COMPOSITIO MATHEMATICA

The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields

Nuno Freitas and Samir Siksek

Compositio Math. **151** (2015), 1395–1415.

doi:10.1112/S0010437X14007957

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
150 YEARS

Compositio Math. 151 (2015) 1395–1415
doi:10.1112/S0010437X14007957

The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields

Nuno Freitas and Samir Siksek

Abstract

Let K be a totally real field. By the *asymptotic Fermat's Last Theorem over* K we mean the statement that there is a constant B_K such that for any prime exponent $p > B_K$, the only solutions to the Fermat equation

$$a^p + b^p + c^p = 0, \quad a, b, c \in K$$

are the trivial ones satisfying $abc = 0$. With the help of modularity, level lowering and image-of-inertia comparisons, we give an algorithmically testable criterion which, if satisfied by K, implies the asymptotic Fermat's Last Theorem over K. Using techniques from analytic number theory, we show that our criterion is satisfied by $K = \mathbb{Q}(\sqrt{d})$ for a subset of $d \geqslant 2$ having density $\frac{5}{6}$ among the squarefree positive integers. We can improve this density to 1 if we assume a standard 'Eichler–Shimura' conjecture.

1. Introduction

1.1 Historical background

Interest in the Fermat equation over various number fields goes back to the 19th and early 20th centuries. For example, Dickson's *History of the Theory of Numbers* [Dic71, pp. 758 and 768] mentions extensions by Maillet (1897) and Furtwängler (1910) of the classical ideas of Kummer to the Fermat equation $x^p + y^p = z^p$, with $p > 3$ prime, over the cyclotomic field $\mathbb{Q}(\zeta_p)$. The ultimate work in this direction [Kol01] is due to Kolyvagin, who showed, among many other results, that if $x^p + y^p = z^p$ has a first case solution in $\mathbb{Q}(\zeta_p)$, then $p^2 \mid (q^p - q)$ for all prime $q \leqslant 89$ (here 'first case' means that $(1 - \zeta_p) \nmid xyz$). For $d \neq 0, 1$ and squarefree, Hao and Parry [HP84] used the Kummer approach to prove several results on the Fermat equation with prime exponent p over $\mathbb{Q}(\sqrt{d})$, subject to the condition that p does not divide the class number of $\mathbb{Q}(\sqrt{d}, \zeta_p)$ (see also [HP84] for references to early work on the Fermat equation with various small exponents over quadratic and cubic fields). Other authors (e.g. [DK94, Fad61, Tze03]) have treated the Fermat equation with fixed exponent p as a curve, and determined the points of low degree subject to restrictions on the Mordell–Weil group of its Jacobian. A beautiful example of this approach is the work of Gross and Rohrlich [GR78, Theorem 5], who determined for $p = 3$, 5, 7 and 11 the solutions to $x^p + y^p = z^p$ over all number fields K of degree no greater than $(p - 1)/2$.

Received 20 April 2014, accepted in final form 8 September 2014, published online 6 March 2015.
2010 Mathematics Subject Classification 11D41 (primary), 11F80, 11F03 (secondary).
Keywords: Fermat, modularity, Galois representation, level lowering.
The first author was supported through a grant within the framework of the DFG Priority Programme 1489 *Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory*. The second author was supported by an EPSRC Leadership Fellowship EP/G007268/1 and EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

However, the elementary, cyclotomic and Mordell–Weil approaches to the Fermat equation have had limited success. Indeed, even over $\mathbb{Q}$, no combination of these approaches is known to yield a proof of Fermat's Last Theorem for infinitely many prime exponents p. We therefore look to Wiles's proof of Fermat's Last Theorem [TW95, Wil95] for inspiration. Modularity of elliptic curves plays a crucial rôle in the proof, yet our understanding of modularity for elliptic curves over general number fields is still embryonic. In contrast, there is a powerful modularity theory for elliptic curves over totally real fields, and it would be natural to apply this theory to the study of the Fermat equation over totally real fields. The only work in this direction that we are aware of is that of Jarvis and Meekin [JM04], who showed that the Fermat equation $x^n+y^n=z^n$ has no solutions $x, y, z \in \mathbb{Q}(\sqrt{2})$ with $xyz \neq 0$ and $n \geqslant 4$.

1.2 Our results

In this paper we combine modularity and level lowering with image-of-inertia comparisons and techniques from analytic number theory to prove several results concerning the Fermat equation over totally real fields. Let K be a totally real field, and let $\mathcal{O}_K$ be its ring of integers. By the *Fermat equation with exponent p over K* we mean the equation

$$a^p + b^p + c^p = 0, \quad a, b, c \in \mathcal{O}_K. \tag{1}$$

A solution (a, b, c) is said to be *trivial* if $abc = 0$; otherwise it is *non-trivial*. The *asymptotic Fermat's Last Theorem over K* is the statement that there is some bound B_K such that for any prime $p > B_K$, all solutions to the Fermat equation (1) are trivial. If B_K is effectively computable, we shall refer to this statement as the *effective asymptotic Fermat's Last Theorem over K*.

Theorem 1. *Let $d \geqslant 2$ be squarefree, satisfying one of the following conditions:*

(i) $d \equiv 3 \pmod 8$;
(ii) $d \equiv 6$ *or* $10 \pmod{16}$;
(iii) $d \equiv 2 \pmod{16}$ *and d has some prime divisor* $q \equiv 5$ *or* $7 \pmod 8$;
(iv) $d \equiv 14 \pmod{16}$ *and d has some prime divisor* $q \equiv 3$ *or* $5 \pmod 8$.

Then the effective asymptotic Fermat's Last Theorem holds over $K = \mathbb{Q}(\sqrt{d})$.

To state our other theorems, we need the following standard conjecture, which of course is a generalization of the Eichler–Shimura theorem over $\mathbb{Q}$.

Conjecture 1 ('Eichler–Shimura'). Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2 and with rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

Theorem 2. *Let $d > 5$ be squarefree, satisfying $d \equiv 5 \pmod 8$. Write $K = \mathbb{Q}(\sqrt{d})$ and assume Conjecture 1 for K. Then the effective asymptotic Fermat's Last Theorem holds over K.*

To state our general theorem, let K be a totally real field, and let

$$\begin{gathered} S = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}, \\ T = \{\mathfrak{P} \in S : f(\mathfrak{P}/2) = 1\}, \quad U = \{\mathfrak{P} \in S : 3 \nmid v_{\mathfrak{P}}(2)\}. \end{gathered} \tag{2}$$

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Here $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. We need the following assumption, which we shall refer to as (ES) throughout the paper:

$$\textbf{(ES)} \quad \begin{cases} \text{either } [K:\mathbb{Q}] \text{ is odd,} \\ \text{or } T \neq \emptyset, \\ \text{or Conjecture 1 holds for } K. \end{cases}$$

Theorem 3. *Let K be a totally real field satisfying (ES). Let S, T and U be as in (2). Write $\mathcal{O}_S^*$ for the group of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^*, \tag{3}$$

either:

(A) *there is some $\mathfrak{P} \in T$ that satisfies $\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leqslant 4\, v_{\mathfrak{P}}(2)$; or*

(B) *there is some $\mathfrak{P} \in U$ that satisfies both $\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leqslant 4\, v_{\mathfrak{P}}(2)$ and $v_{\mathfrak{P}}(\lambda\mu) \equiv v_{\mathfrak{P}}(2) \pmod 3$.*

Then the asymptotic Fermat's Last Theorem holds over K.

We make the following remarks.

- In contrast to Theorems 1 and 2, the constant B_K implicit in the statement of Theorem 3 is ineffective, though it is effectively computable if we assume a suitable modularity statement, such as modularity of elliptic curves over K with full 2-torsion. Elliptic curves over real quadratic fields are modular [FLHS], so the implicit constants B_K in Theorems 1 and 2 are effectively computable.
- By Siegel [Sie29], S-unit equations have a finite number of solutions. These are effectively computable (see, e.g., [Sma98]). Thus, for any totally real field K, there is an algorithm for deciding whether the hypotheses of Theorem 3 are satisfied.
- The S-unit equation (3) has precisely three solutions in $\mathbb{Q} \cap \mathcal{O}_S^*$, namely $(\lambda, \mu) = (2, -1)$, $(-1, 2)$ and $(\frac{1}{2}, \frac{1}{2})$. We shall call these the *irrelevant solutions* to (3), with other solutions being called *relevant*. The irrelevant solutions satisfy condition (A) if $T \neq \emptyset$ and condition (B) if $U \neq \emptyset$.

It is natural to ask, for fixed $n \geqslant 2$, what 'proportion' of totally real fields of degree n are such that the S-unit equation (3) has no relevant solutions. We answer this for $n = 2$. Specifically, let $\mathbb{N}^{\mathrm{sf}} = \{d \geqslant 2 : d \text{ squarefree}\}$. The elements of $\mathbb{N}^{\mathrm{sf}}$ are in bijection with the real quadratic fields via $d \leftrightarrow K = \mathbb{Q}(\sqrt{d})$. For a subset $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, we define the *relative density of $\mathcal{U}$ in $\mathbb{N}^{\mathrm{sf}}$* by

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{U} : d \leqslant X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} : d \leqslant X\}}, \tag{4}$$

provided the limit exists. Let

$$\begin{gathered} \mathcal{C} = \{d \in \mathbb{N}^{\mathrm{sf}} : \text{the } S\text{-unit equation (3) has no relevant solutions in } \mathbb{Q}(\sqrt{d})\}, \\ \mathcal{D} = \{d \in \mathcal{C} : d \not\equiv 5 \pmod 8\}. \end{gathered} \tag{5}$$

Theorem 4. *Let $\mathcal{C}$ and $\mathcal{D}$ be as above. Then*

$$\delta_{\mathrm{rel}}(\mathcal{C}) = 1, \quad \delta_{\mathrm{rel}}(\mathcal{D}) = 5/6. \tag{6}$$

If $d \in \mathcal{D}$, then the effective asymptotic Fermat's Last Theorem holds for $K = \mathbb{Q}(\sqrt{d})$. The same conclusion holds for $d \in \mathcal{C}$ if we assume Conjecture 1.

In other words, we are able to effectively bound the exponent in the Fermat equation unconditionally for $\frac{5}{6}$ of real quadratic fields; and, assuming Conjecture 1, we can do this for almost all real quadratic fields.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

1.3 A quartic example

Let $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, which is plainly a totally real quartic field. Let $\mathfrak{P} = \sqrt{2+\sqrt{2}} \cdot \mathcal{O}_K$. Then $2\mathcal{O}_K = \mathfrak{P}^4$. It follows that $S = T = \{\mathfrak{P}\}$. In particular, the field K satisfies hypothesis (ES). Using [Sma97, Sma99] and a computation in the computer algebra system `Magma` [BCP97], we determined the solutions to the S-unit equation (3); we omit the computational details. There are 585 solutions (including the three irrelevant solutions), which we do not list here. We computed the possible values of $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\}$ for these 585 solutions and found them to be $1, 2, \ldots, 11$, so condition (A) of Theorem 3 is satisfied. Thus the asymptotic Fermat's Last Theorem holds for K.

