND NUMBER THEORY 13:2 (2019)
dx.doi.org/10.2140/ant.2019.13.301

Le théorème de Fermat sur certains corps de nombres totalement réels

Alain Kraus

Soit K un corps de nombres totalement réel. Pour tout nombre premier $p \geq 5$, notons F_p la courbe de Fermat d'équation $x^p + y^p + z^p = 0$. Sous l'hypothèse que 2 est totalement ramifié dans K, on établit quelques résultats sur l'ensemble $F_p(K)$ des points de F_p rationnels sur K. On obtient un critère pour que le théorème de Fermat asymptotique soit vrai sur K, critère relatif à l'ensemble des newforms modulaires paraboliques de Hilbert sur K, de poids parallèle 2 et de niveau l'idéal premier au-dessus de 2. Il peut souvent se tester simplement numériquement, notamment quand le nombre de classes restreint de K vaut 1. Par ailleurs, en utilisant la méthode modulaire, on démontre le théorème de Fermat de façon effective, sur certains corps de nombres dont les degrés sur $\mathbb{Q}$ sont 3, 4, 5, 6 et 8.

Let K be a totally real number field. For all prime number $p \geq 5$, let us denote by F_p the Fermat curve of equation $x^p + y^p + z^p = 0$. Under the assumption that 2 is totally ramified in K, we establish some results about the set $F_p(K)$ of points of F_p rational over K. We obtain a criterion so that the asymptotic Fermat's last theorem is true over K, criterion related to the set of Hilbert modular cuspidal newforms over K, of parallel weight 2 and of level the prime ideal above 2. It is often simply testable numerically, particularly if the narrow class number of K is 1. Furthermore, using the modular method, we prove Fermat's last theorem effectively, over some number fields whose degrees over $\mathbb{Q}$ are 3, 4, 5, 6 and 8.

1. Introduction

Soient K un corps de nombres totalement réel et $p \geq 5$ un nombre premier. Notons

$$F_p : x^p + y^p + z^p = 0 \tag{1-1}$$

la courbe de Fermat d'exposant p. Dans le cas où 2 est totalement ramifié dans K, on se propose de faire quelques remarques sur la description de l'ensemble $F_p(K)$ des points de F_p rationnels sur K. On se préoccupera en particulier de cette description quand de plus le nombre de classes restreint de K vaut 1.

Adoptons la terminologie selon laquelle $F_p(K)$ est trivial, si pour tout point $(x, y, z) \in F_p(K)$ on a $xyz = 0$. Tel est le cas si $K = \mathbb{Q}$ [Wiles 1995]. On dira que le théorème de Fermat asymptotique est vrai sur K, si $F_p(K)$ est trivial dès que p est plus grand qu'une constante qui ne dépend que de K. Parce que K ne contient pas les racines cubiques de l'unité, la conjecture abc sur K implique le théorème de Fermat asymptotique sur K (cf. [Browkin 2006]).

MSC2010 : primary 11D41; secondary 11G05, 11R37.
Mots-clefs : Fermat equation, number fields, elliptic curves, modular method.

Au cours de ces dernières années, les principaux résultats qui ont été établis concernant l'équation de Fermat sur les corps totalement réels sont dus à Freitas et Siksek. Ils ont notamment obtenu un critère permettant parfois de démontrer le théorème de Fermat asymptotique sur un corps totalement réel [Freitas et Siksek 2015a, Theorem 3]. En particulier, ils en ont déduit le théorème de Fermat asymptotique pour une proportion de $5/6$ de corps quadratiques réels. Ils ont par ailleurs démontré que pour $K = \mathbb{Q}(\sqrt{m})$, où $m \leq 23$ est un entier sans facteurs carrés, autre que 5 et 17, l'ensemble $F_p(K)$ est trivial pour tout $p \geq 5$ [Freitas et Siksek 2015b]. Le cas où $m = 2$ avait déjà été établi dans [Jarvis et Meekin 2004].

1.1. ***Le critère de Freitas et Siksek.*** Énonçons leur résultat dans le cas où 2 est totalement ramifié dans K.

On notera dans toute la suite, d le degré de K sur $\mathbb{Q}$, O_K l'anneau d'entiers de K et $\mathscr{L}$ l'idéal premier de O_K au-dessus de 2. On a $2O_K = \mathscr{L}^d$.

Soient $v_{\mathscr{L}}$ la valuation sur K associée à $\mathscr{L}$ et $U_{\mathscr{L}}$ le groupe des $\{\mathscr{L}\}$-unités de K. Posons

$$S = \{a \in U_{\mathscr{L}} \mid 1 - a \in U_{\mathscr{L}}\}.$$

Désignons par (**FS**) la condition suivante :

(**FS**) pour tout $a \in S$, on a

$$|v_{\mathscr{L}}(a)| \leq 4d. \tag{1-2}$$

Leur critère est le suivant :

Théorème 1. *Supposons que la condition* (**FS**) *soit satisfaite par K. Alors, le théorème de Fermat asymptotique est vrai sur K.*

L'ensemble S est fini [Siegel 1929]. Avec les travaux de Smart, on dispose d'algorithmes permettant d'expliciter S, sous réserve que le groupe $U_{\mathscr{L}}$ soit connu [Smart 1998]. Dans ce cas, la condition (**FS**) est donc en principe testable sur K. Cela étant, la détermination de S n'est pas pour l'instant implémentée dans des logiciels de calcul et expliciter S reste un travail généralement important. Par exemple, pour le sous-corps totalement réel maximal $\mathbb{Q}(\mu_{16})^+$ du corps cyclotomique des racines 16-ièmes de l'unité, S est de cardinal 585 [Freitas et Siksek 2015a, 1.3]. On peut vérifier que la condition (**FS**) est satisfaite, en particulier le théorème de Fermat asymptotique est vrai sur le corps $\mathbb{Q}(\mu_{16})^+$ [loc. cit.].

Dans l'objectif de démontrer le théorème de Fermat asymptotique sur certains corps de nombres, dans lesquels 2 est totalement ramifié, on va introduire ci-dessous une nouvelle condition, qui d'un point de vue numérique a l'avantage, à ce jour, de pouvoir se tester souvent simplement sur machine. On établit dans le théorème 2 qu'elle est équivalente à (**FS**), moyennant une hypothèse de modularité pour certaines courbes elliptiques sur K.

1.2. ***La condition*** **(C).** Le nombre premier 2 étant supposé totalement ramifié dans K, désignons par $\mathcal{H}$ l'ensemble des newforms modulaires paraboliques de Hilbert sur K, de poids parallèle 2 et de niveau $\mathscr{L}$. C'est un système fini libre sur $\mathbb{C}$. Pour tout $\mathfrak{f} \in \mathcal{H}$ et tout idéal premier non nul $\mathfrak{q}$ de O_K, notons $a_{\mathfrak{q}}(\mathfrak{f})$ le coefficient de Fourier de $\mathfrak{f}$ en $\mathfrak{q}$. C'est un entier algébrique. Le sous-corps $\mathbb{Q}_{\mathfrak{f}}$ de $\mathbb{C}$ engendré par les

coefficients $a_{\mathfrak{q}}(\mathfrak{f})$ est une extension finie de $\mathbb{Q}$. C'est un corps totalement réel ou un corps CM. (Voir par exemple [Cremona et Dembélé 2014; Dembélé et Voight 2013].)

Pour tout idéal premier $\mathfrak{q}$ de O_K, notons $\mathrm{Norm}(\mathfrak{q})$ sa norme sur $\mathbb{Q}$.

La condition est la suivante :

(**C**) pour tout $\mathfrak{f} \in \mathcal{H}$ tel que $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, il existe un idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, tel que l'on ait

$$a_{\mathfrak{q}}(\mathfrak{f}) \not\equiv \mathrm{Norm}(\mathfrak{q}) + 1 \pmod 4. \tag{1-3}$$

Elle est en apparence moins simple que la condition (**FS**), mais on peut généralement la tester en utilisant le logiciel de calcul `Magma` [Bosma et al. 1997], disons si $d \leq 8$ et si le discriminant de K n'est pas trop grand. Dans le cas où $d \leq 6$, on dispose également de tables de newforms décrivant $\mathcal{H}$, qui sont directement implémentées dans [LMFDB 2013].

Signalons par ailleurs que pour établir le théorème de Fermat asymptotique sur K de façon effective, la détermination de $\mathcal{H}$ est, comme on le verra, a priori indispensable dans la mise en œuvre de la méthode modulaire.

À titre indicatif, le corps quadratique réel de plus petit discriminant pour lequel la condition (**C**) n'est pas satisfaite est $K = \mathbb{Q}(\sqrt{114})$. Il existe une courbe elliptique sur K, de conducteur $\mathscr{L}$, ayant tous ses points d'ordre 2 rationnels sur K [LMFDB 2013], ce qui explique pourquoi (**C**) n'est pas réalisée sur ce corps (théorème 2, lemme 12 et [Freitas et al. 2015]) ; il en est ainsi pour une infinité de corps quadratiques. Par exemple, en utilisant la table 1 de [Freitas et Siksek 2015a], on peut démontrer qu'il existe une infinité de corps quadratiques réels $\mathbb{Q}(\sqrt{m})$, avec m sans facteurs carrés congru à 7 modulo 8, pour lesquels la condition (**C**) n'est pas satisfaite.

Voyons un autre exemple illustrant la condition (**C**). Soit K le sous-corps totalement réel maximal du corps cyclotomique $\mathbb{Q}(\mu_{48})$. C'est le corps totalement réel de degré 8 sur $\mathbb{Q}$ de plus petit discriminant, dans lequel 2 soit totalement ramifié (on peut le vérifier avec les tables de [Voight]). On constate avec `Magma` que l'on a $|\mathcal{H}| = 16$ et que la condition (**C**) est satisfaite par K, car il n'existe pas de newforms $\mathfrak{f} \in \mathcal{H}$ telles que $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$; pour tout $\mathfrak{f} \in \mathcal{H}$, on a $[\mathbb{Q}_{\mathfrak{f}} : \mathbb{Q}] = 4$.

1.3. ***Hypothèse sur le nombre de classes restreint de K.*** Notons h_K^+ le nombre de classes restreint de K. Rappelons que h_K^+ est le degré sur K de l'extension abélienne de K non ramifiée aux places finies maximale.

Malgré de nombreux essais expérimentaux, je ne suis pas parvenu à trouver un exemple de corps de nombres totalement réel K tel que 2 soit totalement ramifié dans K et que $h_K^+ = 1$, sans que la condition (**C**) soit satisfaite. En particulier, a-t-on toujours l'implication

$$2O_K = \mathscr{L}^d \quad \text{et} \quad h_K^+ = 1 \quad \Rightarrow \quad (\mathbf{C}) \quad ?$$

En fait, la réponse est positive si on a $d \in \{1, 2, 4, 8\}$. La raison étant que pour tout entier n, il existe au plus un corps totalement réel K pour lequel on a $d = 2^n$, $2O_K = \mathscr{L}^d$ et $h_K^+ = 1$, à savoir le sous-corps

totalement réel maximal du corps cyclotomique des racines 2^{n+2}-ièmes de l'unité (théorème 6). On indiquera par ailleurs quelques constatations numériques en faveur de cette implication.

Signalons que, comme conséquence du théorème 4, si cette implication était toujours vraie, cela impliquerait le théorème de Fermat asymptotique sur tout corps de nombres totalement réels pour lesquels $2O_K = \mathscr{L}^d$ et $h_K^+ = 1$.

Les hypothèses selon lesquelles $2O_K = \mathscr{L}^d$ et $h_K^+ = 1$ sont très favorables dans l'application de la méthode modulaire pour obtenir des versions effectives du théorème de Fermat sur K. Cela est notamment dû au fait qu'avec ces hypothèses, on peut normaliser toute solution de l'équation de Fermat (1-1) de façon simple (proposition 16). On illustrera cette méthode pour certains corps de nombres de degré $d \in \{3, 4, 5, 6, 8\}$. On établira par exemple que pour le corps $K = \mathbb{Q}(\mu_{16})^+$, l'ensemble $F_p(K)$ est trivial pour tout $p \geq 5$.

Tous les calculs numériques que cet article a nécessités ont été effectués avec les logiciels de calcul `Pari` [PARI 2015] et `Magma`.

Remarque. Pendant la période de l'examen de cet article par le referee, Freitas et Siksek ont démontré une version généralisée de l'implication suggérée ci-dessus ; voir [Freitas et Siksek 2018]. En particulier, compte tenu du théorème 4, si 2 est totalement ramifié dans K et si $h_K^+ = 1$, le théorème de Fermat asymptotique est vrai sur K.

Partie I. Énoncé des résultats

Soit K un corps de nombres totalement réel.

Rappelons qu'une courbe elliptique E/K est dite modulaire s'il existe une newform modulaire parabolique de Hilbert sur K, de poids parallèle 2 et de niveau le conducteur de E, ayant la même fonction L que celle de E.

Conjecturalement, toute courbe elliptique définie sur K est modulaire. Cela est démontré si $K = \mathbb{Q}$ [Wiles 1995; Taylor et Wiles 1995; Breuil et al. 2001] et si K est un corps quadratique [Freitas et al. 2015]. Par ailleurs, à $\overline{K}$-isomorphisme près, l'ensemble des courbes elliptiques sur K qui ne sont pas modulaires est fini [loc. cit.].

2. Les conditions (C) et (FS)

Théorème 2. *Supposons que les deux conditions suivantes soient satisfaites* :

(1) 2 *est totalement ramifié dans* K.

(2) *Toute courbe elliptique définie sur* K, *de conducteur* $\mathscr{L}$, *ayant tous ses points d'ordre* 2 *rationnels sur* K, *est modulaire.*

Alors, *les conditions* (**C**) *et* (**FS**) *sont équivalentes.*

Si K est un corps quadratique dans lequel 2 est totalement ramifié, les conditions (**C**) et (**FS**) sont donc équivalentes.

3. Théorème de Fermat asymptotique

Comme conséquence directe des théorèmes 1 et 2, on obtient l'énoncé suivant :

Théorème 3. *Supposons que les trois conditions suivantes soient satisfaites* :

(1) 2 *est totalement ramifié dans* K.

(2) *Toute courbe elliptique définie sur* K, *de conducteur* $\mathscr{L}$, *ayant tous ses points d'ordre* 2 *rationnels sur* K, *est modulaire.*

(3) *La condition* (**C**) *est satisfaite.*

Alors, le théorème de Fermat asymptotique est vrai sur K.

Remarque. Dans les limites des tables de newforms modulaires de Hilbert sur un corps totalement réel K figurant dans [LMFDB 2013], pour lesquelles 2 est totalement ramifié dans K, on constate les données numériques suivantes. Les corps intervenant dans ces tables sont de degré $d \leq 6$.

(1) Pour $d = 3$, il y a treize tels corps de nombres (à isomorphisme près). Leurs discriminants sont

$$148, 404, 564, 756, 788, 1076, 1300, 1396, 1492, 1524, 1556, 1620, 1940.$$

Pour chacun d'eux, la condition (**C**) est satisfaite.

Cela étant, la condition (**C**) n'est pas toujours satisfaite si $d = 3$. Par exemple, elle ne l'est pas pour le corps $K = \mathbb{Q}(\alpha)$ où $\alpha^3 - 32\alpha + 2 = 0$. En effet, posons $a = 16\alpha$; cet entier est dans S et on a $v_{\mathscr{L}}(a) = 13$. La courbe elliptique E/K d'équation

$$y^2 = x(x-a)(x+1-a)$$

est de conducteur $\mathscr{L}$ et a tous ses points d'ordre 2 rationnels sur K (cf. la démonstration du lemme 12, équation (6-1)). En utilisant le théorème 18, on peut démontrer qu'elle est modulaire. Il existe donc $\mathfrak{f} \in \mathcal{H}$ ayant la même fonction L que celle de E. On a $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ et $\mathfrak{f}$ ne vérifie pas la condition (1-3), d'où notre assertion.

(2) Pour $d = 4$, il y a quinze corps de nombres, dont les discriminants sont

$$2048, 2304, 4352, 6224, 7168, 7488, 11344, 12544, 13824, 14336, 14656, 15952, 16448, 18432, 18688.$$

Pour chacun de ces corps, la condition (**C**) est satisfaite. Excepté pour le corps de discriminant 16448, on a $|\mathcal{H}| = 0$.

Signalons à titre indicatif que pour le corps $K = \mathbb{Q}(\alpha)$ où $\alpha^4 - 12\alpha^2 - 18\alpha - 5 = 0$, la condition (**C**) n'est pas satisfaite. On peut le vérifier comme dans l'alinéa précédent, en considérant l'entier $a = 16(1+\alpha)^2(4+4\alpha+\alpha^2)$. Il appartient à S et on a $v_{\mathscr{L}}(a) = 18$. On constate alors que la courbe elliptique sur K, d'équation $y^2 = x(x-a)(x+1-a)$, est modulaire et que son conducteur est $\mathscr{L}$.

(3) Pour $d = 5$, il y a trois corps de nombres, dont les discriminants sont

$$126032, 153424, 179024,$$

et ils vérifient la condition (**C**). Pour $d = 6$, il n'y a pas de tels corps dans les tables de [LMFDB 2013].

Dans le cas où l'on a $h_K^+ = 1$, on peut s'affranchir de l'hypothèse de modularité :

Théorème 4. *Supposons que les trois conditions suivantes soient satisfaites* :

(1) 2 *est totalement ramifié dans* K.

(2) *On a* $h_K^+ = 1$.

(3) *La condition* (**C**) *est satisfaite.*

Alors, le théorème de Fermat asymptotique est vrai sur K.

4. Question

Certaines constatations numériques concernant les hypothèses faites dans le théorème 4 suggèrent la question suivante :

Question 4.1. Supposons 2 totalement ramifié dans K et $h_K^+ = 1$. La condition (**C**) est-elle toujours satisfaite ? [1]

Proposition 5. *La réponse est positive si on a* $d \in \{1, 2, 4, 8\}$.

C'est une conséquence du résultat qui suit. Sa démonstration repose sur la première assertion du théorème 39 de l'Appendice. Pour tout $n \geq 1$, soit $\mu_{2^{n+2}}$ le groupe des racines 2^{n+2}-ièmes de l'unité. Notons $\mathbb{Q}\big(\mu_{2^{n+2}}\big)^+$ le sous-corps totalement réel maximal de $\mathbb{Q}\big(\mu_{2^{n+2}}\big)$.

Théorème 6. *Soient* n *un entier et* K *un corps de nombres totalement réel, de degré* 2^n *sur* $\mathbb{Q}$, *satisfaisant les conditions suivantes* :

(1) 2 *est totalement ramifié dans* K.

(2) *On a* $h_K^+ = 1$.

Alors, on a $K = \mathbb{Q}\big(\mu_{2^{n+2}}\big)^+$.

Le corps $\mathbb{Q}\big(\mu_{2^{n+2}}\big)^+$ satisfait la première condition. Pour $n \leq 5$, son nombre de classes restreint vaut 1. On conjecture que pour tout n, son nombre de classes vaut 1. Certains résultats récents ont été démontrés dans cette direction [Fukuda et Komatsu 2011].

On peut vérifier directement avec `Magma` que pour $n \leq 3$, la condition (**C**) est satisfaite pour $\mathbb{Q}\big(\mu_{2^{n+2}}\big)^+$, ce qui implique la proposition 5.

1. Comme je l'ai signalé dans la remarque à la fin de l'introduction (page 304), il est maintenant démontré que la réponse à cette question est positive [Freitas et Siksek 2018].

Faits expérimentaux. Indiquons quelques constatations numériques en faveur d'une réponse positive à la question 4.1. En utilisant les tables de Voight, j'ai dressé une liste de corps totalement réels pour lesquels :

(1) $d \in \{3, 5, 6, 7\}$,

(2) 2 est totalement ramifié dans K,

(3) $h_K^+ = 1$,

(4) le discriminant D_K de K est pair plus petit qu'une borne fixée.

Dans le tableau ci-dessous, l'entier N est le nombre de corps totalement réels de degré d et de discriminant D_K pair plus petit que la borne que l'on s'est fixée (à isomorphisme près). Dans la dernière colonne se trouve le nombre de corps pour lesquels 2 est totalement ramifié et $h_K^+ = 1$.

d	Borne sur D_K	N	$2O_K = \mathscr{L}^d$ et $h_K^+ = 1$
3	$21 \cdot 10^3$	378	80
5	$17 \cdot 10^5$	315	23
6	$21 \cdot 10^6$	361	7
7	$207 \cdot 10^6$	32	2

Il y a cent-douze corps K intervenant dans ce tableau pour lesquels $2O_K = \mathscr{L}^d$ et $h_K^+ = 1$. Pour chacun d'eux, on constate avec `Magma` que la condition (**C**) est satisfaite.

Les discriminants de ces cent-douze corps sont explicités ci-dessous. Des éléments primitifs de chacun de ces corps sont déterminés dans les tables de Voight.

$d = 3$										$d = 5$			$d = 6$	$d = 7$
148	2708	4628	7668	9076	10324	12852	15252	16532	19252	126032	629584	1197392	2803712	46643776
404	2804	4692	7700	9204	10580	13172	15284	17556	19348	153424	708944	1280592	4507648	196058176
564	3124	4852	7796	9300	10868	13684	15380	17684	19572	179024	747344	1284944	5163008	
756	3252	5172	8308	9460	11060	13748	15444	17716	20276	207184	970448	1395536	6637568	
1300	3508	5204	8372	9812	11092	13972	15700	17780	20436	223824	981328	1550288	7718912	
1524	3540	5940	8628	10164	11476	14420	16084	18292	20724	394064	1034192	1664592	10766336	
1620	3604	6420	8692	10260	12660	14516	16116	18644	20788	453712	1104464	1665360	20891648	
2228	3892	7028	9044	10292	12788	14964	16180	18740	20948	535120	1172304			

On en déduit avec le théorème 4 l'énoncé suivant :

Proposition 7. *Pour chacun des corps de nombres K indiqués ci-dessus, le théorème de Fermat asymptotique est vrai sur K.*

Signalons que, pour $d \neq 6$, le groupe de Galois sur $\mathbb{Q}$ de la clôture galoisienne de K est isomorphe à $\mathbb{S}_d$. Pour $d = 6$, il est non abélien d'ordre 12 ou 72.

5. Théorème de Fermat effectif – exemples

On établit le théorème de Fermat asymptotique de façon effective pour quelques corps de nombres figurant dans ces tables, ainsi que pour les corps $\mathbb{Q}(\mu_{16})^+$ et $\mathbb{Q}(\mu_{32})^+$.

Théorème 8. *Soit K un corps cubique réel de discriminant $D_K \in \{148, 404, 564\}$. Pour tout $p \geq 5$, l'ensemble $F_p(K)$ est trivial.*

Théorème 9. *Posons $K = \mathbb{Q}(\alpha)$ avec*

$$\alpha^5 - 6\alpha^3 + 6\alpha - 2 = 0. \tag{5-1}$$

(C'est le corps de plus petit discriminant intervenant dans les colonnes "$d = 5$" du tableau ci-dessus.) *Pour tout p distinct de* 5, 13, 17, 19, *l'ensemble $F_p(K)$ est trivial.*

Théorème 10. *Posons $K = \mathbb{Q}(\alpha)$ avec*

$$\alpha^6 + 2\alpha^5 - 11\alpha^4 - 16\alpha^3 + 15\alpha^2 + 14\alpha - 1 = 0. \tag{5-2}$$

(C'est le corps de plus petit discriminant intervenant dans la colonne "$d = 6$" du tableau ci-dessus.) *Pour tout $p \geq 29$, distinct de* 37, *l'ensemble $F_p(K)$ est trivial.*

Théorème 11. (1) *Pour tout $p \geq 5$, l'ensemble $F_p(\mathbb{Q}(\mu_{16})^+)$ est trivial.*

(2) *Pour tout $p > 6724$, l'ensemble $F_p(\mathbb{Q}(\mu_{32})^+)$ est trivial.*

On a $6724 = (1+3^4)^2$, qui est, pour $d = 8$, la borne obtenue dans [Oesterlé 1996] concernant les points de p-torsion des courbes elliptiques sur les corps de nombres de degré d (voir aussi [Derickx 2016]).

Partie II. Les théorèmes 2 et 6

Pour tout idéal premier $\mathfrak{q}$ de O_K, notons $v_{\mathfrak{q}}$ la valuation sur K qui lui est associée, et pour toute courbe elliptique E/K, notons j_E son invariant modulaire.

6. Démonstration du théorème 2

Lemme 12. *Les trois assertions suivantes sont équivalentes* :

(1) *La condition* (**FS**) *est satisfaite.*

(2) *Il n'existe pas de courbe elliptique E/K telle que l'on ait* :

  (i) $v_{\mathscr{L}}(j_E) < 0$,

  (ii) *pour tout idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, on a $v_{\mathfrak{q}}(j_E) \geq 0$,*

  (iii) *E a tous ses points d'ordre* 2 *rationnels sur K.*

(3) *Il n'existe pas de courbe elliptique sur K, de conducteur $\mathscr{L}$, ayant tous ses points d'ordre* 2 *rationnels sur K.*

Démonstration. Vérifions l'implication (1) $\Rightarrow$ (2). Supposons pour cela qu'il existe une courbe elliptique E/K satisfaisant les trois conditions de la deuxième assertion. D'après la condition (iii), à torsion quadratique près, il existe $\lambda \in K$ tel que E/K possède une équation de la forme de Legendre (voir [Silverman 2009, p. 49, Proposition 1.7(a)] et sa démonstration)

$$y^2 = x(x-1)(x-\lambda).$$

Posons

$$\mu = 1 - \lambda.$$

On a les égalités

$$j_E = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1-\lambda)^2} = 2^8 \frac{(1-\lambda\mu)^3}{(\lambda\mu)^2}.$$

Soit $O_{\mathscr{L}}$ l'anneau des $\{\mathscr{L}\}$-entiers de K. D'après la condition (ii), on a

$$j_E \in O_{\mathscr{L}}.$$

De plus, λ, $\frac{1}{\lambda}$, μ et $\frac{1}{\mu}$ sont racines d'un polynôme unitaire (de degré 6) à coefficients dans $O_{\mathscr{L}}$. Par suite, λ et μ appartiennent à S. Posons

$$t = \max\{|v_{\mathscr{L}}(\lambda)|, |v_{\mathscr{L}}(\mu)|\}.$$

Il résulte de la condition (i) que l'on a $t > 0$. L'égalité $\lambda + \mu = 1$ implique alors que l'on a

$$v_{\mathscr{L}}(\lambda) = v_{\mathscr{L}}(\mu) = -t \quad \text{ou} \quad v_{\mathscr{L}}(\lambda) = 0,\ v_{\mathscr{L}}(\mu) = t \quad \text{ou} \quad v_{\mathscr{L}}(\lambda) = t,\ v_{\mathscr{L}}(\mu) = 0.$$

On obtient dans tous les cas

$$v_{\mathscr{L}}(j_E) = 8v_{\mathscr{L}}(2) - 2t = 8d - 2t.$$

La condition (i) implique $t > 4d$ et donc la condition (**FS**) n'est pas satisfaite (inégalité (1-2)). Cela prouve la première implication.

L'implication (2) $\Rightarrow$ (3) est immédiate.

Démontrons l'implication (3) $\Rightarrow$ (1). Supposons la condition (**FS**) non satisfaite, autrement dit qu'il existe $a \in S$ tel que l'on ait

$$|v_{\mathscr{L}}(a)| > 4d.$$

Posons $b = 1 - a$.

Supposons $v_{\mathscr{L}}(a) > 4d$. Vérifions que la courbe elliptique E/K d'équation

$$y^2 = x(x-a)(x+b) \tag{6-1}$$

est de conducteur $\mathscr{L}$, ce qui établira l'implication dans ce cas. Notons $c_4(E)$ et $\Delta(E)$ les invariants standard associés à cette équation. On a

$$c_4(E) = 16(a^2 + ab + b^2) \quad \text{et} \quad \Delta(E) = 16(ab)^2.$$

Pour tout idéal premier $\mathfrak{q}$ de O_K distinct de $\mathscr{L}$, on a $v_{\mathfrak{q}}(\Delta(E)) = 0$, donc E/K a bonne réduction en $\mathfrak{q}$. Posons

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

On obtient comme nouveau modèle de E/K

$$(W): \qquad Y^2 + XY = X^3 - \frac{a}{2}X^2 - \frac{ab}{16}X.$$

On a $v_{\mathscr{L}}(a) > 4d = 4v_{\mathscr{L}}(2)$, donc ce modèle est entier. Par ailleurs, on a

$$v_{\mathscr{L}}(c_4(E)) = 4d \quad \text{et} \quad v_{\mathscr{L}}(\Delta(E)) = 4d + 2v_{\mathscr{L}}(a) > 12d,$$
$$c_4(E) = 2^4 c_4(W) \quad \text{et} \quad \Delta(E) = 2^{12}\Delta(W),$$

d'où

$$v_{\mathscr{L}}(c_4(W)) = 0 \quad \text{et} \quad v_{\mathscr{L}}(\Delta(W)) > 0.$$

Ainsi E a réduction de type multiplicatif en $\mathscr{L}$, d'où notre assertion.