1.4 Limitations of the original Fermat's Last Theorem strategy and variants

We now answer the obvious question of how the proofs of the above differ from the proof of Fermat's Last Theorem over $\mathbb{Q}$. A basic sketch of the proof over $\mathbb{Q}$ is as follows. Suppose that $a, b, c \in \mathbb{Q}$ satisfy $a^p + b^p + c^p = 0$ with $abc \neq 0$ and $p \geqslant 5$ prime. Scale a, b and c so that they become coprime integers. After possibly permuting a, b and c and changing signs, we may suppose that $a \equiv -1 \pmod 4$ and $2 \mid b$. Consider the Frey elliptic curve

$$E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p), \tag{7}$$

and let $\overline{\rho}_{E,p}$ be its mod p Galois representation, where $E = E_{a,b,c}$. Then $\overline{\rho}_{E,p}$ is irreducible by [Maz78] and modular by [Wil95, TW95]. Application of Ribet's level-lowering theorem [Rib90] shows that $\overline{\rho}_{E,p}$ arises from a weight 2 newform of level 2; but there are no such newforms, giving a contradiction. Enough of modularity, irreducibility and level lowering are now known for totally real fields that we may attempt to carry out the same strategy over those fields. Let K be a totally real field. If $a, b, c \in K$ satisfy $a^p + b^p + c^p = 0$ and $abc \neq 0$, we can certainly scale a, b and c so that they belong to the ring of integers $\mathcal{O}_K$, and thus (a, b, c) is a non-trivial solution to (1). If the class number of $\mathcal{O}_K$ is greater than 1, we cannot assume coprimality of a, b and c. We can, however, choose a finite set $\mathcal{H}$ of prime ideals that represent the class group, and assume (after suitable scaling) that a, b and c belong to $\mathcal{O}_K$ and are coprime away from $\mathcal{H}$. The Frey curve $E_{a,b,c}$ (again defined by (7) but over K) is semistable outside $S \cup \mathcal{H}$, where S is given in (2). However, the non-triviality of the class group obstructs the construction of a Frey curve that is semistable outside S. Applying level lowering to $\overline{\rho}_{E,p}$ yields a Hilbert newform $\mathfrak{f}$ of parallel weight 2 and level divisible only by the primes in $S \cup \mathcal{H}$. In general, there are newforms at these levels. This situation was analysed by Jarvis and Meekin [JM04], who found that

> *'... the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$ ... there are no other real quadratic fields for which this is true ...'*

It is helpful here to make a comparison with the equation $x^p + y^p + L^\alpha z^p = 0$ over $\mathbb{Q}$, with L an odd prime, considered by Serre and Mazur [Ser87, p. 204]. A non-trivial solution to this latter equation gives rise, via modularity and level lowering, to a classical weight-2 newform f of level $2L$; for $L \geqslant 13$, there are such newforms and we face the same difficulty. Mazur showed, however, that if p is sufficiently large, then f corresponds to an elliptic curve E' with full 2-torsion and conductor $2L$, and by classifying such elliptic curves he concluded that L is either a Fermat or a Mersenne prime. (Mazur's argument is unpublished but can be found in [Coh07, § 15.5].) Mazur's argument adapted to our setting tells us that a non-trivial solution to the Fermat equation over K with p sufficiently large gives rise to E' with full 2-torsion and good reduction outside $S \cup \mathcal{H}$ (assumption (ES) is needed here). It seems hopeless to classify all such E' over all totally real fields with a set of bad primes that varies with the class group and may be arbitrarily large.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

1.5 Our approach over general totally real fields

To go further, we must somehow eliminate the bad primes coming from the class group. Inspired by [BS04] and [Kra98], we study for $\mathfrak{q} \notin S$ the action of inertia groups $I_\mathfrak{q}$ on $E[p]$ for the Frey curve E. The curves E and E' are related via $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, and so we obtain information about the action of $I_\mathfrak{q}$ on $E'[p]$. We use this to conclude that E' has potentially good reduction away from S. (We say that E' has *potentially good reduction at* $\mathfrak{q}$ if there is some finite extension K' of the completion $K_\mathfrak{q}$ such that E' has good reduction over K'.)

To summarize, assuming (ES), a non-trivial solution to the Fermat equation over K with sufficiently large exponent p yields an E'/K with full 2-torsion and potentially good reduction away from the set S of primes above 2. (There are such elliptic curves over every K, for example the curve $Y^2 = X^3 - X$, so we do not yet have a contradiction.) However, such an E' can be represented by an $\mathcal{O}_S$-point on $Y(1) = X(1)\backslash\{\infty\}$ that pulls back to a $\mathcal{O}_S$-point on $X(2)\backslash\{0, 1, \infty\}$ (here $\mathcal{O}_S$ is the ring of S-integers in K). We can parametrize all such points (and therefore all such E') in terms of solutions (λ, μ) to the S-unit equation (3). This equation has solutions $(2, -1)$, $(-1, 2)$ and $(\frac{1}{2}, \frac{1}{2})$, which we have called irrelevant above (these correspond to $Y^2 = X^3 - X$), and possibly others, so we cannot yet reach a contradiction. However, the action of $I_\mathfrak{P}$ on $E[p]$, for $\mathfrak{P} \in S$, gives information on the valuations $v_\mathfrak{P}(\lambda)$ and $v_\mathfrak{P}(\mu)$, allowing us to prove Theorem 3.

1.6 Our approach over real quadratic fields

Next, we specialize to real quadratic fields $K = \mathbb{Q}(\sqrt{d})$, and we would like to understand solutions (λ, μ) to the S-unit equation (3). By considering $\mathrm{Norm}(\lambda)$ and $\mathrm{Norm}(\mu)$, which must both be of the form $\pm 2^r$, we show that relevant (λ, μ) give rise to solutions to the equation

$$(\eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1)^2 - \eta_1 \cdot 2^{r_1+2} = dv^2 \tag{8}$$

with $\eta_1 = \pm 1$, $\eta_2 = \pm 1$, $r_1 \geqslant r_2 \geqslant 0$ and $v \in \mathbb{Z}\backslash\{0\}$. This approach has the merit of eliminating the field K, since all the unknowns are now rational integers. We solve this equation completely for the d appearing in Theorems 1 and 2; there are a handful of solutions, and these satisfy condition (A) or (B) of Theorem 3. This gives proofs for Theorems 1 and 2.

To prove Theorem 4, we need to show that the set of squarefree $d \geqslant 2$ for which (8) has a solution is of density zero. For this we employ sieving modulo Mersenne numbers, $M_m = 2^m - 1$. Modulo M_m, there are at most $4m^2$ possibilities for the left-hand side of (8). The number of possibilities for squares modulo M_m is roughly at most $M_m/2^{\omega(M_m)}$, where $\omega(n)$ denotes the number of prime divisors of n. *If we can invert* v^2 *modulo* M_m, then we can conclude that d belongs to roughly at most $4m^2 M_m/2^{\omega(M_m)}$ congruence classes modulo M_m, and so the set of possible d has density roughly at most $4m^2/2^{\omega(M_m)}$. Using the *prime number theorem* and the *primitive divisor theorem*, it is possible to choose values of m so that this ratio tends to zero. However, there is no reason to suppose that v and M_m are coprime, and the argument needs to be combined with other techniques from analytic number theory to prove that the density of possible d is indeed zero.

1.7 Relation to other equations of Fermat type and to modular curves

We place our work in the wider Diophantine context by mentioning related results on Fermat-type equations. Many results of Fermat's Last Theorem or asymptotic Fermat's Last Theorem type (but over $\mathbb{Q}$) have been established by Kraus [Kra97], Bennett and Skinner [BS04] and Bennett *et al.* [BVY04] for equations of the form $Ax^p + By^p + Cz^p = 0$, $Ax^p + By^p = Cz^2$ or $Ax^p + By^p = Cz^3$. Perhaps the most satisfying work on Fermat-type equations over $\mathbb{Q}$ is the

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

paper of Halberstadt and Kraus [HK02], in which they show that for any triple of odd pairwise coprime integers A, B and C, there is a set of primes p of positive density such that all solutions to $Ax^p + By^p + Cz^p = 0$ are trivial.

One can also consider the analogy between the Fermat curves and various modular curves such as $X_0(p)$ and $X_1(p)$. In this framework, Mazur's theorems [Maz78] are analogues of Fermat's Last Theorem over $\mathbb{Q}$. Merel's uniform boundedness theorem [Mer96] states that for a number field K there is a bound B_n, depending only on the degree $n = [K : \mathbb{Q}]$, such that for $p > B_n$ the K-points on $X_1(p)$ are cusps. Interestingly, our bounds B_K for the asymptotic Fermat's Last Theorem (when applicable and effective) depend on the totally real field and, indeed, the Hilbert newforms at certain levels. The links between Fermat-type curves and modular curves are far deeper than one might suspect. For example, to solve $x^p + y^p = 2z^p$, $x^p + y^p = z^2$ and $x^p + y^p = z^3$ (and thereby complete the resolution of $x^p + y^p = 2^\alpha z^p$ that was started by Ribet [Rib97]), Darmon and Merel [DM97] not only needed the theorems of Mazur, Ribet and Wiles but were also forced to study the rational points on the modular curves $X^+_{\mathrm{ns}}(p) \times_{X(1)} X_0(r)$ with $r = 2$ or 3. In the reverse direction, methods of the present paper were used in [AS14] to prove asymptotic results for semistable points on $X^+_{\mathrm{ns}}(p)$ and $X^+_{\mathrm{s}}(p)$ over totally real fields.

1.8 Notational conventions

Throughout this paper, p is an odd prime and K is a totally real number field with ring of integers $\mathcal{O}_K$. For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by $[\mathfrak{a}]$ the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(K)$. For a non-trivial solution (a, b, c) to the Fermat equation (1), let

$$\mathcal{G}_{a,b,c} := a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K, \tag{9}$$

and let $[a, b, c]$ denote the class of $\mathcal{G}_{a,b,c}$ in $\mathrm{Cl}(K)$. We exploit the well-known fact (see, e.g., [CF67, Theorem VIII.4]) that every ideal class contains infinitely many prime ideals. Let $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ be the ideal classes of K. For each class $\mathfrak{c}_i$, we choose (and fix) a prime ideal $\mathfrak{m}_i \nmid 2$ of smallest possible norm representing $\mathfrak{c}_i$. The set $\mathcal{H}$ denotes our fixed choice of odd prime ideals representing the class group: $\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}$. The sets S, T and U are given in (2). Observe that $S \cap \mathcal{H} = \emptyset$.