Supposons $v_{\mathscr{L}}(a) < -4d$. Posons

$$a' = \frac{1}{a} \quad \text{et} \quad b' = 1 - a'.$$

On a $b' = -b/a$ donc a' est dans S et on a $v_{\mathscr{L}}(a') > 4d$. Comme ci-dessus, on vérifie que la courbe elliptique d'équation $y^2 = x(x-a')(x+b')$ est de conducteur $\mathscr{L}$. Cela établit l'implication. □

Lemme 13. *Supposons que toute courbe elliptique sur K, de conducteur $\mathscr{L}$, ayant tous ses points d'ordre 2 sur K, soit modulaire. Les deux assertions suivantes sont équivalentes :*

(1) *Il n'existe pas de courbe elliptique sur K, de conducteur $\mathscr{L}$, ayant tous ses points d'ordre 2 rationnels sur K.*

(2) *La condition* (**C**) *est satisfaite.*

Démonstration. Pour tout idéal premier $\mathfrak{q} \neq \mathscr{L}$ de O_K, posons $\mathbb{F}_{\mathfrak{q}} = O_K/\mathfrak{q}$.

Supposons que la première condition soit réalisée. Vérifions que la seconde l'est aussi. Soit $\mathfrak{f}$ une newform de $\mathcal{H}$ telle que $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Procédons par l'absurde en supposant que pour tout idéal premier $\mathfrak{q} \neq \mathscr{L}$ de O_K la condition (1-3) ne soit pas satisfaite. Parce que le niveau de $\mathfrak{f}$ est $\mathscr{L}$, il existe une courbe elliptique E/K, de conducteur $\mathscr{L}$, ayant la même fonction L que celle de $\mathfrak{f}$ [Freitas et Siksek 2015a, Theorem 8]. Pour tout idéal premier $\mathfrak{q} \neq \mathscr{L}$ de O_K, l'ordre de $E(\mathbb{F}_{\mathfrak{q}})$ est donc multiple de 4. Il en résulte que E/K est liée par une isogénie de degré ≤ 2 à une courbe elliptique F/K ayant tous ses points d'ordre 2 sur K [Şengün et Siksek 2018, Lemma 7.5]. Le conducteur de F/K est $\mathscr{L}$, d'où une contradiction. (On n'a pas utilisé ici l'hypothèse de modularité.)

Inversement, supposons qu'il existe une courbe elliptique E/K, de conducteur $\mathscr{L}$, ayant tous ses points d'ordre 2 sur K. Par hypothèse, E étant modulaire, il existe une newform $\mathfrak{f} \in \mathcal{H}$ ayant la même fonction L que celle de E. On a $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Soit $\mathfrak{q}$ un idéal premier de O_K distinct de $\mathscr{L}$. La courbe elliptique E a bonne réduction en $\mathfrak{q}$ et l'application $E(K)[2] \to E(\mathbb{F}_{\mathfrak{q}})$ est injective (cf. [Silverman 2009, Propopsition 3.1,

p. 192]). Par suite, 4 divise l'ordre de $E(\mathbb{F}_{\mathfrak{q}})$, autrement dit, on a $a_{\mathfrak{q}}(\mathfrak{f}) \equiv \mathrm{Norm}(\mathfrak{q}) + 1 \pmod 4$. Ainsi, la condition (**C**) n'est pas satisfaite, d'où le résultat. □

Le théorème 2 est une conséquence directe des lemmes 12 et 13.

Remarque. L'hypothèse de modularité est intervenue dans la démonstration pour établir l'implication (**C**) ⇒ (**FS**).

7. Démonstration du théorème 6

On démontre par récurrence que pour tout $r \geq 1$, tel que $r \leq n+2$, on a l'inclusion

$$\mathbb{Q}(\mu_{2^r})^+ \subseteq K. \tag{7-1}$$

Cela établira le résultat, car $\mathbb{Q}(\mu_{2^{n+2}})^+$ et K sont de même degré 2^n sur $\mathbb{Q}$. L'inclusion (7-1) est vraie si $r = 1$ et $r = 2$. Soit r un entier tel que $2 \leq r < n+2$ et que (7-1) soit vraie. Il s'agit de vérifier que $\mathbb{Q}(\mu_{2^{r+1}})^+$ est contenu dans K. Posons

$$L = K\mathbb{Q}(\mu_{2^{r+1}})^+.$$

L'extension L/K est non ramifiée en dehors des idéaux premiers de O_K au-dessus de 2, y compris aux places à l'infini. Par suite, son conducteur est une puissance de $\mathscr{L}$. Plus précisément :

Lemme 14. *Le conducteur de L/K divise $4O_K$.*

Démonstration. Soit ζ une racine primitive 2^{r+1}-ième de l'unité. Il existe $x \in O_K$ tel que x appartienne à $\mathscr{L}$ et pas à $\mathscr{L}^2$. On a $r-1 \leq n$. Posons

$$a = x^{2^{n-(r-1)}} \quad \text{et} \quad u = \left(\frac{\zeta + \zeta^{-1}}{a}\right)^2.$$

On a $(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2$. Parce que ζ^2 est une racine primitive 2^r-ième de l'unité, on déduit de (7-1) que u appartient à K. Par ailleurs, on a

$$[\mathbb{Q}(\mu_{2^{r+1}})^+ : \mathbb{Q}(\mu_{2^r})^+] = 2 \quad \text{et} \quad \mathbb{Q}(\mu_{2^{r+1}})^+ = \mathbb{Q}(\zeta + \zeta^{-1}).$$

Il en résulte que l'on a $[L : K] \leq 2$, puis l'égalité

$$L = K(\sqrt{u}).$$

On a

$$v_{\mathscr{L}}(u) = 0. \tag{7-2}$$

En effet, v étant la valuation de $\overline{\mathbb{Q}_2}$ normalisée par $v(2) = 1$, on a

$$v(x) = \frac{1}{2^n}, \quad v(a) = \frac{1}{2^{r-1}} \quad \text{et} \quad v(\zeta + \zeta^{-1}) = \frac{1}{2^{r-1}},$$

d'où (7-2). Ainsi, le discriminant de L/K divise $4O_K$. On obtient le résultat car le conducteur et le discriminant de L/K sont égaux [Cassels et Fröhlich 1967, p. 160, si $[L : K] = 2$]. □

Soit K^{4O_K} le corps de classes de rayon modulo $4O_K$ sur K. D'après le lemme précédent, L est contenu dans K^{4O_K}. Par hypothèse, 2 est totalement ramifié dans K et on a $h_K^+ = 1$. D'après l'assertion 1 du théorème 39 de l'Appendice, on a donc $K^{4O_K} = K$. On obtient $L = K$, ce qui montre que $\mathbb{Q}(\mu_{2^{r+1}})^+$ est contenu dans K, d'où le théorème.

Partie III. La méthode modulaire

Les démonstrations du théorème 4 et des résultats annoncés dans le paragraphe 5, reposent sur la méthode modulaire, analogue à celle utilisée par Wiles pour établir le théorème de Fermat sur $\mathbb{Q}$. On peut trouver dans [Freitas et Siksek 2015a] un exposé détaillé de cette méthode. Le principe général consiste à procèder par l'absurde en supposant qu'il existe un point non trivial dans $F_p(K)$. On lui associe ensuite une courbe elliptique définie sur K et en étudiant le module galoisien de ses points de p-torsion, on essaye d'obtenir une contradiction.

Décrivons la mise en œuvre de cette méthode dans notre situation. Soit K un corps de nombres totalement réel, de degré d sur $\mathbb{Q}$, satisfaisant les deux conditions suivantes :

(1) 2 est totalement ramifié dans K.

(2) On a $h_K^+ = 1$.

8. La courbe elliptique E_0/K

Considérons un point $(a, b, c) \in F_p(K)$ tel que $abc \neq 0$. On peut supposer que l'on a

$$a, b, c \in O_K. \tag{8-1}$$

On a $h_K^+ = 1$, en particulier O_K est principal. On supposera désormais, cela n'est pas restrictif, que l'on a

$$aO_K + bO_K + cO_K = O_K. \tag{8-2}$$

Soit E_0/K la cubique, appelée souvent courbe de Frey, d'équation

$$y^2 = x(x - a^p)(x + b^p). \tag{8-3}$$

Les invariants standard qui lui sont associés sont

$$c_4(E_0) = 16\big(a^{2p} + (ab)^p + b^{2p}\big), \quad c_6(E_0) = -32(a^p - b^p)(b^p - c^p)(c^p - a^p), \tag{8-4}$$

$$\Delta(E_0) = 16(abc)^{2p}. \tag{8-5}$$

En particulier, E_0 est une courbe elliptique définie sur K.

8.1. *Réduction de E_0/K.*

Lemme 15. *Soit* $\mathfrak{q}$ *un idéal premier de* O_K *distinct de* $\mathscr{L}$.

1) *L'équation* (8-3) *est minimale en* $\mathfrak{q}$.

2) *Si* $\mathfrak{q}$ *ne divise pas* abc, E_0 *a bonne réduction en* $\mathfrak{q}$.

3) *Si* $\mathfrak{q}$ *divise* abc, E_0 *a réduction de type multiplicatif en* $\mathfrak{q}$.

Démonstration. C'est une conséquence de la condition (8-1) ainsi que des formules (8-2), (8-4) et (8-5). □

Pour tout idéal premier $\mathfrak{q}$ de O_K, notons $\Delta_{\mathfrak{q}}$ un discriminant local minimal de E_0 en $\mathfrak{q}$.

Proposition 16. *Supposons* $p > 4d$. *Quitte à multiplier* (a, b, c) *par une unité convenable de* O_K, *les deux conditions suivantes sont satisfaites* :

(1) E_0 *a réduction de type multiplicatif en* $\mathscr{L}$.

(2) *On a*

$$v_{\mathscr{L}}(\Delta_{\mathscr{L}}) = 2pv_{\mathscr{L}}(abc) - 8d.$$

En particulier, avec une telle normalisation, E_0/K *est semi-stable.*

Démonstration. Le nombre premier 2 étant totalement ramifié dans K, on a $O_K/\mathscr{L} = \mathbb{F}_2$. L'un des entiers a, b, c est donc divisible par $\mathscr{L}$. On peut supposer que $\mathscr{L}$ divise b et que $\mathscr{L}$ ne divise pas ac. On a de plus $h_K^+ = 1$, donc le corps de classes de rayon modulo $4O_K$ sur K est égal à K (théorème 39). Soit U_K le groupe des unités de O_K. Le morphisme naturel $U_K \to (O_K/4O_K)^*$ est surjectif (lemme 41). Il existe ainsi $\varepsilon \in U_K$ tel que l'on ait

$$\varepsilon^{-1} \equiv -a \pmod 4.$$

Posons

$$a' = \varepsilon a, \quad b' = \varepsilon b, \quad c' = \varepsilon c.$$

Considérons alors la courbe elliptique E_0'/K d'équation

$$y^2 = x(x - a'^p)(x + b'^p). \tag{8-6}$$

En effectuant le changement de variables

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

on obtient comme nouveau modèle

$$(W) : \qquad Y^2 + XY = X^3 + \left(\frac{b'^p - a'^p - 1}{4}\right)X^2 - \frac{(a'b')^p}{16}X.$$

On a

$$a'^p + 1 \equiv 0 \pmod 4,$$

et d'après l'hypothèse faite sur p,

$$v_{\mathscr{L}}(b'^p) = pv_{\mathscr{L}}(b') \geq p > 4d = 4v_{\mathscr{L}}(2).$$

Par suite, (W) est un modèle entier. En notant $c_4(W)$ et $\Delta(W)$ les invariants standard qui lui sont associés, on a

$$c_4(E_0') = 2^4 c_4(W) \quad \text{et} \quad \Delta(E_0') = 2^{12}\Delta(W).$$

D'après les formules (8-4) et (8-5), utilisées avec l'équation (8-6), on obtient

$$v_{\mathscr{L}}(c_4(W)) = 0 \quad \text{et} \quad v_{\mathscr{L}}(\Delta(W)) = 2pv_{\mathscr{L}}(a'b'c') - 8d > 0.$$

Ainsi, (W) est un modèle minimal de E_0'/K, qui a donc réduction de type multiplicatif en $\mathscr{L}$. Parce que ε est une unité de O_K, et compte tenu du lemme 15, cela entraîne le résultat. □

Dans le cas où $p > 4d$, on supposera, dans toute la suite, que le triplet $(a, b, c) \in F_p(K)$ est normalisé de sorte que les deux conditions de la proposition 16 soient satisfaites.

8.2. ***Modularité de E_0/K.*** D'après le corollaire 2.1 de [Freitas et Siksek 2015a] :

Théorème 17. *La courbe elliptique E_0/K est modulaire si p est plus grand qu'une constante qui ne dépend que de K.*

D'après la remarque qui suit le corollaire 2.1 de [loc. cit.], ce résultat n'est pas effectif en général. Cependant l'énoncé suivant permet parfois de démontrer qu'une elliptique semi-stable définie sur K est modulaire [Freitas et al. 2015, Theorem 7] :

Théorème 18. *Posons $\ell = 5$ ou $\ell = 7$. Supposons qu'il existe un idéal premier de O_K au-dessus de ℓ en lequel l'extension $K/\mathbb{Q}$ soit non ramifiée. Soit E/K une courbe elliptique semi-stable sur K. Si $E(\overline{K})$ n'a pas de sous-groupe d'ordre ℓ stable par* $\mathrm{Gal}(\overline{K}/K)$, *alors E/K est modulaire.*

9. La représentation $\rho_{E_0,p}$

Notons

$$\rho_{E_0,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_0[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

la représentation donnant l'action de $\mathrm{Gal}(\overline{K}/K)$ sur le groupe des points de p-torsion de E_0.