Let $G_K = \mathrm{Gal}(\overline{K}/K)$. For an elliptic curve E/K, we write

$$\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p) \tag{10}$$

for the representation of G_K on the p-torsion of E. For a Hilbert eigenform $\mathfrak{f}$ over K, we let $\mathbb{Q}_\mathfrak{f}$ denote the field generated by its eigenvalues. In this situation ϖ will denote a prime of $\mathbb{Q}_\mathfrak{f}$ above p; of course, if $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$, we write p instead of ϖ. All other primes we consider are primes of K. We reserve the symbol $\mathfrak{P}$ for primes belonging to S, and $\mathfrak{m}$ for primes belonging to $\mathcal{H}$. An arbitrary prime of K is denoted by $\mathfrak{q}$, and $G_\mathfrak{q}$ and $I_\mathfrak{q}$ are, respectively, the decomposition and inertia subgroups of G_K at $\mathfrak{q}$.

2. Theoretical background

In this section we summarize the theoretical results we need for modularity, irreducibility of mod p Galois representations, level lowering, and Conjecture 1.

2.1 Modularity of the Frey curve

We shall need the following special case (see [FLHS]) of the modularity conjecture for elliptic curves over totally real fields.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Theorem 5. *Let K be a totally real field. Up to isomorphism over $\overline{K}$, there are at most finitely many non-modular elliptic curves E over K. Moreover, if K is real quadratic, then all elliptic curves over K are modular.*

Corollary 2.1. *Let K be a totally real field. There is some constant A_K, depending only on K, such that for any non-trivial solution (a, b, c) of the Fermat equation (1) with prime exponent $p > A_K$, the Frey curve $E_{a,b,c}$ given by (7) is modular.*

Proof. By Theorem 5, there are at most finitely many possible $\overline{K}$-isomorphism classes of elliptic curves over K that are non-modular. Let $j_1, \ldots, j_n \in K$ be the j-invariants of these classes. Write $\lambda = -b^p/a^p$. The j-invariant of $E_{a,b,c}$ is

$$j(\lambda) = 2^8 \cdot (\lambda^2 - \lambda + 1)^3 \cdot \lambda^{-2}(\lambda - 1)^{-2}.$$

Each equation $j(\lambda) = j_i$ has at most six solutions $\lambda \in K$. Thus there are values $\lambda_1, \ldots, \lambda_m \in K$ (with $m \leqslant 6n$) such that if $\lambda \neq \lambda_k$ for all k then $E_{a,b,c}$ is modular. If $\lambda = \lambda_k$, then

$$(-b/a)^p = \lambda_k, \quad (-c/a)^p = 1 - \lambda_k.$$

This pair of equations results in a bound for p unless λ_k and $1 - \lambda_k$ are both roots of unity, which is impossible because K is real; so the only roots of unity are ± 1. □

Remark. The constant A_K is ineffective: in [FLHS] it is shown that an elliptic curve E over a totally real field K is modular except possibly if it gives rise to a K-point on one of a handful of modular curves of genus at least 2, and Faltings' theorem [Fal83] (which is ineffective) gives the finiteness. If K is quadratic, we can take $A_K = 0$.

2.2 Irreducibility of mod p representations of elliptic curves

We need the following result, derived in [FS, Theorem 2] from the work of David [Dav11] and Momose [Mom95], which in turn builds on Merel's uniform boundedness theorem [Mer96].

Theorem 6. *Let K be a Galois totally real field. There is an effective constant C_K, depending only on K, such that the following holds: if $p > C_K$ is prime and E is an elliptic curve over K which is semistable at all $\mathfrak{q} \mid p$, then $\overline{\rho}_{E,p}$ is irreducible.*

2.3 Level lowering

We need a level-lowering result that plays the rôle of the Ribet step [Rib90] in the proof of Fermat's Last Theorem. Fortunately, such a result follows by combining the work of Fujiwara [Fuj06], Jarvis [Jar04] and Rajaei [Raj01].

Theorem 7 (Level lowering). *Let K be a totally real field and E/K an elliptic curve of conductor $\mathcal{N}$. Let p be a rational prime. For a prime ideal $\mathfrak{q}$ of K, denote by $\Delta_\mathfrak{q}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let*

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \| \mathcal{N}, \\ p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \quad \mathcal{N}_p := \frac{\mathcal{N}}{\mathcal{M}_p}. \tag{11}$$

Suppose that the following hold:

(i) *$p \geqslant 5$, the ramification index $e(\mathfrak{q}/p) < p - 1$ for all $\mathfrak{q} \mid p$, and $\mathbb{Q}(\zeta_p)^+ \not\subseteq K$;*
(ii) *E is modular;*

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

(iii) $\overline{\rho}_{E,p}$ *is irreducible;*
(iv) E *is semistable at all* $\mathfrak{q} \mid p$*;*
(v) $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ *for all* $\mathfrak{q} \mid p$.

Then there exist a Hilbert eigenform $\mathfrak{f}$ *of parallel weight* 2 *that is new at level* $\mathcal{N}_p$ *and some prime* ϖ *of* $\mathbb{Q}_{\mathfrak{f}}$ *such that* $\varpi \mid p$ *and* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$.

Proof. As noted above, we make use of the theorems in [Fuj06, Jar04, Raj01]. Assumption (i) takes care of some technical restrictions in those theorems.

By assumption (ii), there is a newform $\mathfrak{f}_0$ of parallel weight 2, level $\mathcal{N}$ and field of coefficients $\mathbb{Q}_{\mathfrak{f}_0} = \mathbb{Q}$ such that $\rho_{E,p} \sim \rho_{\mathfrak{f}_0,p}$. Thus $\overline{\rho}_{E,p}$ is modular, and by (iii) it is irreducible. Since K may be of even degree, in order to apply the main result of [Raj01] we need to add an auxiliary (special or supercuspidal) prime to the level. By [Raj01, Theorem 5], we can add an auxiliary (special) prime $\mathfrak{q}_0 \nmid \mathcal{N}$ so that $\overline{\rho}_{\mathfrak{f}_0,p}(\sigma_{\mathfrak{q}_0})$ is conjugate to $\overline{\rho}_{\mathfrak{f}_0,p}(\sigma)$, where $\sigma_{\mathfrak{q}_0}$ denotes a Frobenius element of G_K at $\mathfrak{q}_0$ and σ is complex conjugation. We now apply the main theorem of [Raj01] to remove from the level all primes $\mathfrak{q} \nmid p$ that divide $\mathcal{M}_p$. Next, we remove from the level the primes above p without changing the weight. By [Jar04, Theorem 6.2], we can do this provided that $\overline{\rho}_{E,p}|_{G_{\mathfrak{q}}}$ is finite at all $\mathfrak{q} \mid p$, where $G_{\mathfrak{q}}$ is the decomposition subgroup of G_K at $\mathfrak{q}$. But, from (iv), $\mathfrak{q}$ is a prime of good or multiplicative reduction for E. In the former case, $\overline{\rho}_{E,p}|_{G_{\mathfrak{q}}}$ is finite; in the latter case, it is finite by (v). Finally, from the condition imposed on $\mathfrak{q}_0$, it follows that $\mathrm{Norm}(\mathfrak{q}_0) \not\equiv 1 \pmod{p}$, and we can apply Fujiwara's version of Mazur's principle [Fuj06] to remove $\mathfrak{q}_0$ from the level. We conclude that there is an eigenform $\mathfrak{f}$ of parallel weight 2 which is new at level $\mathcal{N}_p$, as well as a prime $\varpi \mid p$ of $\mathbb{Q}_{\mathfrak{f}}$ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f}_0,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$. □

2.4 Eichler–Shimura

The following is a partial result towards Conjecture 1.

Theorem 8 (Blasius and Hida). *Let* K *be a totally real field, and let* $\mathfrak{f}$ *be a Hilbert newform over* K *of level* $\mathcal{N}$ *and parallel weight* 2*, such that* $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$*. Suppose that either:*

(a) $[K : \mathbb{Q}]$ *is odd; or*
(b) *there is a finite prime* $\mathfrak{q}$ *such that* $v_{\mathfrak{q}}(\mathcal{N}) = 1$.

Then there is an elliptic curve $E_{\mathfrak{f}}/K$ *of conductor* $\mathcal{N}$ *with the same* L*-function as* $\mathfrak{f}$.

A proof of Theorem 8 is given by Blasius [Bla04], who derived it from the work of Hida [Hid81]. Other proofs are provided by Darmon [Dar04] and Zhang [Zha01].

Corollary 2.2. *Let* E *be an elliptic curve over a totally real field* K *and let* p *be an odd prime. Suppose that* $\overline{\rho}_{E,p}$ *is irreducible and that* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},p}$ *for some Hilbert newform* $\mathfrak{f}$ *over* K *of level* $\mathcal{N}$ *and parallel weight* 2 *which satisfies* $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$*. Let* $\mathfrak{q} \nmid p$ *be a prime of* K *such that:*

(a) E *has potentially multiplicative reduction at* $\mathfrak{q}$*;*
(b) $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$*;*
(c) $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}) \pm 1)$.

Then there is an elliptic curve $E_{\mathfrak{f}}/K$ *of conductor* $\mathcal{N}$ *with the same* L*-function as* $\mathfrak{f}$.

Proof. Write c_4 and c_6 for the usual c-invariants of E, which are non-zero as E has potentially multiplicative reduction at $\mathfrak{q}$. Let $\gamma = -c_4/c_6$. Write χ for the quadratic character associated to $K(\sqrt{\gamma})/K$ and $E \otimes \chi$ for the γ-quadratic twist of E. By [Sil94, Theorem V.5.3], $E \otimes \chi$ has split multiplicative reduction at $\mathfrak{q}$. Let $\mathfrak{g} = \mathfrak{f} \otimes \chi$. As χ is quadratic and $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, we have $\mathbb{Q}_{\mathfrak{g}} = \mathbb{Q}$.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Suppose that $\mathfrak{g}$ is new at level $\mathcal{N}_\mathfrak{g}$. We will prove that $\upsilon_\mathfrak{q}(\mathcal{N}_\mathfrak{g}) = 1$. Then, by Theorem 8, there is an elliptic curve $E_\mathfrak{g}$ over K having the same L-function as $\mathfrak{g}$. Thus the L-functions of $E_\mathfrak{g} \otimes \chi$ and $\mathfrak{g} \otimes \chi = \mathfrak{f}$ are equal, and we take $E_\mathfrak{f} = E_\mathfrak{g} \otimes \chi$.

It remains to prove that $\upsilon_\mathfrak{q}(\mathcal{N}_\mathfrak{g}) = 1$. Since $\overline{\rho}_{E\otimes\chi,p} \sim \overline{\rho}_{\mathfrak{g},p}$, the two representations have the same optimal Serre level $\mathfrak{N}$ (say). Now $E \otimes \chi$ has multiplicative reduction at $\mathfrak{q}$, so $\upsilon_\mathfrak{q}(\mathfrak{N}) = 0$ or 1. Since E and $E \otimes \chi$ are isomorphic over $K(\sqrt{\gamma})$ and $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$, we have $p \mid \#\overline{\rho}_{E\otimes\chi,p}(I_\mathfrak{q})$. Hence $\upsilon_\mathfrak{q}(\mathfrak{N}) \neq 0$, and so $\upsilon_\mathfrak{q}(\mathfrak{N}) = 1$.

We now think of $\mathfrak{N}$ as the optimal Serre level $\overline{\rho}_{\mathfrak{g},p}$ and compare it with the level $\mathcal{N}_\mathfrak{g}$ of $\mathfrak{g}$. To carry out this comparison, we shall make use of [Jar99, Theorem 1.5]; to apply [Jar99], we need the irreducibility of $\overline{\rho}_{\mathfrak{g},p} \sim \overline{\rho}_{E\otimes\chi,p}$, which follows from the irreducibility of $\overline{\rho}_{E,p}$. By [Jar99, Theorem 1.5], $\upsilon_\mathfrak{q}(\mathfrak{N}) = \upsilon_\mathfrak{q}(\mathcal{N}_\mathfrak{g})$, except possibly when $\upsilon_\mathfrak{q}(\mathcal{N}_\mathfrak{g}) = 1$ and $\upsilon_\mathfrak{q}(\mathfrak{N}) = 0$ or when $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}) \equiv \pm 1 \pmod{p}$. The former is impossible as $\upsilon_\mathfrak{q}(\mathfrak{N}) = 1$, and the latter is ruled out by (c). Thus, $\upsilon_\mathfrak{q}(\mathcal{N}_\mathfrak{g}) = 1$. □

3. Computations

3.1 Behaviour at odd primes

For $u, v, w \in \mathcal{O}_K$ such that $uvw \neq 0$ and $u + v + w = 0$, let

$$E : y^2 = x(x - u)(x + v). \tag{12}$$

The invariants c_4, c_6, Δ and j have their usual meanings and are given by

$$\begin{aligned} c_4 &= 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv), \\ c_6 &= -32(u - v)(v - w)(w - u), \quad \Delta = 16u^2v^2w^2, \quad j = c_4^3/\Delta. \end{aligned} \tag{13}$$

The following elementary lemma is a straightforward consequence of the properties of elliptic curves over local fields (see, e.g., [Sil86, §§ VII.1 and VII.5]).

Lemma 3.1. *With the above notation, let $\mathfrak{q} \nmid 2$ be a prime and let*

$$s = \min\{\upsilon_\mathfrak{q}(u), \upsilon_\mathfrak{q}(v), \upsilon_\mathfrak{q}(w)\}.$$

Write $E_{\min}$ for a local minimal model at $\mathfrak{q}$.

(i) *$E_{\min}$ has good reduction at $\mathfrak{q}$ if and only if s is even and*

$$\upsilon_\mathfrak{q}(u) = \upsilon_\mathfrak{q}(v) = \upsilon_\mathfrak{q}(w). \tag{14}$$

(ii) *$E_{\min}$ has multiplicative reduction at $\mathfrak{q}$ if and only if s is even and (14) fails to hold. In this case, the minimal discriminant $\Delta_\mathfrak{q}$ at $\mathfrak{q}$ satisfies*

$$\upsilon_\mathfrak{q}(\Delta_\mathfrak{q}) = 2\,\upsilon_\mathfrak{q}(u) + 2\,\upsilon_\mathfrak{q}(v) + 2\,\upsilon_\mathfrak{q}(w) - 6s.$$

(iii) *$E_{\min}$ has additive reduction if and only if s is odd.*

3.2 Conductor of the Frey curve

Let (a, b, c) be a non-trivial solution to the Fermat equation (1) with prime exponent p. Let $\mathcal{G}_{a,b,c}$ be as given in (9), which we think of as the greatest common divisor of a, b and c. If p is sufficiently large, then an odd prime not dividing $\mathcal{G}_{a,b,c}$ is a prime of good or multiplicative reduction for $E_{a,b,c}$ and does not appear in the final level $\mathcal{N}_p$, as we shall see in due course, whereas an odd prime dividing $\mathcal{G}_{a,b,c}$ exactly once is an additive prime and does appear in $\mathcal{N}_p$. To control $\mathcal{N}_p$, we need to control $\mathcal{G}_{a,b,c}$. The following lemma achieves this. We refer to § 1.8 for the notation.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Lemma 3.2. *Let (a,b,c) be a non-trivial solution to (1). There is a non-trivial integral solution (a',b',c') to (1) such that the following hold.*

(i) *For some $\xi \in K^*$, we have $a' = \xi a$, $b' = \xi b$ and $c' = \xi c$.*
(ii) *$\mathcal{G}_{a',b',c'} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$.*
(iii) *$[a',b',c'] = [a,b,c]$.*

Proof. Let $\mathfrak{m} \in \mathcal{H}$ satisfy $[\mathcal{G}_{a,b,c}] = [\mathfrak{m}]$, so that $\mathfrak{m} = (\xi) \cdot \mathcal{G}_{a,b,c}$ for some $\xi \in K^*$. Let a', b' and c' be as in (i). Note that $(a') = (\xi) \cdot (a) = \mathfrak{m} \cdot \mathcal{G}_{a,b,c}^{-1}(a)$, which is an integral ideal, since $\mathcal{G}_{a,b,c}$ (by definition) divides a. Thus a' is in $\mathcal{O}_K$ and, similarly, so are b' and c'. For (ii) and (iii), note that

$$\mathcal{G}_{a',b',c'} = a'\mathcal{O}_K + b'\mathcal{O}_K + c'\mathcal{O}_K = (\xi) \cdot (a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K) = (\xi) \cdot \mathcal{G}_{a,b,c} = \mathfrak{m}. \qquad \square$$

Lemma 3.3. *Let (a,b,c) be a non-trivial solution to the Fermat equation (1) with prime exponent p that satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ where $\mathfrak{m} \in \mathcal{H}$. Write E for the Frey curve in (7), and let Δ be its discriminant. Then, at all $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$, the model E is minimal and semistable and satisfies $p \mid v_{\mathfrak{q}}(\Delta)$. Let $\mathcal{N}$ be the conductor of E, and let $\mathcal{N}_p$ be as defined in (11). Then*

$$\mathcal{N} = \mathfrak{m}^2 \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r_{\mathfrak{P}}} \cdot \prod_{\substack{\mathfrak{q} \mid abc \\ \mathfrak{q} \notin S \cup \{\mathfrak{m}\}}} \mathfrak{q}, \quad \mathcal{N}_p = \mathfrak{m}^2 \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}, \tag{15}$$

where $0 \leqslant r'_{\mathfrak{P}} \leqslant r_{\mathfrak{P}} \leqslant 2 + 6\, v_{\mathfrak{P}}(2)$.

Proof. Suppose first that $\mathfrak{q} \mid abc$ and $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. Since $\mathcal{G}_{a,b,c} = \mathfrak{m}$, the prime $\mathfrak{q}$ divides precisely one of a, b and c. From (13), $\mathfrak{q} \nmid c_4$, so the model equation (7) is minimal and has multiplicative reduction at $\mathfrak{q}$, and $p \mid v_{\mathfrak{q}}(\Delta)$. By (11), we see that $\mathfrak{q} \nmid \mathcal{N}_p$.

For $\mathfrak{P} \in S$, we have that $r_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathcal{N}) \leqslant 2 + 6\, v_{\mathfrak{P}}(2)$ by [Sil94, Theorem IV.10.4]. We observe that, by (11), $r'_{\mathfrak{P}} = r_{\mathfrak{P}}$ unless E has multiplicative reduction at $\mathfrak{P}$ and $p \mid v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$, in which case $r_{\mathfrak{P}} = 1$ and $r'_{\mathfrak{P}} = 0$. Finally, recall that by our choice of class group representatives $\mathcal{H}$, we have $\mathfrak{m} \nmid 2$. As E has full 2-torsion over K, the wild part of the conductor of E/K at $\mathfrak{m}$ vanishes (see [Sil94, p. 380]). Thus $v_{\mathfrak{m}}(\mathcal{N}) \leqslant 2$. However, since $\mathcal{G}_{a,b,c} = \mathfrak{m}$, it follows from Lemma 3.1 that E has additive reduction at $\mathfrak{m}$, and so $v_{\mathfrak{m}}(\mathcal{N}) = v_{\mathfrak{m}}(\mathcal{N}_p) = 2$. $\square$

3.3 Images of inertia

We gather the information we need regarding images of inertia $\overline{\rho}_{E,p}(I_{\mathfrak{q}})$. This is crucial for applying Corollary 2.2 and for controlling the behaviour at the primes in $S \cup \{\mathfrak{m}\}$ of the newform obtained by level lowering.

Lemma 3.4. *Let E be an elliptic curve over K with j-invariant j. Let $p \geqslant 5$ and let $\mathfrak{q} \nmid p$ be a prime of K. Then $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $v_{\mathfrak{q}}(j) < 0$) and $p \nmid v_{\mathfrak{q}}(j)$.*

Proof. If E has potentially good reduction at $\mathfrak{q}$, then $\#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$ divides 24 (e.g. [Kra90, Introduction]). For E with potentially multiplicative reduction, the result is a well-known consequence of the theory of the Tate curve (e.g. [Sil94, Proposition V.6.1]). $\square$

Lemma 3.5. *Let $\mathfrak{q} \notin S$. Let (a,b,c) be a solution to the Fermat equation (1) with prime exponent $p \geqslant 5$ such that $\mathfrak{q} \nmid p$. Let $E = E_{a,b,c}$ be the Frey curve in (7). Then $p \nmid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$.*

Proof. By (13), if a, b and c have unequal valuations at $\mathfrak{q}$, then $v_{\mathfrak{q}}(j) < 0$ and $p \mid v_{\mathfrak{q}}(j)$; otherwise, $v_{\mathfrak{q}}(j) \geqslant 0$. In either case, the result follows from Lemma 3.4. $\square$

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Lemma 3.6. *Let E be an elliptic curve over K, and let $p \geqslant 3$. Let $\mathfrak{P} \in S$ and suppose that E has potentially good reduction at $\mathfrak{P}$. Let Δ be the discriminant of E (not necessarily minimal at $\mathfrak{P}$). Then $3 \mid \rho_{E,p}(I_\mathfrak{P})$ if and only if $3 \nmid v_\mathfrak{P}(\Delta)$.*

Proof. This is a special case of [Kra90, Théorème 3]. □

Lemma 3.7. *Let $\mathfrak{P} \in S$. Let (a, b, c) be a solution to the Fermat equation (1) with prime exponent $p > 4\, v_\mathfrak{P}(2)$. Let $E = E_{a,b,c}$ be the Frey curve in (7), and write j for its j-invariant.*