9.1. ***Le conducteur de $\rho_{E_0,p}$.*** Notons N_{E_0} le conducteur de E_0/K. Posons

$$M_p = \prod_{\substack{\mathfrak{q} \mid N_{E_0} \\ p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q} \quad \text{et} \quad N_p = \frac{N_{E_0}}{M_p}.$$

Lemme 19. *Supposons $p > 4d$. On a $N_p = \mathscr{L}$.*

Démonstration. D'après le lemme 15 et la formule (8-5), pour tout idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, on a

$$v_{\mathfrak{q}}(\Delta_{\mathfrak{q}}) \equiv 0 \pmod{p}.$$

La seconde condition de la proposition 16 entraîne alors le résultat. □

Remarque. La terminologie adoptée dans ce paragraphe se justifie par le fait que si l'on a $p > 4d$, on peut démontrer que $\mathscr{L}$ le conducteur de Serre de $\rho_{E_0,p}$ (cf. [Serre 1987] pour $K = \mathbb{Q}$).

9.2. ***Irréductibilité de $\rho_{E_0,p}$.*** Le corps K étant totalement réel, il ne contient pas le corps de classes de Hilbert d'un corps quadratique imaginaire. D'après la proposition de l'Appendice B de [Kraus 2007], on a ainsi l'énoncé suivant :

Théorème 20. *La représentation $\rho_{E_0,p}$ est irréductible si p est plus grand qu'une constante que ne dépend que de K.*

En ce qui concerne l'effectivité de cet énoncé, considérons plus généralement dans la suite de ce paragraphe une courbe elliptique E/K semi-stable. Notons $\rho_{E,p}$ la représentation donnant l'action $\mathrm{Gal}(\overline{K}/K)$ sur son groupe des points de p-torsion. Rappelons un critère permettant souvent d'établir de manière effective que $\rho_{E,p}$ est irréductible (cf. [Kraus 2007]).

Soit p_0 le plus grand nombre premier pour lequel il existe une courbe elliptique définie sur K ayant un point d'ordre p_0 rationnel sur K. Il est borné par une fonction de d [Merel 1996] ; plus précisément, on a (voir [Oesterlé 1996; Derickx 2016])

$$p_0 \leq (1+3^{d/2})^2.$$

Notons $\left[\frac{d}{2}\right]$ la partie entière de $\frac{d}{2}$. Soit U_K^+ le groupe des unités totalement positives de O_K. Pour tout $u \in U_K^+$ et tout entier n tel que $1 \leq n \leq \left[\frac{d}{2}\right]$, on définit le polynôme $H_n^{(u)} \in \mathbb{Z}[X]$ comme suit. Soient H le polynôme minimal de u sur $\mathbb{Q}$ et t son degré. On pose

$$H_1^{(u)} = H \quad \text{et} \quad G = X^t H\left(\frac{Y}{X}\right) \in \mathbb{Z}[Y][X]. \tag{9-1}$$

Pour tout $n \geq 2$, $H_n^{(u)}$ est le polynôme de $\mathbb{Z}[X]$ obtenu en substituant Y par X dans

$$\mathrm{Res}_X\left(H_{n-1}^{(u)}, G\right) \in \mathbb{Z}[Y], \tag{9-2}$$

le résultant par rapport à X de $H_{n-1}^{(u)}$ et G. Il est unitaire de degré t^n et ses racines sont les produits de n racines de H comptées avec multiplicités. Posons

$$A_n = \mathrm{pgcd}_{u \in U_K^+} H_n^{(u)}(1) \quad \text{et} \quad R_K = \prod_{n=1}^{[d/2]} A_n. \tag{9-3}$$

L'énoncé qui suit est une reformulation du théorème 1 de [Kraus 2007] dans le cas où $h_K^+ = 1$ (voir aussi la proposition 4 de [loc. cit.] pour $d = 3$). Seule la condition $h_K^+ = 1$ intervient ici. On n'utilise pas l'hypothèse que 2 est totalement ramifié dans K.

Théorème 21. *Soit p un nombre premier ne divisant pas $D_K R_K$. Si $\rho_{E,p}$ est réductible, alors E/K, ou bien une courbe elliptique sur K liée à E par une K-isogénie de degré p, possède un point d'ordre p rationnel sur K. En particulier, si $p > p_0$ alors $\rho_{E,p}$ est irréductible.*

Démonstration. Rappelons les principaux arguments. Supposons $\rho_{E,p}$ réductible. Il existe des caractères $\varphi, \varphi' : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_p^*$ tels que $\rho_{E,p}$ soit représentable sous la forme $\left(\begin{smallmatrix} \varphi & * \\ 0 & \varphi' \end{smallmatrix}\right)$.

Soit $\mathcal{A}_p$ l'ensemble des idéaux premiers de O_K au-dessus de p. Les caractères φ et φ' sont non ramifiés en tout idéal premier qui n'est pas dans $\mathcal{A}_p$. De plus, pour tout $\mathfrak{p} \in \mathcal{A}_p$ l'un des caractères φ et φ' est

non ramifié en $\mathfrak{p}$. Par suite, il existe un sous-ensemble $\mathcal{A}$ de $\mathcal{A}_p$ tel que l'un des caractères φ et φ' soit non ramifié en dehors de $\mathcal{A}$ et que pour tout $\mathfrak{p} \in \mathcal{A}$ sa restriction à un sous-groupe d'inertie en $\mathfrak{p}$ soit le caractère cyclotomique.

Supposons $\mathcal{A}$ vide. Alors, φ ou φ' est partout non ramifié aux places finies. Parce que $h_K^+ = 1$, φ ou φ' est donc trivial. Si $\varphi = 1$, E a un point d'ordre p rationnel sur K. Si $\varphi' = 1$, E est liée par une K-isogénie de degré p a une courbe elliptique sur K ayant un point d'ordre p sur K.

Si $\mathcal{A}$ n'est pas vide, alors p divise $D_K R_K$ (voir la fin de la preuve du Theorem 1 de [Kraus 2007], p. 619, alinéa (2)), d'où le résultat. □

Remarque. Si R_K n'est pas nul, on obtient ainsi une constante explicite c_K, telle que pour tout $p > c_K$ et toute courbe elliptique E/K semi-stable sur K, la représentation $\rho_{E,p}$ soit irréductible. Dans ce cas, on obtient une version effective du théorème 20. Par exemple, R_K n'est pas nul si $d \in \{1, 2, 3, 5, 7\}$ [loc. cit., Theorem 2].

10. Le théorème d'abaissement du niveau

Il s'agit de l'analogue du théorème de Ribet intervenant dans la démonstration du théorème de Fermat sur $\mathbb{Q}$ [Ribet 1990]. Dans notre situation, si on a $p > 4d$, il s'énonce comme suit ([Freitas et Siksek 2015a, Theorem 7], les lemmes 15, 19 et l'égalité (8-5)) :

Théorème 22. *Supposons que les conditions suivantes soient satisfaites* :

(1) *On a* $p > 4d$.

(2) *L'indice de ramification de tout idéal premier de* O_K *au-dessus de* p *est strictement plus petit que* $p - 1$ *et le corps* $\mathbb{Q}(\mu_p)^+$ *n'est pas contenu dans* K.

(3) *La courbe elliptique* E_0/K *est modulaire.*

(4) *La représentation* $\rho_{E_0,p}$ *est irréductible.*

Alors, il existe $\mathfrak{f} \in \mathcal{H}$ *et un idéal premier* $\mathfrak{p}$ *de l'anneau d'entiers* $O_{\mathbb{Q}_\mathfrak{f}}$ *de* $\mathbb{Q}_\mathfrak{f}$ *au-dessus de* p, *tels que, en notant*

$$\rho_{\mathfrak{f},\mathfrak{p}} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(O_{\mathbb{Q}_\mathfrak{f}}/\mathfrak{p})$$

la représentation galoisienne associée à $\mathfrak{f}$ *et* $\mathfrak{p}$, *on ait*

$$\rho_{E_0,p} \simeq \rho_{\mathfrak{f},\mathfrak{p}}. \tag{10-1}$$

Proposition 23. *Les hypothèses faites dans l'énoncé du théorème 22 sont satisfaites si* p *est plus grand qu'une constante qui ne dépend que de* K.

Démonstration. La seconde condition est réalisée si p est non ramifié dans K. Les théorèmes 17 et 20 entraînent alors le résultat. □

Les représentations $\rho_{E_0,p}$ et $\rho_{\mathfrak{f},\mathfrak{p}}$ sont non ramifiées en dehors de $\mathscr{L}$ et des idéaux premiers de O_K au-dessus de p. Parce que $\rho_{E_0,p}$ est irréductible, l'isomorphisme (10-1) se traduit par les conditions suivantes : pour tout idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, qui n'est pas au-dessus de p, on a

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E_0) \pmod{\mathfrak{p}} \quad \text{si} \quad E_0 \text{ a bonne réduction en } \mathfrak{q}, \tag{10-2}$$

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv \pm(\mathrm{Norm}(\mathfrak{q})+1) \pmod{\mathfrak{p}} \quad \text{si} \quad E_0 \text{ a réduction de type multiplicatif en } \mathfrak{q}. \tag{10-3}$$

On en déduit l'énoncé ci-dessous permettant parfois d'obtenir une contradiction à l'existence de $(a, b, c) \in F_p(K)$ (cf. [Freitas et Siksek 2015b, lemme 7.1]). Pour tout idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, posons

$$A_{\mathfrak{q}} = \left\{ t \in \mathbb{Z} \mid |t| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})} \quad \text{et} \quad \mathrm{Norm}(\mathfrak{q})+1 \equiv t \pmod 4 \right\}, \tag{10-4}$$

$$B_{\mathfrak{f},\mathfrak{q}} = \mathrm{Norm}(\mathfrak{q})\big((\mathrm{Norm}(\mathfrak{q})+1)^2 - a_{\mathfrak{q}}(\mathfrak{f})^2\big) \prod_{t \in A_{\mathfrak{q}}} (t - a_{\mathfrak{q}}(\mathfrak{f})). \tag{10-5}$$

Proposition 24. *Supposons les quatre conditions du théorème 22 satisfaites. Soient $\mathfrak{f} \in \mathcal{H}$ et $\mathfrak{p}$ un idéal premier de $O_{\mathbb{Q}_{\mathfrak{f}}}$ au-dessus de p tels que $\rho_{E_0,p} \simeq \rho_{\mathfrak{f},\mathfrak{p}}$. Soit $\mathfrak{q}$ un idéal premier de O_K distinct de $\mathscr{L}$. Alors, p divise la norme de $\mathbb{Q}_{\mathfrak{f}}$ sur $\mathbb{Q}$ de $B_{\mathfrak{f},\mathfrak{q}}$.*

Démonstration. Si $\mathfrak{q}$ divise p, alors p divise $\mathrm{Norm}(\mathfrak{q})$, en particulier p divise la norme de $\mathbb{Q}_{\mathfrak{f}}$ sur $\mathbb{Q}$ de $B_{\mathfrak{f},\mathfrak{q}}$. Supposons que $\mathfrak{q}$ ne divise pas p. La courbe elliptique E_0 a bonne réduction ou réduction de type multiplicatif en $\mathfrak{q}$.

Supposons que E_0 ait bonne réduction en $\mathfrak{q}$. Parce que E_0 a tous ses points d'ordre 2 rationnels que K et que $\mathfrak{q}$ est distinct de $\mathscr{L}$, le nombre de points de la courbe elliptique déduite de E_0 par réduction est multiple de 4. Par ailleurs, on a $|a_{\mathfrak{q}}(E_0)| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}$ (borne de Weil), donc $a_{\mathfrak{q}}(E_0)$ appartient à $A_{\mathfrak{q}}$. La condition (10-2) implique alors notre assertion dans ce cas.

Si E_0 a réduction de type multiplicatif en $\mathfrak{q}$, la condition (10-3) est satisfaite, d'où le résultat. □

11. Démonstration du théorème 4

Compte tenu des propositions 23 et 24, le théorème 4 résulte de l'énoncé suivant :

Proposition 25. *Pour tout $\mathfrak{f} \in \mathcal{H}$, il existe un idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, tel que l'on ait $B_{\mathfrak{f},\mathfrak{q}} \neq 0$.*

Démonstration. Soit $\mathfrak{f}$ un élément de $\mathcal{H}$.

Supposons $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$. Il existe alors un idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, tel que $a_{\mathfrak{q}}(\mathfrak{f})$ ne soit pas dans $\mathbb{Z}$ (cf. [Cremona et Dembélé 2014, Theorem 9]), d'où $B_{\mathfrak{f},\mathfrak{q}} \neq 0$.

Supposons $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. D'après la condition (**C**), il existe un idéal premier $\mathfrak{q}$ de O_K, distinct de $\mathscr{L}$, tel que l'on ait $a_{\mathfrak{q}}(\mathfrak{f}) \not\equiv \mathrm{Norm}(\mathfrak{q})+1 \pmod 4$. En particulier, $a_{\mathfrak{q}}(\mathfrak{f})$ n'est pas dans $A_{\mathfrak{q}}$. De plus, on a $(\mathrm{Norm}(\mathfrak{q})+1)^2 \neq a_{\mathfrak{q}}(\mathfrak{f})^2$: dans le cas contraire, on aurait $a_{\mathfrak{q}}(\mathfrak{f}) = -(\mathrm{Norm}(\mathfrak{q})+1)$. Or $\mathfrak{q}$ étant distinct de $\mathscr{L}$, on a $2(\mathrm{Norm}(\mathfrak{q})+1) \equiv 0 \pmod 4$, ce qui conduit à une contradiction. Par suite, on a $B_{\mathfrak{f},\mathfrak{q}} \neq 0$, d'où l'assertion. □

Partie IV. Les théorèmes 8, 9, 10 et 11

Dans toute cette partie, on suppose qu'il existe un point $(a, b, c) \in F_p(K)$ tel que $abc \neq 0$. Rappelons que pour $p > 4d$, on suppose implicitement qu'il est normalisé comme indiqué dans l'énoncé de la proposition 16.

12. Sur l'irréductibilité de $\rho_{E_0,p}$

Dans le cas où p est ramifié dans K, le théorème 21 ne permet pas d'établir que la représentation $\rho_{E_0,p}$ est irréductible (si tel est le cas). On dispose néanmoins du résultat suivant permettant parfois de conclure, qui vaut sans hypothèse de ramification en p. Pour tout cycle $\mathfrak{m}$ of K, notons $K^{\mathfrak{m}}$ le corps de classes de rayon modulo $\mathfrak{m}$ sur K.

Lemme 26. *Soit $\mathfrak{p}$ un idéal premier de O_K au-dessus de p. Notons $\mathfrak{m}_\infty$ le produit des places archimédiennes de K. Soit $\varphi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_p^*$ un caractère non ramifié en dehors $\mathfrak{m}_\infty\mathfrak{p}$. Alors, le corps laissé fixe par le noyau de φ est contenu dans $K^{\mathfrak{m}_\infty\mathfrak{p}}$.*

Démonstration. Soit $n \geq 1$ un entier. Il suffit de montrer que

$$\mathrm{Gal}\big(K^{\mathfrak{m}_\infty\mathfrak{p}^n}/K^{\mathfrak{m}_\infty\mathfrak{p}}\big) \quad \text{est un } p\text{-groupe.} \tag{12-1}$$

En effet, d'après l'hypothèse faite, il existe $j \geq 1$ tel que le corps laissé fixe par le noyau de φ soit contenu dans $K^{\mathfrak{m}_\infty\mathfrak{p}^j}$. D'après l'assertion (12-1), le groupe $\mathrm{Gal}\big(K^{\mathfrak{m}_\infty\mathfrak{p}^j}/K^{\mathfrak{m}_\infty\mathfrak{p}}\big)$ est contenu dans le noyau φ, ce qui implique alors le résultat.

Démontrons (12-1). Posons $\mathfrak{m} = m_\infty\mathfrak{p}^{n+1}$ et $\mathfrak{n} = \mathfrak{m}_\infty\mathfrak{p}^n$. Notons $U_{\mathfrak{m},1}$ le groupe des unités de O_K congrues à 1 modulo $\mathfrak{m}$ et $U_{\mathfrak{n},1}$ l'analogue de $U_{\mathfrak{m},1}$ en ce qui concerne le cycle $\mathfrak{n}$. Le corollaire 3.2.4 of [Cohen 2000] entraîne l'égalité

$$[K^{\mathfrak{m}} : K^{\mathfrak{n}}](U_{\mathfrak{n},1} : U_{\mathfrak{m},1}) = \mathrm{Norm}(\mathfrak{p}). \tag{12-2}$$

Par ailleurs, pour tout $x \in U_{\mathfrak{n},1}$, on a $x^p \in U_{\mathfrak{m},1}$. Ainsi, $U_{\mathfrak{n},1}/U_{\mathfrak{m},1}$ est un p-groupe. D'après l'égalité (12-2), $[K^{\mathfrak{m}} : K^{\mathfrak{n}}]$ est donc une puissance de p, ce qui entraîne l'assertion (12-1). □

On utilisera ce résultat de la façon suivante. Supposons $p > 4d$ et $\rho_{E_0,p}$ réductible. Soient φ et φ' ses caractères d'isogénie. Ils sont non ramifiés en dehors de $\mathfrak{m}_\infty$ et des idéaux premiers de O_K au-dessus de p. Supposons qu'il existe un idéal premier $\mathfrak{p}$ de O_K au-dessus de p tel que φ ou φ' soit non ramifié en dehors de $\mathfrak{m}_\infty\mathfrak{p}$ et que de plus on ait $[K^{\mathfrak{m}_\infty\mathfrak{p}} : K] \leq 2$. On déduit alors du lemme 26, l'existence d'une courbe elliptique sur K ayant un point d'ordre p rationnel sur K, ce qui, si p est assez grand par rapport à d, conduit à une contradiction.

13. Corps cubiques et modularité

On va démontrer ici un critère permettant parfois d'établir que toute courbe elliptique semi-stable définie sur un corps cubique réel est modulaire. Rappelons que l'entier R_K est défini par la seconde formule de (9-3).

Théorème 27. *Soit K un corps cubique réel satisfaisant les conditions suivantes :*

(1) *On a $h_K^+ = 1$.*

(2) *5 et 7 ne divisent pas $D_K R_K$.*

(3) *3 n'est pas inerte dans K.*

Alors, toute courbe elliptique semi-stable définie sur K est modulaire.

13.1. ***Courbes elliptiques et points de 35-torsion.*** Commençons par établir l'énoncé qui suit, qui est une conséquence d'un résultat de Bruin et Najman [2016].

Proposition 28. *Soit K un corps cubique tel que 3 ne soit pas inerte dans K. Alors, il n'existe pas de courbes elliptiques définies sur K ayant un point d'ordre 35 rationnel sur K.*

Démonstration. On utilise le théorème 1 de [Bruin et Najman 2016], ainsi que la remarque 4 à la fin du paragraphe 2 de [loc. cit.] qui est très utile dans son application. Avec les notations de ce théorème, on prend

$$A = \mathbb{Z}/35\mathbb{Z}, \quad L = \mathbb{Q}, \quad m = 1, \quad n = 35, \quad X = X' = X_1(35), \quad \pi = \mathrm{id} \quad \text{et} \quad p = \mathfrak{p}_0 = 3.$$

Il s'agit de vérifier que les six conditions i)-vi) de cet énoncé sont satisfaites. Parce que 3 ne divise pas n, on a $A' = \mathbb{Z}/35\mathbb{Z}$ et $h = 1$. Pour toute pointe Z de $X_1(35)$, l'ensemble $L(Z)$ est le corps de rationalité de Z. C'est donc l'un des corps

$$\mathbb{Q}, \quad \mathbb{Q}(\mu_5), \quad \mathbb{Q}(\mu_7) \quad \text{et} \quad \mathbb{Q}(\mu_{35})^+.$$

Par hypothèse, 3 n'est pas inerte dans K, on a donc

$$S_{K,\mathfrak{p}_0} = \{1, 2\}.$$

La gonalité de $X_1(35)$ vaut 12 et sa Jacobienne est de rang 0 sur $\mathbb{Q}$ [Derickx 2016, p. 19 et lemme 1, p. 30]. Pour tout idéal premier $\mathfrak{p}$ de O_K au-dessus de 3, il n'existe pas de courbes elliptiques définies sur $k(\mathfrak{p})$ ayant un point rationnel d'ordre 35. Par ailleurs, 3 est inerte dans $\mathbb{Q}(\mu_5)$, $\mathbb{Q}(\mu_7)$ et $\mathbb{Q}(\mu_{35})^+$. Les six conditions considérées sont donc satisfaites, d'où le résultat. □

Remarque. Il existe des courbes elliptiques définies sur $\mathbb{F}_{27}$ ayant un point rationnel d'ordre 35, ce qui explique l'hypothèse que 3 n'est pas inerte dans K dans l'énoncé de la proposition (cf. [Waterhouse 1969, Theorem 4.1]).

13.2. ***Démonstration du théorème 27.*** Soit E/K une courbe elliptique semi-stable sur K. On utilise le théorème 18. Par hypothèse, 5 et 7 sont non ramifiés dans K. Il s'agit ainsi de montrer que l'une au moins des représentations $\rho_{E,5}$ et $\rho_{E,7}$ est irréductible. Supposons le contraire, i.e., que $\rho_{E,5}$ et $\rho_{E,7}$ soient réductibles. Parce que l'on a $h_K^+ = 1$ et que 5 et 7 ne divisent pas $D_K R_K$, quitte à remplacer E par une courbe elliptique sur K qui lui est liée par une K-isogénie de degré 1, 5, 7 ou 35, on peut supposer que E a un point d'ordre 5 et un point d'ordre 7 rationnels sur K (théorème 21). Elle possède donc un point d'ordre 35 rationnel sur K, ce qui conduit à une contradiction (proposition 28), d'où le résultat.

14. Corps cubiques et irréductibilité de $\rho_{E_0,13}$

On utilisera dans la démonstration du théorème 8 le résultat suivant.

Théorème 29. *Soit K un corps cubique satisfaisant les conditions suivantes* :

(1) *On a $h_K^+ = 1$.*

(2) 13 *ne divise pas $D_K R_K$.*

(3) 3 *n'est pas inerte dans K.*

Alors, pour toute courbe elliptique semi-stable E/K, ayant un point d'ordre 2 *rationnel sur K, la représentation $\rho_{E,13}$ est irréductible.*

Démonstration. Elle est analogue à celle du théorème 27. Soit E/K une courbe elliptique semi-stable ayant un point d'ordre 2 rationnel sur K. Supposons $\rho_{E,13}$ réductible. Parce que $h_K^+ = 1$ et que 13 ne divise pas $D_K R_K$, la courbe elliptique E, ou bien une courbe elliptique sur K liée à E par une K-isogénie de degré 13, possède un point d'ordre 13 rationnel K (théorème 21). Il existe donc une courbe elliptique sur K ayant un point d'ordre 26 rationnel sur K.

Avec les notations du théorème 1 de [Bruin et Najman 2016], on prend $A = \mathbb{Z}/26\mathbb{Z}$, $m = 1$, $n = 26$, $\mathfrak{p}_0 = 3$, $X = X' = X_1(26)$ et π est l'identité de X. Parce que 3 ne divise pas n, on a $A' = \mathbb{Z}/26\mathbb{Z}$ et $h = 1$. Le corps de rationalité des pointes de $X_1(26)$ est $\mathbb{Q}$ ou $\mathbb{Q}(\mu_{13})^+$. Par hypothèse, 3 n'est pas inerte dans K, donc on a $S_{K,\mathfrak{p}_0} = \{1, 2\}$. La gonalité de $X_1(26)$ vaut 6 et sa Jacobienne est de rang 0 sur $\mathbb{Q}$ [Derickx 2016, p. 19 et lemme 1, p. 30]. Pour tout idéal premier $\mathfrak{p}$ de O_K au-dessus de 3, il n'existe pas de courbes elliptiques définies sur $k(\mathfrak{p})$ ayant un point rationnel d'ordre 26. Par ailleurs, dans l'anneau d'entiers de $\mathbb{Q}(\mu_{13})^+$, l'idéal engendré par 3 est le produit de deux idéaux premiers de degré 3, et 3 n'est pas dans $S_{K,\mathfrak{p}_0}$. Le théorème 1 de [Bruin et Najman 2016] entraîne alors contradiction et le résultat. □

15. Démonstration du théorème 8

Gross et Rohrlich [1978, Theorem 5.1] ont démontré que l'ensemble des points rationnels de F_7 et F_{11} sur tout corps cubique est trivial. Par ailleurs, Klassen et Tzermias [1997, Theorem 1] ont établi qu'il en est de même pour F_5. On supposera donc que l'on a

$$p \geq 13.$$

En particulier, l'inégalité $p > 4d$ est satisfaite. De plus, on a $p_0 = 13$ [Parent 2003].

15.1. ***Cas où $D_K = 148$.*** On a [Voight]

$$K = \mathbb{Q}(\alpha) \quad \text{où} \quad \alpha^3 - \alpha^2 - 3\alpha + 1 = 0.$$

Le nombre premier 3 étant inerte dans K, les théorèmes 27 et 29 ne s'appliquent pas.

Lemme 30. *La courbe elliptique E_0/K est modulaire.*

Démonstration. On utilise le théorème 18 avec $\ell = 5$, qui ne divise pas D_K. Supposons que E_0 possède un sous-groupe d'ordre 5 stable par $\mathrm{Gal}(\overline{K}/K)$. Parce que E_0 a tous ses points d'ordre 2 rationnels sur K, il en résulte que E_0 est liée par une K-isogénie de degré au plus 2 à une courbe elliptique sur K ayant un sous-groupe cyclique d'ordre 20 stable par $\mathrm{Gal}(\overline{K}/K)$ (cf. par exemple [Anni et Siksek 2016, p. 1163]). La courbe modulaire $X_0(20)$ est la courbe elliptique, de conducteur 20, numérotée 20A1 dans les tables de Cremona [1997], d'équation

$$y^2 = x^3 + x^2 + 4x + 4.$$

Elle possède six pointes, toutes rationnelles sur $\mathbb{Q}$. Le groupe $X_0(20)(\mathbb{Q})$ est d'ordre 6, et on vérifie avec `Magma`[2] qu'il en est de même du groupe $X_0(20)(K)$. Cela montre que $Y_0(20)(K)$ est vide, d'où une contradiction et notre assertion. □

Lemme 31. *La représentation $\rho_{E_0,p}$ est irréductible.*

Démonstration. Posons $u = \alpha^2$. C'est une unité totalement positive de K. Son polynôme minimal est $H = X^3 - 7X^2 + 11X - 1$. On a $H(1) = 4$, donc R_K divise 4 (formules (9-1) et (9-3)). Par ailleurs, on a $D_K = 4.37$. Cela entraîne le résultat si $p \neq 13, 37$ (théorème 21).

Supposons $\rho_{E_0,13}$ réductible. Dans ce cas, E_0 est liée par une K-isogénie de degré au plus 2 à une courbe elliptique sur K ayant un sous-groupe cyclique d'ordre 52 stable par $\mathrm{Gal}(\overline{K}/K)$. Il existe un morphisme défini sur $\mathbb{Q}$, de degré 3, de la courbe modulaire $X_0(52)$ sur la courbe elliptique $F/\mathbb{Q}$, numérotée 52A1 dans les tables de Cremona [1997, p. 363], d'équation

$$y^2 = x^3 + x - 10.$$

La courbe $X_0(52)$ possède six pointes, toutes rationnelles sur $\mathbb{Q}$. Avec `Magma`, on constate que l'on a $F(K) = F(\mathbb{Q})$, qui est d'ordre 2. On en déduit que $Y_0(52)(K)$ est vide, d'où une contradiction et le fait que $\rho_{E_0,13}$ soit irréductible.