(i) *If $\mathfrak{P} \in T$, then $v_\mathfrak{P}(j) < 0$ and p divides the order of $\overline{\rho}_{E,p}(I_\mathfrak{P})$.*

(ii) *If $\mathfrak{P} \in U$, then either $v_\mathfrak{P}(j) < 0$ and p divides the order of $\overline{\rho}_{E,p}(I_\mathfrak{P})$, or $v_\mathfrak{P}(j) \geqslant 0$ and 3 divides the order of $\overline{\rho}_{E,p}(I_\mathfrak{P})$.*

Proof. Let π be a uniformizer for $K_\mathfrak{P}$. Let

$$t = \min\{v_\mathfrak{P}(a), v_\mathfrak{P}(b), v_\mathfrak{P}(c)\}, \quad \alpha = \pi^{-t}a, \quad \beta = \pi^{-t}b, \quad \gamma = \pi^{-t}c.$$

Then $\alpha, \beta, \gamma \in \mathcal{O}_\pi$. Suppose first that $\mathfrak{P} \in T$. By the definition of T, the prime $\mathfrak{P}$ has residue field $\mathbb{F}_2$. As $\alpha^p + \beta^p + \gamma^p = 0$, precisely one of α, β and γ is divisible by π. Thus $v_\mathfrak{P}(a)$, $v_\mathfrak{P}(b)$ and $v_\mathfrak{P}(c)$ are not all equal; two out of a, b and c have valuation t (say) and one has valuation $t + k$ with $k \geqslant 1$. From the formulae in (13), we have that $v_\mathfrak{P}(j) = 8\, v_\mathfrak{P}(2) - 2kp$. As $p > 4\, v_\mathfrak{P}(2)$, we see that $v_\mathfrak{P}(j) < 0$ and $p \nmid v_\mathfrak{P}(j)$. Thus (i) follows from Lemma 3.4.

Suppose now that $\mathfrak{P} \in U$. If $v_\mathfrak{P}(a)$, $v_\mathfrak{P}(b)$ and $v_\mathfrak{P}(c)$ are not all equal, then (ii) follows as above. Suppose they are all equal. Then, by the formulae in (13), we have

$$v_\mathfrak{P}(j) \geqslant 8\, v_\mathfrak{P}(2) > 0, \quad v_\mathfrak{P}(\Delta) = 4\, v_\mathfrak{P}(2) + 6tp.$$

By the definition of U, we have $3 \nmid v_\mathfrak{P}(2)$ and so $3 \nmid v_\mathfrak{P}(\Delta)$. Now (ii) follows from Lemma 3.6. □

4. Level lowering and Eichler–Shimura

Theorem 9. *Let K be a totally real field satisfying (ES). There is a constant B_K depending only on K such that the following hold. Let (a, b, c) be a non-trivial solution to the Fermat equation (1) with prime exponent $p > B_K$, and rescale (a, b, c) so that it remains integral and satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Write E for the Frey curve (7). Then there is an elliptic curve E' over K such that:*

(i) *the elliptic curve E' has good reduction away from $S \cup \{\mathfrak{m}\}$;*
(ii) *$\#E'(K)[2] = 4$;*
(iii) *$\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$.*

Write j' for the j-invariant of E'. Then:

(a) *for $\mathfrak{P} \in T$, we have $v_\mathfrak{P}(j') < 0$;*
(b) *for $\mathfrak{P} \in U$, we have either $v_\mathfrak{P}(j') < 0$ or $3 \nmid v_\mathfrak{P}(j')$;*
(c) *for $\mathfrak{q} \notin S$, we have $v_\mathfrak{q}(j') \geqslant 0$.*

Proof. We first observe, by Lemma 3.3, that E is semistable outside $S \cup \{\mathfrak{m}\}$. By taking B_K to be sufficiently large, we see from Corollary 2.1 that E is modular and from Theorem 6 that $\overline{\rho}_{E,p}$ is irreducible; to apply Theorem 6, we need that E is semistable at the primes dividing p, and this is true once we enlarge B_K to ensure that $\mathfrak{m} \nmid p$. Applying Theorem 7 and Lemma 3.3

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

(where once again we may need to enlarge B_K), we see that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\varpi \mid p$ of $\mathbb{Q}_\mathfrak{f}$. Here $\mathbb{Q}_\mathfrak{f}$ is the field generated by the Hecke eigenvalues of $\mathfrak{f}$.

Next, we reduce to the case where $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$, after possibly enlarging B_K by an effective amount. This step uses standard ideas, originally due to Mazur as indicated in the introduction, which can be found in [BS04, § 4], [Coh07, Proposition 15.4.2] and [Kra97, § 3], so we omit the details. We have assumed (ES): $T \neq \emptyset$, or $[K : \mathbb{Q}]$ is odd, or Conjecture 1 holds. We would like to show that there is some elliptic curve E'/K having the same L-function as $\mathfrak{f}$. This is immediate if we assume Conjecture 1, and follows from Theorem 8 if $[K : \mathbb{Q}]$ is odd. Suppose $T \neq \emptyset$ and let $\mathfrak{P} \in T$. By Lemma 3.7, E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{P})$. The existence of E' follows from Corollary 2.2 after possibly enlarging B_K to ensure that $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{P}) \pm 1)$.

We now know that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ for some E'/K with conductor $\mathcal{N}_p$ given by (15). After enlarging B_K by an effective amount and possibly replacing E' by an isogenous curve, we may assume that E' has full 2-torsion; this step again uses standard ideas (e.g. [Coh07, Proposition 15.4.2], [Kra97, § 3]), so we omit the details.

It remains to prove (a)–(c). There are finitely many elliptic curves E' with (full 2-torsion and) good reduction outside $S \cup \{\mathfrak{m}\}$. Therefore we may, after possibly enlarging B_K, suppose that for all primes $\mathfrak{q}$, if $\upsilon_\mathfrak{q}(j') < 0$ then $p \nmid \upsilon_\mathfrak{q}(j')$. Now we know from Lemma 3.5 that for $\mathfrak{q} \notin S$, $p \nmid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$ and so $p \nmid \#\overline{\rho}_{E',p}(I_\mathfrak{q})$. By Lemma 3.4, we see that $\upsilon_\mathfrak{q}(j') \geqslant 0$, which proves (c).

For (a), let $\mathfrak{P} \in T$. Applying Lemma 3.7 gives $p \mid \overline{\rho}_{E,p}(I_\mathfrak{P})$ and so $p \mid \overline{\rho}_{E',p}(I_\mathfrak{P})$. Now, by Lemma 3.4, we have $\upsilon_\mathfrak{P}(j') < 0$, which proves (a).

For (b), suppose $\mathfrak{P} \in U$. If $p \mid \overline{\rho}_{E,p}(I_\mathfrak{P})$, then again $\upsilon_\mathfrak{P}(j') < 0$ as required. Thus, suppose $p \nmid \overline{\rho}_{E,p}(I_\mathfrak{P})$. By Lemma 3.7 we have that $3 \mid \overline{\rho}_{E,p}(I_\mathfrak{P})$. It follows that $p \nmid \overline{\rho}_{E',p}(I_\mathfrak{P})$ and $3 \mid \overline{\rho}_{E',p}(I_\mathfrak{P})$. The first conclusion, together with Lemma 3.4, shows that $\upsilon_\mathfrak{P}(j') \geqslant 0$ (recall that we have imposed above the condition that $\upsilon_\mathfrak{q}(j') < 0$ implies $p \nmid \upsilon_\mathfrak{q}(j')$ for all $\mathfrak{q}$). By Lemma 3.6, as $3 \mid \overline{\rho}_{E',p}(I_\mathfrak{P})$, we have $3 \nmid \upsilon_\mathfrak{P}(\Delta')$, where Δ' is the discriminant of E'. But $j' = (c_4')^3/\Delta'$, so $3 \nmid \upsilon_\mathfrak{P}(j')$ as required. □

Remark. The constant B_K is ineffective, as it depends on the ineffective constant A_K in Corollary 2.1. However, if we know that the Frey curve is modular (for instance when K is real quadratic), the constant B_K becomes effectively computable. Indeed, by the recipe in [Coh07, § 15.4], all that is needed are algorithms to compute the Hilbert newforms at the levels $\mathcal{N}_p$, the fields generated by their eigenvalues, and a finite number of eigenvalues for each, and there are effective algorithms for doing this [DV13].

5. Proof of Theorem 3

Theorem 9 relates non-trivial solutions of the Fermat equation (with p sufficiently large) to elliptic curves E' with full 2-torsion having potentially good reduction outside S and satisfying certain additional properties. In this section we relate such elliptic curves E' to solutions to the S-unit equation (3), using basic facts about λ-invariants of elliptic curves (see, e.g., [Sil86, pp. 53–55]), and use this relation to prove Theorem 3. As E' has full 2-torsion over K, it has a model

$$E' : y^2 = (x - e_1)(x - e_2)(x - e_3). \tag{16}$$

Here, of course, e_1, e_2 and e_3 are distinct and so their *cross ratio* $\lambda = (e_3 - e_1)/(e_2 - e_1)$ belongs to $\mathbb{P}^1(K) - \{0, 1, \infty\}$. Write $\mathfrak{S}_3$ for the symmetric group on three letters. The action of $\mathfrak{S}_3$

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

on (e_1, e_2, e_3) extends via the cross ratio to an action on $\mathbb{P}^1(K) - \{0, 1, \infty\}$ and allows us to identify $\mathfrak{S}_3$ with the following subgroup of $\mathrm{PGL}_2(K)$:

$$\mathfrak{S}_3 = \{z,\ 1/z,\ 1-z,\ 1/(1-z),\ z/(z-1),\ (z-1)/z\}.$$

The *λ-invariants of E'* are the six elements (counted with multiplicity) of the $\mathfrak{S}_3$-orbit of λ; they are related to the j-invariant j' by

$$j' = 2^8 \cdot (\lambda^2 - \lambda + 1)^3 \cdot \lambda^{-2}(\lambda - 1)^{-2}. \tag{17}$$

Proof of Theorem 3. Let K be a totally real field satisfying assumption (ES). Let B_K be as in Theorem 9, and let (a, b, c) be a non-trivial solution to the Fermat equation (1) with exponent $p > B_K$. By Lemma 3.2, we may rescale (a, b, c) so that it remains integral but $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. We now apply Theorem 9, which yields an elliptic curve E'/K with full 2-torsion and potentially good reduction outside S whose j-invariant j' satisfies the following two conditions:

(a) for all $\mathfrak{P} \in T$, we have $\upsilon_{\mathfrak{P}}(j') < 0$;
(b) for all $\mathfrak{P} \in U$, we have $\upsilon_{\mathfrak{P}}(j') < 0$ or $3 \nmid \upsilon_{\mathfrak{P}}(j')$.

Let λ be any of the λ-invariants of E'. Note that $j' \in \mathcal{O}_S$, where $\mathcal{O}_S$ is the ring of S-integers in K. By (17), $\lambda \in K$ satisfies a monic degree 6 equation with coefficients in $\mathcal{O}_S$, and therefore $\lambda \in \mathcal{O}_S$. However, $1/\lambda$, $\mu := 1 - \lambda$ and $1/\mu$ are also solutions to (17) and so belong to $\mathcal{O}_S$. Hence (λ, μ) is a solution to the S-unit equation (3). By assumption, this solution must satisfy either hypothesis (A) or hypothesis (B) in Theorem 3. We now rewrite (17) as

$$j' = 2^8 \cdot (1 - \lambda\mu)^3 \cdot (\lambda\mu)^{-2} \tag{18}$$

and let $t := \max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\}$. Suppose that (λ, μ) satisfies (A): there is some $\mathfrak{P} \in T$ so that $t \leqslant 4\,\upsilon_{\mathfrak{P}}(2)$. If $t = 0$, then $\upsilon_{\mathfrak{P}}(j') \geqslant 8\,\upsilon_{\mathfrak{P}}(2) > 0$, which contradicts (a) above. We may therefore suppose that $t > 0$. Now the relation $\lambda + \mu = 1$ forces either $\upsilon_{\mathfrak{P}}(\lambda) = \upsilon_{\mathfrak{P}}(\mu) = -t$, or $\upsilon_{\mathfrak{P}}(\lambda) = 0$ and $\upsilon_{\mathfrak{P}}(\mu) = t$, or $\upsilon_{\mathfrak{P}}(\lambda) = t$ and $\upsilon_{\mathfrak{P}}(\mu) = 0$. Thus $\upsilon_{\mathfrak{P}}(\lambda\mu) = -2t < 0$ or $\upsilon_{\mathfrak{P}}(\lambda\mu) = t > 0$. Either way, $\upsilon_{\mathfrak{P}}(j') = 8\,\upsilon_{\mathfrak{P}}(2) - 2t \geqslant 0$, which again contradicts (a).

Thus (λ, μ) satisfies (B): there is some $\mathfrak{P} \in U$ such that $t \leqslant 4\,\upsilon_{\mathfrak{P}}(2)$ and $\upsilon_{\mathfrak{P}}(\lambda\mu) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$. The former implies $\upsilon_{\mathfrak{P}}(j') \geqslant 0$ as above, and the latter, together with (18), gives $3 \mid \upsilon_{\mathfrak{P}}(j')$. This contradicts (b), completing the proof. □

6. Proofs of Theorems 1 and 2

We would like to understand the solutions to (3) for real quadratic K. Let

$$\Lambda_S = \{(\lambda, \mu) : \lambda + \mu = 1,\ \lambda, \mu \in \mathcal{O}_S^*\}. \tag{19}$$

The following two lemmas are easy consequences of the definitions.

Lemma 6.1. *The action of $\mathfrak{S}_3$ on $\mathbb{P}^1(K) - \{0, 1, \infty\}$ induces an action on Λ_S given by $(\lambda, \mu)^\sigma := (\lambda^\sigma, 1 - \lambda^\sigma)$ for $(\lambda, \mu) \in \Lambda_S$ and $\sigma \in \mathfrak{S}_3$.*

Lemma 6.2. *Let (λ_1, μ_1) and (λ_2, μ_2) be elements of Λ_S belonging to the same $\mathfrak{S}_3$-orbit. Then:*

(i) $\max\{|\upsilon_{\mathfrak{P}}(\lambda_1)|, |\upsilon_{\mathfrak{P}}(\mu_1)|\} \leqslant 4\,\upsilon_{\mathfrak{P}}(2)$ *if and only if* $\max\{|\upsilon_{\mathfrak{P}}(\lambda_2)|, |\upsilon_{\mathfrak{P}}(\mu_2)|\} \leqslant 4\,\upsilon_{\mathfrak{P}}(2)$;
(ii) $\upsilon_{\mathfrak{P}}(\lambda_1\mu_1) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$ *if and only if* $\upsilon_{\mathfrak{P}}(\lambda_2\mu_2) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Proof. Suppose that (λ_1, μ_1) and (λ_2, μ_2) belong to the same orbit. Then the elliptic curves $E_i : y^2 = x(x-1)(x-\lambda_i)$ have the same j-invariant. The lemma follows by comparing the $\mathfrak{P}$-valuation of this j-invariant expressed in terms of (λ_1, μ_1) and in terms of (λ_2, μ_2). □

We denote the set of $\mathfrak{S}_3$-orbits in Λ_S by $\mathfrak{S}_3 \backslash \Lambda_S$. The three elements $(2, -1)$, $(-1, 2)$ and $(\frac{1}{2}, \frac{1}{2})$ of Λ_S form a single orbit. As stated in the introduction, we call these the *irrelevant solutions* to (3), and we call their orbit the *irrelevant orbit*; other solutions are said to be *relevant*.

In this section, $K = \mathbb{Q}(\sqrt{d})$ where $d \geqslant 2$ is a squarefree integer. Note that $T \neq \emptyset$ or $U \neq \emptyset$. The irrelevant orbit satisfies condition (A) of Theorem 3 if $T \neq \emptyset$ and satisfies condition (B) if $U \neq \emptyset$.

Lemma 6.3. *Let $(\lambda, \mu) \in \Lambda_S$.*

(i) *λ, $\mu \in \mathbb{Q}$ if and only if (λ, μ) belongs to the irrelevant orbit.*

(ii) *There is an element $\sigma \in \mathfrak{S}_3$ such that $(\lambda', \mu') = (\lambda, \mu)^\sigma$ satisfies $\lambda', \mu' \in \mathcal{O}_K$.*

Proof. Note that λ and μ are in $\mathbb{Q}$ if and only if they both have the form $\pm 2^r$. From the relation $\lambda + \mu = 1$ we quickly deduce (i). For (ii), as K is quadratic, $|S| = 1$ or 2, and the lemma follows from examining the possible signs for $v_{\mathfrak{P}}(\lambda)$ and $v_{\mathfrak{P}}(\lambda^\sigma)$ for $\mathfrak{P} \in S$ and $\sigma \in \mathfrak{S}_3$. □

Lemma 6.4. *Up to the action of $\mathfrak{S}_3$, every relevant $(\lambda, \mu) \in \Lambda_S$ has the form*

$$\lambda = \frac{\eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1 + v\sqrt{d}}{2}, \quad \mu = \frac{\eta_2 \cdot 2^{r_2} - \eta_1 \cdot 2^{r_1} + 1 - v\sqrt{d}}{2}, \tag{20}$$

where

$$\eta_1 = \pm 1, \quad \eta_2 = \pm 1, \quad r_1 \geqslant r_2 \geqslant 0, \quad v \in \mathbb{Z}, \quad v \neq 0 \tag{21}$$

are related by

$$(\eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1)^2 - \eta_1 \cdot 2^{r_1+2} = dv^2, \tag{22}$$

$$(\eta_2 \cdot 2^{r_2} - \eta_1 \cdot 2^{r_1} + 1)^2 - \eta_2 \cdot 2^{r_2+2} = dv^2. \tag{23}$$

Moreover, if $d \not\equiv 1 \pmod 8$, then we can take $r_2 = 0$.

Observe that (22) and (23) are equivalent in the sense that we can rearrange either of the equations to obtain the other, but it is convenient to have both.

Proof. Suppose that η_1, η_2, r_1, r_2 and v satisfy (21)–(23), and let λ and μ be given by (20). It is clear that λ and μ belong to $\mathcal{O}_S$ but not $\mathbb{Q}^*$, and that $\lambda + \mu = 1$. Moreover, from (22) and (23), the norms of λ and μ are $\eta_i 2^{r_i}$, and thus $\lambda, \mu \in \mathcal{O}_S^*$. Hence (λ, μ) is a relevant element of Λ_S. Conversely, suppose that (λ, μ) is a relevant element of Λ_S. Then $\lambda, \mu \notin \mathbb{Q}$, and by Lemma 6.3 we may suppose that $\lambda, \mu \in \mathcal{O}_K$. Let $x \mapsto \overline{x}$ denote conjugation in K. Then

$$\lambda\overline{\lambda} = \eta_1 \cdot 2^{r_1}, \quad \mu\overline{\mu} = \eta_2 \cdot 2^{r_2}, \quad \eta_1 = \pm 1, \quad \eta_2 = \pm 1.$$

Swapping λ and μ if necessary (which does not change the orbit), we may suppose that $r_1 \geqslant r_2 \geqslant 0$. Note that if $d \not\equiv 1 \pmod 8$, then S consists of one element, and the relation $\lambda + \mu = 1$ forces $r_2 = 0$. Now,

$$\lambda + \overline{\lambda} = \lambda\overline{\lambda} - (1-\lambda)(1-\overline{\lambda}) + 1 = \lambda\overline{\lambda} - \mu\overline{\mu} + 1 = \eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1.$$

Moreover, we can write $\lambda - \overline{\lambda} = v\sqrt{d}$ where $v \in \mathbb{Z}$, and as $\lambda \notin \mathbb{Q}$ we have $v \neq 0$. The expressions for $\lambda + \overline{\lambda}$ and $\lambda - \overline{\lambda}$ give the expression for λ in (20), and we deduce the expression for μ from $\mu = 1 - \lambda$. Finally, the identity $(\lambda + \overline{\lambda})^2 - (\lambda - \overline{\lambda})^2 = 4\lambda\overline{\lambda}$ gives (22), and the corresponding identity for μ gives (23). □

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

TABLE 1. The relevant elements of Λ_S for $d \geqslant 2$ squarefree, $d \not\equiv 1 \pmod 8$.

d	Relevant elements of Λ_S up to the action of $\mathfrak{S}_3$ and Galois conjugation	Extra conditions
$d = 2$	$(\sqrt{2}, 1-\sqrt{2})$, $(-16+12\sqrt{2}, 17-12\sqrt{2})$, $(4+2\sqrt{2}, -3+2\sqrt{2})$, $(-2+2\sqrt{2}, 3-2\sqrt{2})$	
$d = 3$	$(2+\sqrt{3}, -1-\sqrt{3})$, $(8+4\sqrt{3}, -7-4\sqrt{3})$	
$d = 5$	$((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, $(-8+4\sqrt{5}, 9-4\sqrt{5})$, $(-1+\sqrt{5}, 2-\sqrt{5})$	
$d = 6$	$(-4+2\sqrt{6}, 5-2\sqrt{6})$	
$d \equiv 3 \pmod 8$, $d \neq 3$	None	
$d \equiv 5 \pmod 8$, $d \neq 5$	None	
$d \equiv 7 \pmod 8$	$(2^{2s+1} + 2^{s+1}w\sqrt{d},\ 1 - 2^{2s+1} - 2^{s+1}w\sqrt{d})$	$4^s - 1 = dw^2$, $s \geqslant 2$, $w \neq 0$
$d \equiv 2 \pmod{16}$, $d \neq 2$	$(-2^{2s} + 2^s w\sqrt{d}, 1 + 2^{2s} - 2^s w\sqrt{d})$	$4^s + 2 = dw^2$, $s \geqslant 2$, $w \neq 0$
$d \equiv 6 \pmod{16}$, $d \neq 6$	None	
$d \equiv 10 \pmod{16}$	None	
$d \equiv 14 \pmod{16}$	$(2^{2s} + 2^s w\sqrt{d}, 1 - 2^{2s} - 2^s w\sqrt{d})$	$4^s - 2 = dw^2$, $s \geqslant 2$, $w \neq 0$