Supposons $\rho_{E_0,37}$ réductible. Soient φ et φ' ses caractères d'isogénie. On a $37O_K = \mathfrak{p}_1^2\mathfrak{p}_2$, où $\mathfrak{p}_i$ est un idéal premier de O_K. L'idéal $\mathfrak{p}_2$ est non ramifié. Par ailleurs, E_0 a en $\mathfrak{p}_2$ réduction semi-stable. D'après l'hypothèse faite sur $\rho_{E_0,37}$, si E_0 a bonne réduction en $\mathfrak{p}_2$, cette réduction est nécessairement de hauteur 1

2. À de nombreuses reprises dans cet article, comme dans la démonstration du lemme 30, on est amené à déterminer le rang sur des corps de nombres de certaines courbes elliptiques définies sur $\mathbb{Q}$. Pour cela, on utilise directement le programme relatif à l'instruction `MordellWeilGroup` du logiciel `Magma`. De plus, cette instruction indique si les résultats obtenus sont inconditionnels. Tel est le cas de tous ceux intervenant dans la suite.

(cf. [Serre 1972, proposition 12]). On en déduit que l'un des caractères φ et φ' est non ramifié en $\mathfrak{p}_2$ [loc. cit., corollaire p. 274 et corollaire p. 277]. Quitte à remplacer E_0 par une courbe elliptique qui lui est liée par une K-isogénie de degré 37, on peut supposer que c'est φ. Par suite, φ est non ramifié en dehors de $\mathfrak{p}_1$ et des places archimédiennes. D'après le lemme 26, le corps laissé fixe par le noyau de φ est donc contenu dans le corps de rayon $K^{\mathfrak{m}_\infty \mathfrak{p}_1}$. On vérifie que l'on a $[K^{\mathfrak{m}_\infty \mathfrak{p}_1} : K] = 2$ [PARI 2015]. Ainsi, φ est d'ordre au plus 2. On a $\varphi \neq 1$, car E_0 n'a pas de point d'ordre 37 rationnel sur K. Le caractère φ est donc d'ordre 2 et la courbe elliptique déduite de E_0 par torsion quadratique par φ a donc un point d'ordre 37 sur K, d'où une contradiction et le résultat. □

Les quatre conditions du théorème d'abaissement de niveau sont donc satisfaites. Par ailleurs, on a $|\mathcal{H}| = 0$, i.e., il n'existe pas de newforms modulaires paraboliques de Hilbert sur K de poids parallèle 2 et de niveau $\mathscr{L}$ [LMFDB 2013]. On obtient ainsi une contradiction à l'existence de (a, b, c), d'où le théorème dans ce cas.

15.2. ***Cas où $D_K = 404$.*** On a

$$K = \mathbb{Q}(\alpha) \quad \text{où} \quad \alpha^3 - \alpha^2 - 5\alpha - 1 = 0.$$

On a $3O_K = \wp_1\wp_2$, où $\wp_1$ est un idéal premier de degré 1 et où $\wp_2$ est de degré 2. En particulier, 3 n'est pas inerte dans K.

Le polynôme minimal de $\alpha^2 \in U_K^+$ est $H = X^3 - 11X^2 + 23X - 1$ et on a $H(1) = 12$. On a $D_K = 2^2 \cdot 101$, donc 5, 7 et 13 ne divisent pas $D_K R_K$.

Il résulte alors du théorème 27 que E_0/K est modulaire. Pour $p \neq 101$, les théorèmes 21 et 29 entraînent que $\rho_{E_0,p}$ est irréductible. La décomposition de $101O_K$ en produit d'idéaux premiers est de la forme $\mathfrak{p}_1^2\mathfrak{p}_2$ et on a $[K^{\mathfrak{m}_\infty \mathfrak{p}_1} : K] = 2$. On en déduit, comme dans la démonstration du lemme 31, que $\rho_{E_0,101}$ est irréductible.

Par ailleurs, on a $|\mathcal{H}| = 1$, i.e., il existe une unique newform modulaire parabolique de Hilbert $\mathfrak{f}$ sur K de poids parallèle 2 et de niveau $\mathscr{L}$ [LMFDB 2013]. En particulier, on a $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Soit $\mathfrak{q}$ l'idéal premier de O_K au-dessus de 7 de degré 1. On a $a_{\mathfrak{q}}(\mathfrak{f}) = -2$. D'après les égalités (10-4) et (10-5), on a

$$A_{\mathfrak{q}} = \{-4, 0, 4\} \quad \text{et} \quad B_{\mathfrak{f},\mathfrak{q}} = -2^5 \cdot 3^2 \cdot 5 \cdot 7.$$

Ainsi, $B_{\mathfrak{f},\mathfrak{q}}$ n'est pas divisible par p, d'où la conclusion dans ce cas (proposition 24).

15.3. ***Cas où $D_K = 564$.*** On a

$$K = \mathbb{Q}(\alpha) \quad \text{où} \quad \alpha^3 - \alpha^2 - 5\alpha + 3 = 0.$$

On a $3O_K = \wp_1^2\wp_2$, où $\wp_i$ est un idéal premier de degré 1.

Le polynôme minimal de $(\alpha + 2)^2 \in U_K^+$ est $H = X^3 - 27X^2 + 135X - 1$ et on a $H(1) = 2^2 \cdot 3^3$.

On a $D_K = 2^2 \cdot 3 \cdot 47$. On en déduit que E_0/K est modulaire (théorème 27) et que $\rho_{E_0,p}$ est irréductible pour $p \neq 47$ (théorème 21 et théorème 29). On a $47O_K = \mathfrak{p}_1^2\mathfrak{p}_2$ et $[K^{\mathfrak{m}_\infty \mathfrak{p}_1} : K] = 2$, il en est donc de même de $\rho_{E_0,47}$.

L'ensemble $\mathcal{H}$, qui est de cardinal 2, est formé d'une newform $\mathfrak{f}$ et de sa conjuguée galoisienne telle que $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}(\beta)$ où $\beta^2 + 3\beta - 1 = 0$ [LMFDB 2013]. Soit $\mathfrak{q}$ l'idéal premier de O_K au-dessus de 3 tel que $a_{\mathfrak{q}}(\mathfrak{f}) = \beta$. Il est de degré 1. On a $A_{\mathfrak{q}} = \{0\}$ et $B_{\mathfrak{f},\mathfrak{q}} = -3\beta(16-\beta^2)$. Sa norme sur $\mathbb{Q}$ étant -3^6, on obtient la conclusion cherchée.

Cela termine la démonstration du théorème 8.

16. Démonstration du théorème 9

L'ensemble des points rationnels de F_{11} sur tout corps de degré 5 sur $\mathbb{Q}$ est trivial [Gross et Rohrlich 1978, Theorem 5.1]. Tzermias [1998, Theorem 1] a démontré qu'il en est de même pour F_7. On supposera donc que l'on a

$$p \geq 23.$$

En particulier, on a $p > 4d$. Par ailleurs, on a $D_K = 2^4 \cdot 7877$.

Lemme 32. *La courbe elliptique E_0/K est modulaire.*

Démonstration. On utilise le théorème 18 avec $\ell = 7$. Supposons que E_0 possède un sous-groupe d'ordre 7 stable par $\mathrm{Gal}(\overline{K}/K)$. Dans ce cas, E_0 possède un sous-groupe cyclique d'ordre 14 stable par $\mathrm{Gal}(\overline{K}/K)$. La courbe modulaire $X_0(14)$ est la courbe elliptique, de conducteur 14, numérotée 14A1 dans les tables de Cremona [1997], d'équation

$$y^2 + xy + y = x^3 + 4x - 6.$$

Elle possède quatre pointes, qui sont rationnelles sur $\mathbb{Q}$. On vérifie avec `Magma` que l'on a $X_0(14)(K) = X_0(14)(\mathbb{Q})$ qui est d'ordre 6. Par ailleurs, les points non cuspidaux de $X_0(14)$ correspondent à deux classes d'isomorphisme de courbes elliptiques sur $\mathbb{Q}$ d'invariants modulaires entiers (-15^3 et 255^3). Parce que celui de E_0 n'est pas entier en $\mathscr{L}$, on obtient une contradiction et le résultat. □

Lemme 33. *La représentation $\rho_{E_0,p}$ est irréductible.*

Démonstration. L'entier α étant défini par l'égalité (5-1), posons

$$u_1 = (\alpha - 1)^2 \quad \text{et} \quad u_2 = (\alpha^2 + \alpha - 1)^2.$$

Ce sont des unités totalement positives de O_K. On vérifie que l'on a (formules (9-1) et (9-2))

$$H_1^{(u_1)}(1) = -12 \quad \text{et} \quad \mathrm{pgcd}\big(H_2^{(u_1)}(1), H_2^{(u_2)}(1)\big) = 2^{12} \cdot 3 \cdot 5^2.$$

Il en résulte que R_K n'est pas divisible pas un nombre premier plus grand que 7. On a $p_0 = 19$ [Derickx 2016, Chapter III, Theorem 1.1], d'où l'assertion si $p \neq 7877$. Par ailleurs, on a $7877 O_K = \mathfrak{p}_1^2 \mathfrak{p}_2$, où $\mathfrak{p}_1$ est un idéal premier de degré 1 et $\mathfrak{p}_2$ un idéal premier de degré 3. On vérifie que l'on a $[K^{\mathfrak{m}_\infty \mathfrak{p}_1} : K] = 2$, ce qui entraîne le résultat pour $p = 7877$. □

Par ailleurs, on a $|\mathcal{H}| = 2$. Plus précisément, $\mathcal{H}$ est formé d'une newform $\mathfrak{f}$ et de sa conjuguée galoisienne, et on a $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}(\beta)$ où $\beta^2 + \beta - 3 = 0$ [LMFDB 2013]. Soit $\mathfrak{q}$ l'idéal premier de O_K au-dessus de 3 de

degré 1. On a $a_{\mathfrak{q}}(\mathfrak{f}) = \beta$. D'après les égalités (10-4) et (10-5), on a $A_{\mathfrak{q}} = \{0\}$ et $B_{\mathfrak{f},\mathfrak{q}} = -3\beta(16-\beta^2)$. La norme sur $\mathbb{Q}$ de $B_{\mathfrak{f},\mathfrak{q}}$ est $-3^5 \cdot 17$, qui n'est pas divisible par p. La proposition 24 implique alors le théorème.

17. Démonstration du théorème 10

On a $D_K = 2^{11} \cdot 37^2$. On vérifie, comme dans la démonstration du lemme 32, que l'on a $X_0(14)(\mathbb{Q}) = X_0(14)(K)$, d'où l'on déduit que E_0/K est modulaire.

Démontrons que $\rho_{E_0,p}$ est irréductible. Par hypothèse, on a $p > 4d = 24$ et $p \neq 37$. L'entier α étant défini par l'égalité (5-2), on considère les unités totalement positives

$$u_1 = \frac{1}{58^2}\big(4\alpha^5 + 19\alpha^4 - 28\alpha^3 - 170\alpha^2 - 16\alpha + 41\big)^2,$$
$$u_2 = \frac{1}{58^2}\big(14\alpha^5 + 23\alpha^4 - 156\alpha^3 - 160\alpha^2 + 176\alpha + 13\big)^2.$$

On vérifie que l'on a

$$H_1^{(u_1)}(1) = 16, \quad H_2^{(u_1)}(1) = 2^{32} \cdot 5^4 \quad \text{et} \quad H_3^{(u_2)}(1) = 2^{216} \cdot 7^{54}.$$

Par suite, R_K n'est pas divisible par un nombre premier plus grand que 7. Il n'existe pas de courbes elliptiques sur K ayant un point d'ordre p rationnel sur K [Derickx 2016, Chapter III, Theorem 1.1)], d'où l'assertion.

Par ailleurs, on vérifie avec `Magma` que l'on a $|\mathcal{H}| = 2$ et que $\mathcal{H}$ est formé d'une newform $\mathfrak{f}$ et de sa conjuguée galoisienne, dont le corps de rationalité est $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}(\beta)$ où $\beta^2 - \beta - 21 = 0$. En utilisant la proposition 24, on conclut alors en considérant l'idéal premier $\mathfrak{q}_1$ de O_K de degré 1 au-dessus de 17, tel que $a_{\mathfrak{q}_1}(\mathfrak{f}) = \beta$ et l'idéal premier $\mathfrak{q}_2$ de degré 1 au-dessus de 23, tel que $a_{\mathfrak{q}_2}(\mathfrak{f}) = \beta - 2$.

18. Démonstration du théorème 11

Posons $K_n = \mathbb{Q}(\mu_{2^{n+2}})^+$.

Lemme 34. *Toute courbe elliptique définie sur K_n est modulaire.*

Démonstration. Le corps K_n est le n-ième étage de la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$, d'où l'assertion [Thorne 2015, Theorem 1]. □

18.1. ***L'assertion* (1).** Elle est déjà connue si $p = 7$ [Tzermias 1998, Theorem 1] et si $p = 11$ [Gross et Rohrlich 1978]. Le fait que $F_5(K_2)$ soit trivial est une conséquence directe du théorème 2 de [Kraus 2018]. On supposera donc

$$p \geq 13.$$

On est amené à distinguer deux cas suivant que $p = 13$ ou $p \geq 17$ (car $4d = 16$).

18.1.1. *Cas où* $p \geq 17$.

Lemme 35. *Pour tout* $p \geq 17$, *la représentation* $\rho_{E_0,p}$ *est irréductible.*

Démonstration. On a $D_{K_2} = 2^{11}$ et $K_2 = \mathbb{Q}(\alpha)$ où

$$\alpha^4 - 4\alpha^2 + 2 = 0.$$

Posons $u = (\alpha+1)^2$. On a $u \in U_{K_2}^+$. Son polynôme minimal est $H_1^{(u)} = X^4 - 12X^3 + 34X^2 - 20X + 1$ et on a $H_1^{(u)}(1) = 4$. On vérifie que $H_2^{(u)}(1) = 2^{16} \cdot 17$. Par ailleurs, on a $p_0 = 17$ [Derickx 2016, Theorem 1.1], d'où le résultat si $p \neq 17$ (théorème 21).