LEMMA 6.5. *Let $d \not\equiv 1 \pmod 8$ be squarefree and at least 2. The relevant elements of Λ_S, up to the action of $\mathfrak{S}_3$ and Galois conjugation, are as given in Table 1.*

Proof. We apply Lemma 6.4. As $d \not\equiv 1 \pmod 8$, we have $r_2 = 0$. Values $0 \leqslant r_1 \leqslant 5$ (together with $\eta_1 = \pm 1$ and $\eta_2 = \pm 1$) in (22) yield the solutions given in Table 1 for $d = 2$, 3, 5 and 6, as well as the solution $(16 - 4\sqrt{14},\ -15 + 4\sqrt{14})$ which is included under the table entry for $d \equiv 14 \pmod{16}$. We may therefore suppose that $r_1 \geqslant 6$. If $\eta_2 = -1$, then (23) gives $2^{2r_1} + 4 = dv^2$. As d is squarefree and $r_1 \geqslant 6$, this gives $d \equiv 1 \pmod 8$, which is a contradiction. Thus $\eta_2 = 1$. Now (22) gives

$$2^{r_1+2}(2^{r_1-2} - \eta_1) = dv^2.$$

As d is squarefree, we see that r_1 is even precisely when d is odd. Suppose first that d is odd, so $r_1 = 2s + 2$ and $v = 2^{s+2}w$ for some non-zero integer w. As $r_1 \geqslant 6$, we have $s \geqslant 2$. Then $4^s - \eta_1 = dw^2$. As $\eta_1 = \pm 1$, this equation is impossible if $d \equiv 3$ or $5 \pmod 8$. This completes the proofs of the entries in the table for $d \equiv 3, 5 \pmod 8$ (including $d = 3$ and $d = 5$). If $d \equiv 7 \pmod 8$, then reducing mod 8 shows that $\eta_1 = 1$. This gives the solution in Table 1 for $d \equiv 7 \pmod 8$.

Suppose now that d is even, so that $r_1 = 2s + 1$ and $v = 2^{s+1}w$ for some non-zero integer w and $s \geqslant 2$. Then $2^{2s-1} - \eta_1 = (d/2)w^2$. This gives a contradiction modulo 8, if $d/2 \equiv 3$ or 5

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

(mod 8), and proves the correctness of the entries in the table for $d \equiv 6, 10 \pmod{16}$ (including $d = 6$). Moreover, if $d \equiv 2$ or $14 \pmod{16}$, then $\eta = -1$ or 1, respectively, completing the proof except for the $d = 2$ case.

For $d = 2$, we have $2^{2s-1} + 1 = w^2$. The factorization $(w-1)(w+1) = 2^{2s-1}$ quickly leads to a contradiction, so there are no further solutions. □

6.1 Proof of Theorem 1

For now, let $d \geqslant 2$ be squarefree and satisfy $d \not\equiv 1 \pmod 4$. Write $K = \mathbb{Q}(\sqrt{d})$. Then $S = T = \{\mathfrak{P}\}$, say; in particular, assumption (ES) is satisfied. We apply Theorem 3 and focus on verifying condition (A). In view of Lemma 6.2, we only have to verify (A) for one representative of each $\mathfrak{S}_3$-orbit. It is easy to check that the irrelevant orbit, as well as the solutions listed in Table 1 for $d = 2$, 3 and 6, all satisfy (A). For $d \equiv 3 \pmod 8$ or $d \equiv 6, 10 \pmod{16}$, there are no further solutions and so the proof is complete for parts (i) and (ii) of Theorem 1. Suppose $d \equiv 2 \pmod{16}$ and $d \neq 2$. We know from Table 1 that the S-unit equation has no relevant solutions, unless there are $s \geqslant 2$ and $w \neq 0$ such that $4^s + 2 = dw^2$. Now, if $q \mid d$ is an odd prime, then -2 is a quadratic residue modulo q, and so $q \equiv 1, 3 \pmod 8$. This proves (iii) of Theorem 1, and (iv) is obtained similarly.

6.2 Proof of Theorem 2

Here $d \equiv 5 \pmod 8$. Again we apply Theorem 3, but now we check condition (B) of the theorem. Note that $U = S = \{\mathfrak{P}\}$ where $\mathfrak{P} = 2 \cdot \mathcal{O}_K$. Moreover, the irrelevant solutions to the S-unit equation (3) satisfy condition (B). From Table 1, there are no further solutions to the S-unit equation for $d \neq 5$. This completes the proof. For $d = 5$, Table 1 lists three solutions to the S-unit equation that satisfy $v_{\mathfrak{P}}(\lambda\mu) = 0$, 2 and 1; we cannot complete the proof in this case, which is why it is excluded from the statement of the theorem.

7. Proof of Theorem 4

For a set $\mathcal{U}$ of positive integers and a positive real number X, we let $\mathcal{U}(X) = \{d \in \mathcal{U} : d \leqslant X\}$. We define the *absolute density* of $\mathcal{U}$ to be

$$\delta(\mathcal{U}) = \lim_{X \to \infty} \#\mathcal{U}(X)/X,$$

provided the limit exists. In this section, as in the introduction, we let $\mathbb{N}^{\mathrm{sf}}$ be the set of squarefree integers $d \geqslant 2$. For $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, recall the definition of the *relative density* of $\mathcal{U}$ in $\mathbb{N}^{\mathrm{sf}}$ given in (4), which we can now write as

$$\delta_{\mathrm{rel}}(\mathcal{U}) = \lim_{X \to \infty} \#\mathcal{U}(X)/\#\mathbb{N}^{\mathrm{sf}}(X),$$

provided the limit exists. We need the following two classical analytic theorems.

Theorem 10 (e.g. [Lan09, p. 636]). *For integers r and N with N positive, let*

$$\mathbb{N}^{\mathrm{sf}}_{r,N} = \{d \in \mathbb{N}^{\mathrm{sf}} : d \equiv r \pmod N\}.$$

Let $s = \gcd(r, N)$ and suppose that s is squarefree. Then

$$\#\mathbb{N}^{\mathrm{sf}}_{r,N}(X) \sim \frac{\varphi(N)}{s\varphi(N/s)N\prod_{q \mid N}(1 - q^{-2})} \cdot \frac{6}{\pi^2} X,$$

where φ denotes Euler's totient function.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Theorem 11 (e.g. [Lan09, pp. 641–643]). *Let N be a positive integer. Let $r_1, \dots, r_m$ be distinct modulo N, satisfying $\gcd(r_i, N) = 1$. Let E be the set of positive integers d such that every prime factor q of d satisfies $q \equiv r_i \pmod N$ for some $i = 1, \dots, k$. Then there is some positive constant $\gamma = \gamma(N, r_1, \dots, r_m)$ such that*

$$\#E(X) \sim \gamma \cdot X/\log(X)^{1-m/\varphi(N)}.$$

Let $\mathcal{C}$ and $\mathcal{D}$ be as given in (5).

Lemma 7.1. *Let $\mathcal{C}' = \mathbb{N}^{\mathrm{sf}} \backslash \mathcal{C}$. Then $\delta(\mathcal{C}') = 0$.*

The proof of Lemma 7.1 is somewhat lengthy. Before embarking on the proof, we show that the lemma is enough to imply Theorem 4.

Proof of Theorem 4. Observe that Theorem 4 follows immediately from Theorem 3 if we can prove the density claims in (6). Theorem 10 applied to $\mathbb{N}^{\mathrm{sf}} = \mathbb{N}^{\mathrm{sf}}_{0,1}$ gives $\#\mathbb{N}^{\mathrm{sf}}(X) \sim 6X/\pi^2$. It follows that for $\mathcal{U} \subseteq \mathbb{N}^{\mathrm{sf}}$, $\delta(\mathcal{U})$ exists if and only if $\delta_{\mathrm{rel}}(\mathcal{U})$ exists, and in this case the two are related by $\delta_{\mathrm{rel}}(\mathcal{U}) = \pi^2\delta(\mathcal{U})/6$. By Lemma 7.1, we have $\delta_{\mathrm{rel}}(\mathcal{C}') = \delta(\mathcal{C}') = 0$. As $\mathcal{C}'$ and $\mathcal{C}$ are complements in $\mathbb{N}^{\mathrm{sf}}$, we have $\delta_{\mathrm{rel}}(\mathcal{C}) = 1$. It remains to show that $\delta_{\mathrm{rel}}(\mathcal{D}) = 5/6$. By definition, $\mathcal{D} = \mathcal{C} \cap (\mathbb{N}^{\mathrm{sf}} - \mathbb{N}^{\mathrm{sf}}_{5,8})$, so it suffices to prove that $\delta_{\mathrm{rel}}(\mathbb{N}^{\mathrm{sf}}_{5,8}) = 1/6$; this follows from Theorem 10. □

7.1 Proof of Lemma 7.1

To complete the proof of Theorem 4, we need to prove Lemma 7.1. By definition, $\mathcal{C}'$ is the set of squarefree $d \geqslant 2$ such that the S-unit equation (3) has a relevant solution in $\mathbb{Q}(\sqrt{d})$. By Lemma 6.4, this is precisely the set of squarefree $d \geqslant 2$ satisfying (22) and (23), where $\eta_1 = \pm 1$, $\eta_2 = \pm 1$, $r_1 \geqslant r_2 \geqslant 0$ and $v \neq 0$. For $\eta_1, \eta_2 = \pm 1$ and $\kappa_1, \kappa_2 = 0, 1$, write $\mathcal{C}'(\eta_1, \eta_2, \kappa_1, \kappa_2)$ for the set of $d \geqslant 2$ satisfying (22) and (23) with $r_i \equiv \kappa_i \pmod 2$. Then $\mathcal{C}'$ is the union of all 16 $\mathcal{C}'(\eta_1, \eta_2, \kappa_1, \kappa_2)$. Let q be an odd prime divisor of d. If $d \in \mathcal{C}'(\eta_1, \eta_2, \kappa_1, \kappa_2)$, then reducing (22) and (23) modulo q shows that $\eta_1 2^{\kappa_1}$ and $\eta_2 2^{\kappa_2}$ are both quadratic residues modulo q. If $(\eta_1, \eta_2, \kappa_1, \kappa_2) \neq (1, 1, 0, 0)$, then the possible odd prime divisors q of d belong to a *proper* subset of the congruence classes $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ modulo 8. It follows from Theorem 11 that $\delta(\mathcal{C}'(\eta_1, \eta_2, \kappa_1, \kappa_2)) = 0$ for $(\eta_1, \eta_2, \kappa_1, \kappa_2) \neq (1, 1, 0, 0)$.