Supposons $p = 17$. La courbe modulaire $X_0(17)$ est $\mathbb{Q}$-isomorphe à la courbe elliptique de conducteur 17, notée $17A1$ dans les tables de Cremona [1997], d'équation

$$y^2 + xy + y = x^3 - x^2 - x - 14.$$

Elle possède deux pointes, qui sont rationnelles sur $\mathbb{Q}$. Avec `Magma`, on constate que l'on a $X_0(17)(K) = X_0(17)(\mathbb{Q})$, qui est cyclique d'ordre 4. Les points non cuspidaux de $X_0(17)(\mathbb{Q})$ correspondent à deux classes d'isomorphisme de courbes elliptiques sur $\mathbb{Q}$ d'invariants modulaires (voir par exemple [Dahmen 2008, p. 30, Table 2.1])

$$j_1 = -\frac{17 \cdot 373^3}{2^{17}} \quad \text{et} \quad j_2 = -\frac{17^2 \cdot 101^3}{2}.$$

Ils sont distincts de $j(E_0)$. En effet, on peut supposer $v_{\mathscr{L}}(b) > 0$ et $v_{\mathscr{L}}(ac) = 0$; on a

$$j(E_0) = 2^8\left(\frac{(a^{34} + (ab)^{17} + b^{34})^3}{(abc)^{34}}\right),$$

d'où $v_{\mathscr{L}}(j(E_0)) = 32 - 34v_{\mathscr{L}}(abc)$. Par ailleurs, on a $v_{\mathscr{L}}(j_1) = -68$ et $v_{\mathscr{L}}(j_2) = -4$, ce qui entraîne l'assertion et le lemme. □

On constate dans les tables de [LMFDB 2013] que l'on a $|\mathcal{H}| = 0$, d'où le résultat dans ce cas.

18.1.2. *Cas où* $p = 13$. A priori, on ne peut plus normaliser $(a, b, c) \in F_{13}(K_2)$ de sorte que la courbe de Frey E_0/K_2 soit semi-stable. On va donc utiliser le théorème d'abaissement du niveau dans le cas général [Freitas et Siksek 2015a, Theorem 7].

Considérons un point $(a, b, c) \in F_{13}(K_2)$ tel que $abc \neq 0$ et que a, b, c soient premiers entre eux dans O_{K_2}. On a $v_{\mathscr{L}}(abc) \geq 1$. Soit E_0/K_2 la courbe elliptique d'équation

$$y^2 = x(x - a^{13})(x + b^{13}). \tag{18-1}$$

Rappelons que l'on a

$$c_4(E_0) = 2^4\big(a^{26} + (ab)^{13} + b^{26}\big) \quad \text{et} \quad \Delta(E_0) = 2^4(abc)^{26}. \tag{18-2}$$

Lemme 36. *La représentation* $\rho_{E_0,13}$ *est irréductible.*

Démonstration. Supposons $\rho_{E_0,13}$ réductible. Dans ce cas, E_0/K_2 possède un sous-groupe d'ordre 26 stable par $\mathrm{Gal}(\overline{K_2}/K_2)$. La courbe modulaire $X_0(26)$ possède donc un point rationnel sur K_2 qui n'est pas l'une de ses quatre pointes. Soit $\mathcal{C}/\mathbb{Q}$ la courbe hyperelliptique d'équation

$$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1.$$

Il existe un unique $\mathbb{Q}$-isomorphisme de $X_0(26)$ sur $\mathcal{C}$ appliquant les quatre pointes de $X_0(26)$ sur $(0, 1)$, $(0, -1)$ et les deux points à l'infini de $\mathcal{C}$ (cf. [Mazur et Vélu 1972]). Par suite, il existe un point $P = (x_0, y_0) \in \mathcal{C}(K_2)$ tel que $x_0 \neq 0$.

Soit $F/\mathbb{Q}$ la courbe elliptique d'équation, numérotée 26B1 dans les tables de Cremona, d'équation

$$Y^2 + XY + Y = X^3 - X^2 - 3X + 3.$$

Les formules

$$X = -\frac{(x+1)^2}{(x-1)^2} \quad \text{et} \quad Y = \frac{2(x(x-1) - y)}{(x-1)^3},$$

définissent un morphisme $\varphi : \mathcal{C} \to F$ de degré 2 [loc. cit., 2.3] On vérifie alors avec `Magma` que l'on a $F(K_2) = F(\mathbb{Q})$ qui est cyclique d'ordre 7. On en déduit que l'on a

$$F(K_2) = \big\{0, (-1, 2), (3, -6), (1, 0), (1, -2), (3, 2), (-1, -2)\big\}.$$

On a $x_0 \neq 1$ car sinon $y_0^2 = -16$, or -1 n'est pas un carré dans K_2. Parce que x_0 n'est pas nul, on a ainsi

$$\varphi(P) \in \big\{(3, -6), (1, 0), (1, -2), (3, 2)\big\}.$$

Cela conduit à une contradiction car -3 et -1 ne sont pas des carrés dans K_2, d'où le lemme. □

Remarque. Le même argument que celui utilisé dans démonstration du lemme 31, pour $p = 13$, ne convient pas ici pour conclure. En effet, on peut vérifier avec `Magma`, seulement conditionnellement, que le groupe des points K_2-rationnels de la courbe elliptique numérotée 52A1 dans les tables de Cremona est d'ordre 2.

Supposons $v_{\mathscr{L}}(abc) \geq 2$. Dans ce cas, par les mêmes arguments que ceux utilisés dans la démonstration de la proposition 16, on peut encore normaliser (a, b, c) de sorte que E_0 ait réduction de type multiplicatif en $\mathscr{L}$ et que E_0 soit semi-stable. On peut alors conclure comme dans l'alinéa précédent.

Supposons donc désormais que l'on a

$$v_{\mathscr{L}}(abc) = 1. \tag{18-3}$$

Lemme 37. *Quitte à multiplier (a, b, c) par une unité convenable de O_{K_2}, on a*

$$v_{\mathscr{L}}(N_{E_0}) \in \{5, 6, 8\}.$$

Démonstration. D'après (18-2) et (18-3), on a

$$v_{\mathscr{L}}(c_4(E_0)) = 16, \quad v_{\mathscr{L}}(c_6(E_0)) = 24, \quad v_{\mathscr{L}}(\Delta(E_0)) = 42. \tag{18-4}$$

On a $v_{\mathscr{L}}(j_{E_0}) = 6$, donc E_0 a potentiellement bonne réduction en $\mathscr{L}$.

On peut supposer que l'on a $v_{\mathscr{L}}(b) = 1$, auquel cas $v_{\mathscr{L}}(ac) = 0$. Par ailleurs, il existe une unité ε de O_{K_2} telle que l'on ait $\varepsilon a + 1 \equiv 0 \pmod 4$ (Appendice, théorème 39 et lemme 41). En remplaçant (a, b, c) par $(\varepsilon a, \varepsilon b, \varepsilon c)$, on se ramène au cas où l'on a

$$a^{13} + 1 \equiv 0 \pmod 4. \tag{18-5}$$

Le modèle (18-1) n'est pas minimal en $\mathscr{L}$. En effet, posons

$$x = \alpha^4 X \quad \text{et} \quad y = \alpha^6 Y + \alpha^4 X.$$

On obtient comme nouveau modèle

$$(W): \qquad Y^2 + \frac{2}{\alpha^2} XY = X^3 + \left(\frac{b^{13} - a^{13} - 1}{\alpha^4}\right) X^2 - \frac{(ab)^{13}}{\alpha^8} X.$$

D'après (18-5) et le fait que 2 soit associé à α^4, c'est un modèle entier. On a

$$c_4(E_0) = \alpha^8 c_4(W), \quad c_6(E_0) = \alpha^{12} c_6(W), \quad \Delta(E_0) = \alpha^{24} \Delta(W),$$

d'où (formules (18-4))

$$v_{\mathscr{L}}(c_4(W)) = 8, \quad v_{\mathscr{L}}(c_6(W)) = 12, \quad v_{\mathscr{L}}(\Delta(W)) = 18.$$

On vérifie avec les tables de [Papadopoulos 1993] que le type de Néron en $\mathscr{L}$ de (W) est I_6^* ou bien que (W) n'est pas minimal en $\mathscr{L}$. Si le type de Néron est I_6^*, on a $v_{\mathscr{L}}(N_{E_0}) = 8$. Si (W) n'est pas minimal, le triplet de valuations de ses invariants minimaux en $\mathscr{L}$ est $(4, 6, 6)$. On constate alors que son type de Néron est II, auquel cas $v_{\mathscr{L}}(N_{E_0}) = 6$, ou bien que son type de Néron est III et on a $v_{\mathscr{L}}(N_{E_0}) = 5$, d'où le lemme. □

Supposons (a, b, c) normalisé comme dans l'énoncé du lemme précédent. Notons $\mathcal{S}_2^+(\mathscr{L}^r)$ le $\mathbb{C}$-espace vectoriel engendré par les newforms modulaires paraboliques de Hilbert sur K_2, de poids parallèle 2 et de niveau $\mathscr{L}^r$. On a [LMFDB 2013]

$$\dim \mathcal{S}_2^+(\mathscr{L}^5) = 1, \quad \dim \mathcal{S}_2^+(\mathscr{L}^6) = 3 \quad \text{et} \quad \dim \mathcal{S}_2^+(\mathscr{L}^8) = 8.$$

Compte tenu des lemmes 34 et 36, les conditions du théorème d'abaissement du niveau sont satisfaites [Freitas et Siksek 2015a, Theorem 7]. Il existe donc $\mathfrak{f} \in \mathcal{S}_2^+(\mathscr{L}^r)$ avec $r \in \{5, 6, 8\}$ et un idéal premier $\mathfrak{p}$ au-dessus de 13 dans $O_{\mathbb{Q}_{\mathfrak{f}}}$, tels que

$$\rho_{\mathfrak{f},\mathfrak{p}} \simeq \rho_{E_0,13}.$$

Considérons alors le nombre premier 79. Il est totalement décomposé dans K_2. Soit $\mathfrak{q}$ un idéal premier de O_{K_2} au-dessus de 79. On constate que l'on a

$$a_{\mathfrak{q}}(\mathfrak{f}) \in \{-8, 0, 8\}.$$

Si E_0 a réduction multiplicative en $\mathfrak{q}$, on a

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv \pm 2 \pmod{\mathfrak{p}},$$

ce qui n'est pas. Ainsi E_0 a bonne réduction en $\mathfrak{q}$. On a donc la congruence

$$a_{\mathfrak{q}}(E_0) \equiv a_{\mathfrak{q}}(\mathfrak{f}) \pmod{\mathfrak{p}}.$$

On a $v_{\mathfrak{q}}(abc) = 0$, donc a^{13}, b^{13}, c^{13} sont des racines 6-ièmes de l'unité modulo $\mathfrak{q}$. On a ainsi

$$a^{13}, b^{13}, c^{13} \equiv 1, 23, 24, 55, 56, 78 \pmod{\mathfrak{q}}.$$

L'égalité $a^{13} + b^{13} + c^{13} = 0$ implique

$$(a^{13}, b^{13}) \equiv (1, 23), (1, 55), (23, 1), (23, 55), (24, 56), (24, 78), (55, 1), (55, 23), (56, 24), (56, 78), (78, 24), (78, 56) \pmod{\mathfrak{q}}.$$

Dans tous les cas, on obtient

$$a_{\mathfrak{q}}(E_0) = \pm 4,$$

d'où la contradiction cherchée et le résultat pour $p = 13$.

18.2. ***L'assertion* (2).**

Lemme 38. *Pour tout $p > 6724$, la représentation $\rho_{E_0,p}$ est irréductible.*

Démonstration. On a $D_{K_3} = 2^{31}$ et $K_3 = \mathbb{Q}(\alpha)$ où

$$\alpha^8 - 8\alpha^6 + 20\alpha^4 - 16\alpha^2 + 2 = 0.$$

Posons

$$u_1 = \left(-\alpha^6 - 2\alpha^5 + 5\alpha^4 + 10\alpha^3 - 4\alpha^2 - 9\alpha - 1\right)^2, \quad u_2 = \left(\alpha^7 + \alpha^6 - 6\alpha^5 - 5\alpha^4 + 9\alpha^3 + 5\alpha^2 - 3\alpha - 1\right)^2,$$
$$u_3 = \left(-2\alpha^7 - 2\alpha^6 + 11\alpha^5 + 10\alpha^4 - 13\alpha^3 - 9\alpha^2 + \alpha + 1\right)^2.$$

Ce sont des unité totalement positives de O_{K_3}. En utilisant le théorème 21 avec les u_i, on vérifie que on a l'implication

$$R_{K_3} \equiv 0 \pmod{p} \;\Rightarrow\; p \leq 607.$$

Par ailleurs, on a $p_0 < 6724$ (voir [Oesterlé 1996; Derickx 2016]), d'où l'assertion. □

Les conditions du théorème 22 sont satisfaites. On constate avec `Magma` que l'on a $|\mathcal{H}| = 40$. À conjugaison près, $\mathcal{H}$ est formé de quatre newforms $\mathfrak{f}$ telles que $[\mathbb{Q}_{\mathfrak{f}} : \mathbb{Q}] = 4$ et d'une newform dont le corps de rationalité est de degré 24 sur $\mathbb{Q}$.

Les nombres premiers 31 et 97 sont totalement décomposés dans K_3. En utilisant la proposition 24, et en prenant pour $\mathfrak{q}$ un idéal premier de O_{K_3} au-dessus de 31, puis un idéal premier au-dessus de 97, on obtient alors le résultat.

Partie V. Appendice

Soit K un corps de nombres totalement réel. Notons K^{4O_K} le corps de classes de rayon modulo $4O_K$ sur K. On établit ici l'énoncé suivant, que l'on utilise, tout au moins sa première assertion, dans les démonstrations du théorème 6, de la proposition 16 et du lemme 37.

Théorème 39. (1) *Supposons* 2 *totalement ramifié dans* K *et* $h_K^+ = 1$. *Alors, on a* $K = K^{4O_K}$.

(2) *Supposons* $K = K^{4O_K}$. *Alors, on a* $h_K^+ = 1$.

En particulier :

Corollaire 40. *Supposons* 2 *totalement ramifié dans* K. *On a* $h_K^+ = 1$ *si et seulement si* $K = K^{4O_K}$.

18.3. ***Résultats préliminaires.*** Notons U_K le groupe des unités de O_K et h_K le nombre de classes de K. Rappelons que d désigne le degré de K sur $\mathbb{Q}$. Posons

$$G = (O_K/4O_K)^*.$$

Soit $\varphi : U_K \to G$ le morphisme qui à $u \in U_K$ associe $u + 4O_K$.

Lemme 41. *On a* $K = K^{4O_K}$ *si et seulement si* $h_K = 1$ *et* φ *est une surjection sur* G.

Démonstration. C'est conséquence directe de [Cohen 2000, Proposition 3.2.3]. □

Lemme 42. *Les deux conditions suivantes sont équivalentes* :

(1) *On a* $h_K^+ = 1$.

(2) *On a* $h_K = 1$ *et toute unité totalement positive est un carré dans* K.

Démonstration. On a l'égalité (cf. [Cohen 2000, Proposition 3.2.3], avec pour $\mathfrak{m}$ le produit des places à l'infini)

$$h_K^+ = \frac{2^d}{[U_K : U_K^+]} h_K.$$

Supposons $h_K^+ = 1$. On a alors $h_K = 1$, puis $[U_K : U_K^+] = 2^d$. D'après le théorème de Dirichlet, on a $[U_K : U_K^2] = 2^d$, d'où $U_K^+ = U_K^2$. Inversement, si $h_K = 1$ et $U_K^+ = U_K^2$, la formule ci-dessus implique $h_K^+ = 1$. □

Lemme 43. *Supposons* 2 *totalement ramifié dans* K. *On a*

$$|G/G^2| = 2^d.$$

Démonstration. Soit a un élément de G. Soit $\mathscr{L}$ l'idéal premier de O_K au-dessus de 2. On a $O_K/\mathscr{L} = \mathbb{F}_2$, donc il existe $x \in \mathscr{L}$ tel que $a = 1 + x + 4O_K$. On a $a^2 = 1 + x(2 + x) + 4O_K$, d'où il résulte que l'on a

$$a^2 = 1 \Leftrightarrow x \in 2O_K.$$

Posons $G[2] = \{z \in G \mid z^2 = 1\}$. On en déduit une application $f : G[2] \to 2O_K/4O_K$ définie pour tout $a \in G[2]$ par l'égalité

$$f(a) = x + 4O_K \quad \text{où} \quad a = 1 + x + 4O_K.$$

C'est un isomorphisme de groupes. Le groupe $2O_K/4O_K$ est isomorphe à $O_K/2O_K$ qui est d'ordre 2^d. Par ailleurs, les ordres de $G[2]$ et G/G^2 sont égaux, d'où le lemme. □

Lemme 44. *Supposons* 2 *totalement ramifié dans* K. *Les deux conditions suivantes sont équivalentes* :

(1) *On a* $K = K^{4O_K}$.

(2) *On a* $h_K = 1$ *et toute unité congrue à un carré modulo* 4 *est un carré dans* K.

Démonstration. Notons $\psi : U_K \to G \to G/G^2$ le morphisme naturel déduit de φ.

Supposons $K = K^{4O_K}$. Le morphisme ψ est une surjection (lemme 41). Les ordres de U_K/U_K^2 et G/G^2 sont égaux (lemme 43). Par suite, U_K^2 est le noyau de ψ, donc toute unité congrue à un carré modulo 4 est un carré.

Inversement, supposons la seconde condition satisfaite. Démontrons que le morphisme φ est surjectif, ce qui, d'après le lemme 41, impliquera la première assertion. D'après l'hypothèse faite, le noyau de ψ est U_K^2. Les ordres de U_K/U_K^2 et G/G^2 étant égaux, on en déduit que ψ est une surjection. Ainsi, l'image de $\varphi(U_K)$ dans G/G^2 est G/G^2. Parce que 2 est totalement ramifié dans K, G est un 2-groupe [Cohen 2000, p. 137]. Il en résulte que $\varphi(U_K) = G$, d'où le résultat. (Si p est premier, le sous-groupe de Frattini d'un p-groupe abélien fini A est A^p, voir par exemple [Rotman 1995, Theorem 5.48]. Si B est un sous-groupe de A tel que $BA^p = A$, on a donc $A = B$.) □

18.4. ***Fin de la démonstration du théorème 39.*** (1) Supposons 2 totalement ramifié dans K et $h_K^+ = 1$. Soit u une unité de O_K congrue à un carré modulo 4. L'extension $K(\sqrt{u})/K$ est alors partout non ramifiée aux places finies de K [Cox 1989, Lemma 5.32, p. 114]. On a $h_K^+ = 1$, donc u est un carré dans K. Vu que $h_K = 1$, on a donc $K = K^{4O_K}$ (lemme 44).

(2) Supposons $K = K^{4O_K}$. On a $h_K = 1$. Soit u une unité totalement positive de O_K. D'après le lemme 42, il s'agit de montrer que u est un carré dans K. L'extension $K(\sqrt{u})/K$ est non ramifiée aux places à l'infini et en dehors des idéaux premiers de O_K au-dessus de 2. Le conducteur de l'extension $K(\sqrt{u})/K$ est égal à son discriminant [Cassels et Fröhlich 1967, p. 160], qui divise $4O_K$. Par suite, $K(\sqrt{u})$ est contenu dans K^{4O_K}, d'où $K(\sqrt{u}) = K$ et notre assertion.

Remerciements

J'ai bénéficié de conversations avec J. Oesterlé concernant l'Appendice de cet article et son application au théorème 6. Je l'en remercie vivement. Je remercie également R. Barbaud pour l'aide qu'il m'a apportée dans la réalisation de certains programmes intervenant dans le logiciel `Magma`, ainsi que D. Bernardi pour les commentaires dont il m'a fait part. Par ailleurs, je remercie le referee de cet article pour sa lecture détaillée et pour toutes ses remarques.

Bibliographie

[Anni et Siksek 2016] S. Anni et S. Siksek, "Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$", *Algebra Number Theory* **10**:6 (2016), 1147–1172. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon et C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond et R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR Zbl

[Browkin 2006] J. Browkin, "The *abc*-conjecture for algebraic numbers", *Acta Math. Sin.* (*Engl. Ser.*) **22**:1 (2006), 211–222. MR Zbl

[Bruin et Najman 2016] P. Bruin et F. Najman, "A criterion to rule out torsion groups for elliptic curves over number fields", *Res. Number Theory* **2** (2016), art. id. 3. MR Zbl

[Cassels et Fröhlich 1967] J. W. S. Cassels et A. Fröhlich (éditeurs), *Algebraic number theory* (Brighton, 1965), Academic Press, London, 1967. MR

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Math. **193**, Springer, 2000. MR Zbl

[Cox 1989] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, New York, 1989. MR

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd éd., Cambridge Univ. Press, 1997. MR Zbl

[Cremona et Dembélé 2014] J. E. Cremona et L. Dembélé, "Modular forms over number fields", preprint, 2014, https ://tinyurl.com/cremdem.

[Dahmen 2008] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, Utrecht University, 2008, https ://tinyurl.com/srdahmen.

[Dembélé et Voight 2013] L. Dembélé et J. Voight, "Explicit methods for Hilbert modular forms", pp. 135–198 dans *Elliptic curves, Hilbert modular forms and Galois deformations*, édité par H. Darmon et al., Birkhäuser, Basel, 2013. MR Zbl

[Derickx 2016] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, Ph.D. thesis, Leiden University, 2016, http ://hdl.handle.net/1887/43186.

[Freitas et Siksek 2015a] N. Freitas et S. Siksek, "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields", *Compos. Math.* **151**:8 (2015), 1395–1415. MR Zbl

[Freitas et Siksek 2015b] N. Freitas et S. Siksek, "Fermat's last theorem over some small real quadratic fields", *Algebra Number Theory* **9**:4 (2015), 875–895. MR Zbl

[Freitas et Siksek 2018] N. Freitas et S. Siksek, "On the asymptotic Fermat's last theorem", preprint, 2018. arXiv

[Freitas et al. 2015] N. Freitas, B. V. Le Hung et S. Siksek, "Elliptic curves over real quadratic fields are modular", *Invent. Math.* **201**:1 (2015), 159–206. MR Zbl

[Fukuda et Komatsu 2011] T. Fukuda et K. Komatsu, "Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III", *Int. J. Number Theory* **7**:6 (2011), 1627–1635. MR Zbl

[Gross et Rohrlich 1978] B. H. Gross et D. E. Rohrlich, "Some results on the Mordell–Weil group of the Jacobian of the Fermat curve", *Invent. Math.* **44**:3 (1978), 201–224. MR Zbl

[Jarvis et Meekin 2004] F. Jarvis et P. Meekin, "The Fermat equation over $\mathbb{Q}(\sqrt{2})$", *J. Number Theory* **109**:1 (2004), 182–196. MR Zbl

[Klassen et Tzermias 1997] M. Klassen et P. Tzermias, "Algebraic points of low degree on the Fermat quintic", *Acta Arith.* **82**:4 (1997), 393–401. MR Zbl

[Kraus 2007] A. Kraus, "Courbes elliptiques semi-stables sur les corps de nombres", *Int. J. Number Theory* **3**:4 (2007), 611–633. MR Zbl

[Kraus 2018] A. Kraus, "Quartic points on the Fermat quintic", *Ann. Math. Blaise Pascal* **25**:1 (2018), 199–205. MR Zbl

[LMFDB 2013] LMFDB Collaboration, "The L-functions and modular forms database", 2013, http ://www.lmfdb.org.

[Mazur et Vélu 1972] B. Mazur et J. Vélu, "Courbes de Weil de conducteur 26", *C. R. Acad. Sci. Paris Sér. A-B* **275** (1972), 743–745. MR Zbl

[Merel 1996] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124**:1-3 (1996), 437–449. MR Zbl

[Oesterlé 1996] J. Oesterlé, note non publiée, 1996.

[Papadopoulos 1993] I. Papadopoulos, "Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3", *J. Number Theory* **44**:2 (1993), 119–152. MR Zbl

[Parent 2003] P. Parent, "No 17-torsion on elliptic curves over cubic number fields", *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838. MR Zbl

[PARI 2015] PARI Group, PARI/GP version 2.7.3, 2015, http ://pari.math.u-bordeaux.fr.

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

[Rotman 1995] J. J. Rotman, *An introduction to the theory of groups*, 4th éd., Graduate Texts in Math. **148**, Springer, 1995. MR Zbl

[Şengün et Siksek 2018] M. H. Şengün et S. Siksek, "On the asymptotic Fermat's last theorem over number fields", *Comment. Math. Helv.* **93**:2 (2018), 359–375. MR Zbl

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR Zbl

[Serre 1987] J.-P. Serre, "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$", *Duke Math. J.* **54**:1 (1987), 179–230. MR Zbl

[Siegel 1929] C. L. Siegel, "Über einige Anwendungen diophantischer Approximationen", *Abh. Preuß. Akad. Wiss., Phys.-Math. Kl.* **1929**:1 (1929), 1–41. JFM

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd éd., Graduate Texts in Math. **106**, Springer, 2009. MR Zbl

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Math. Soc. Student Texts **41**, Cambridge Univ. Press, 1998. MR Zbl

[Taylor et Wiles 1995] R. Taylor et A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* (2) **141**:3 (1995), 553–572. MR Zbl

[Thorne 2015] J. A. Thorne, "Elliptic curves over $\mathbb{Q}_\infty$ are modular", 2015. À paraître dans *J. Eur. Math. Soc.* arXiv

[Tzermias 1998] P. Tzermias, "Algebraic points of low degree on the Fermat curve of degree seven", *Manuscripta Math.* **97**:4 (1998), 483–488. MR Zbl

[Voight] J. Voight, "Tables of totally real number fields", https ://math.dartmouth.edu/∼jvoight/nf-tables.

[Waterhouse 1969] W. C. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. École Norm. Sup.* (4) **2**:4 (1969), 521–560. MR Zbl

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

Communicated by Christopher Skinner
Received 2017-09-24 Revised 2018-04-13 Accepted 2018-09-23

alain.kraus@imj-prg.fr *Institut de Mathématiques de Jussieu - Paris Rive Gauche, Sorbonne Université, UMR 7586 CNRS - Paris Diderot, 75005 Paris, France*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA
Antoine Chambert-Loir	Université Paris-Diderot, France
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France
Brian D. Conrad	Stanford University, USA
Samit Dasgupta	University of California, Santa Cruz, USA
Hélène Esnault	Freie Universität Berlin, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany
Hubert Flenner	Ruhr-Universität, Germany
Sergey Fomin	University of Michigan, USA
Edward Frenkel	University of California, Berkeley, USA
Andrew Granville	Université de Montréal, Canada
Joseph Gubeladze	San Francisco State University, USA
Roger Heath-Brown	Oxford University, UK
Craig Huneke	University of Virginia, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA
János Kollár	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne
Susan Montgomery	University of Southern California, USA
Shigefumi Mori	RIMS, Kyoto University, Japan
Martin Olsson	University of California, Berkeley, USA
Raman Parimala	Emory University, USA
Jonathan Pila	University of Oxford, UK
Anand Pillay	University of Notre Dame, USA
Michael Rapoport	Universität Bonn, Germany
Victor Reiner	University of Minnesota, USA
Peter Sarnak	Princeton University, USA
Joseph H. Silverman	Brown University, USA
Michael Singer	North Carolina State University, USA
Christopher Skinner	Princeton University, USA
Vasudevan Srinivas	Tata Inst. of Fund. Research, India
J. Toby Stafford	University of Michigan, USA
Pham Huu Tiep	University of Arizona, USA
Ravi Vakil	Stanford University, USA
Michel van den Bergh	Hasselt University, Belgium
Akshay Venkatesh	Institute for Advanced Study, USA
Marie-France Vignéras	Université Paris VII, France
Kei-Ichi Watanabe	Nihon University, Japan
Melanie Matchett Wood	University of Wisconsin, Madison, USA
Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2019 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 13 No. 2 2019

High moments of the Estermann function 251
SANDRO BETTIN

Le théorème de Fermat sur certains corps de nombres totalement réels 301
ALAIN KRAUS

G-valued local deformation rings and global lifts 333
REBECCA BELLOVIN and TOBY GEE

Functorial factorization of birational maps for qe schemes in characteristic 0 379
DAN ABRAMOVICH and MICHAEL TEMKIN

Effective generation and twisted weak positivity of direct images 425
YAJNASENI DUTTA and TAKUMI MURAYAMA

Lovász–Saks–Schrijver ideals and coordinate sections of determinantal varieties 455
ALDO CONCA and VOLKMAR WELKER

On rational singularities and counting points of schemes over finite rings 485
ITAY GLAZER

The Maillot–Rössler current and the polylogarithm on abelian schemes 501
GUIDO KINGS and DANNY SCARPONI

Essential dimension of inseparable field extensions 513
ZINOVY REICHSTEIN and ABHISHEK KUMAR SHUKLA

1937-0652(2019)13:2;1-B