To show $\delta(\mathcal{C}') = 0$, it is now enough to show that $\delta(\mathcal{C}'(1, 1, 0, 0)) = 0$. Suppose $d \in \mathcal{C}'(1, 1, 0, 0)$. Thus there is a solution to (22) and (23) with $\eta_1 = \eta_2 = 1$, $r_1 = 2s$, $r_2 = 2t$ and $s \geqslant t \geqslant 0$. Equations (22) and (23) are now equivalent to

$$(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1) = dv^2. \tag{24}$$

Since $d > 0$, we in fact have $s > t$. We write $\mathcal{C}'(1, 1, 0, 0) = \mathcal{L} \cup \mathcal{M}$, where $\mathcal{L}$ is the subset of d for which there is a solution to (24) with $t > 0$, and $\mathcal{M}$ is the subset of d for which there is a solution $t = 0$. We separately show that $\delta(\mathcal{L}) = 0$ and $\delta(\mathcal{M}) = 0$. Suppose now that $d \in \mathcal{L}$. Write $\mathbf{s} = (s, t)$ and let

$$\alpha_{1,\mathbf{s}} = 2^s + 2^t + 1, \quad \alpha_{2,\mathbf{s}} = 2^s + 2^t - 1, \quad \alpha_{3,\mathbf{s}} = 2^s - 2^t + 1, \quad \alpha_{4,s} = 2^s - 2^t - 1. \tag{25}$$

These are odd and pairwise coprime. Then $\alpha_{i,\mathbf{s}} = d_{i,\mathbf{s}} v_{i,\mathbf{s}}^2$, where the $d_{i,\mathbf{s}}$ are squarefree, and $d = \prod d_{i,\mathbf{s}}$. Thus

$$\mathcal{L} = \{d_{1,\mathbf{s}} d_{2,\mathbf{s}} d_{3,\mathbf{s}} d_{4,\mathbf{s}} : \mathbf{s} = (s, t),\ s > t > 0\}.$$

Recall that we want to show $\delta(\mathcal{L}) = 0$. In fact, we shall prove the equivalent statement that $\delta_{\sup}(\mathcal{L}) = 0$, where $\delta_{\sup}(\mathcal{L}) = \limsup_{X \to \infty} \#\mathcal{L}(X)/X$.

For a positive integer m, we write $M_m = 2^m - 1$; this is the mth Mersenne number. We will make frequent use of the fact that $M_n \mid M_m$ whenever $n \mid m$.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Lemma 7.2. *Let m be a positive integer. Let $M_m = 2^m - 1$. Suppose $\mathbf{s}_1 \equiv \mathbf{s}_2 \pmod{m}$. Then $\alpha_{i,\mathbf{s}_1} \equiv \alpha_{i,\mathbf{s}_2} \pmod{M_m}$ for $i = 1, \ldots, 4$.*

Proof. Write $\mathbf{s}_1 = (s_1, t_1)$ and $\mathbf{s}_2 = (s_2, t_2)$. If $\mathbf{s}_1 \equiv \mathbf{s}_2 \pmod{m}$, then $f = |s_1 - s_2|$ and $g = |t_1 - t_2|$ are divisible by m. But $\alpha_{i,\mathbf{s}_1} - \alpha_{i,\mathbf{s}_2}$ can be written as a linear combination of $2^f - 1$ and $2^g - 1$, and is therefore divisible by M_m. □

Lemma 7.3. *Let m be a positive integer. Let $s_0 > t_0 > 0$ and write $\mathbf{s}_0 = (s_0, t_0)$. Let*

$$\mathcal{A}_{m,\mathbf{s}_0} = \{d_{1,\mathbf{s}} : \mathbf{s} = (s,t),\ s > t > 0,\ \mathbf{s} \equiv \mathbf{s}_0 \pmod{m}\}.$$

Let $p_1, \ldots, p_k$ be the distinct primes dividing M_m that do not divide $\alpha_{1,\mathbf{s}_0}$, and write $N = p_1 \cdots p_k$. Then

$$\#\mathcal{A}_{m,\mathbf{s}_0}(X) \leqslant 2^{-k} \cdot X + N.$$

Proof. Clearly $N \mid M_m$, and $\alpha_{1,\mathbf{s}_0}$ is coprime to N. Suppose $\mathbf{s} \equiv \mathbf{s}_0 \pmod{m}$. By Lemma 7.2, $\alpha_{1,\mathbf{s}} \equiv \alpha_{1,\mathbf{s}_0} \pmod{N}$, and so $\alpha_{1,\mathbf{s}}$ is also coprime to N. As $\alpha_{i,\mathbf{s}} = d_{i,\mathbf{s}} v_{i,\mathbf{s}}^2$, we have $d_{1,\mathbf{s}} \equiv \alpha_{1,\mathbf{s}_0} v_{1,\mathbf{s}}^{-2} \pmod{N}$. Thus $d_{1,\mathbf{s}}$ modulo N belongs to the set $\{\alpha_{1,\mathbf{s}_0} \cdot w^2 : w \in (\mathbb{Z}/N\mathbb{Z})^*\}$. As N is squarefree with k distinct odd prime factors, this set has cardinality $\varphi(N)/2^k$. The lemma follows. □

We denote the number of distinct prime divisors of a positive integer n by $\omega(n)$.

Lemma 7.4. *For $m \geqslant 1$, let $h_m = \omega(M_m)$. Then $\delta_{\sup}(\mathcal{L}) \leqslant 2^{-h_m/2} \cdot m^2$.*

Proof. For now, fix some $\mathbf{s}_0$ and let k and N be as in Lemma 7.3. Let

$$\mathcal{L}_{m,\mathbf{s}_0} = \{d_{1,\mathbf{s}} d_{2,\mathbf{s}} d_{3,\mathbf{s}} d_{4,\mathbf{s}} : \mathbf{s} = (s,t),\ s > t > 0,\ \mathbf{s} \equiv \mathbf{s}_0 \pmod{m}\}.$$

Then

$$\#\mathcal{L}_{m,\mathbf{s}_0}(X) \leqslant \#\mathcal{A}_{m,\mathbf{s}_0}(X) \leqslant 2^{-k} X + N \leqslant 2^{-k} X + M_m,$$

where the first inequality is clear from the definitions of $\mathcal{L}_{m,\mathbf{s}_0}$ and $\mathcal{A}_{m,\mathbf{s}_0}$, and the second and third inequalities follow from Lemma 7.3. Now let $q_1, \ldots, q_{k'}$ be the distinct prime divisors of M_m that do not divide $\alpha_{2,\mathbf{s}_0}$. Then (similarly to the above) we have

$$\#\mathcal{L}_{m,\mathbf{s}_0}(X) \leqslant 2^{-k'} X + M_m.$$

As $\alpha_{1,\mathbf{s}_0}$ and $\alpha_{2,\mathbf{s}_0}$ are coprime, either $k \geqslant h_m/2$ or $k' \geqslant h_m/2$. Hence

$$\#\mathcal{L}_{m,\mathbf{s}_0}(X) \leqslant 2^{-h_m/2} X + M_m.$$

Now let $\mathbf{s}_1, \ldots, \mathbf{s}_{m^2}$ be a complete system of representatives for $\mathbf{s}$ modulo m. Then $\mathcal{L}$ is the disjoint union of $\mathcal{L}_{m,\mathbf{s}_1}, \ldots, \mathcal{L}_{m,\mathbf{s}_{m^2}}$. Thus

$$\#\mathcal{L}(X) \leqslant 2^{-h_m/2} \cdot m^2 \cdot X + m^2 M_m.$$ □

A prime ℓ is a *primitive divisor* of M_m if $\ell \mid M_m$ but $\ell \nmid M_{m'}$ for all $m' < m$. The following is a special case of the celebrated primitive divisor theorem of Bilu *et al.* [BHV01].

Theorem 12. *If $n \neq 1, 6$, then M_n has a primitive divisor.*

Corollary 7.5. *With notation as above, $h_m \geqslant 2^{\omega(m)} - 2$.*

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Proof. The number of divisors $n \mid m$ is at least $2^{\omega(m)}$. For $n \neq 1, 6$ dividing m, let ℓ_n be a primitive divisor of M_n. Then ℓ_n divides M_m, and by definition $\ell_n \neq \ell_{n'}$ whenever $n \neq n'$. This gives at least $2^{\omega(m)} - 2$ distinct primes dividing M_m. □

Lemma 7.6. *With notation as above,* $\delta(\mathcal{L}) = 0$.

Proof. Combining Lemma 7.4 and Corollary 7.5, we have

$$0 \leqslant \delta_{\sup}(\mathcal{L}) \leqslant \frac{m^2}{2^{(h_m/2)}} \leqslant \frac{m^2}{2^{(2^{\omega(m)-1}-1)}} \tag{26}$$

for any $m \geqslant 1$. Now let y be large, and let $m = \prod_{p \leqslant y} p$. Then $\omega(m) = \pi(y)$ and $m = \exp(\vartheta(y))$, where π and ϑ are, respectively, the prime counting function and the first Chebyshev function. By the prime number theorem (see, e.g., [Apo76, ch. 4])

$$\pi(y) \sim y/\log y, \quad \vartheta(y) \sim y.$$

Letting $y \to \infty$ in (26) clearly gives $\delta_{\sup}(\mathcal{L}) = 0$, as required. □

Recall that we had written $\mathcal{C}'(1, 1, 0, 0) = \mathcal{L} \cup \mathcal{M}$ and wanted to show that $\delta(\mathcal{L}) = \delta(\mathcal{M}) = 0$. The following completes the proof of Lemma 7.1 and hence Theorem 4.

Lemma 7.7. *With notation as above,* $\delta(\mathcal{M}) = 0$.

Proof. The set $\mathcal{M}$ is the set of squarefree $d \geqslant 2$ such that (24) holds with $s > 0$ and $t = 0$. Then $(2^{s-1} - 1)(2^{s-1} + 1) = dw^2$ where $w = v/2^{s+1} \in \mathbb{Z} \backslash \{0\}$. Now we can apply a straightforward simplification of the above argument to show that $\delta(\mathcal{M}) = 0$. □

Acknowledgements

We thank A. Meyerowitz, G. Helms and other users of `mathoverflow.net`[1] for suggesting alternative proofs of Lemma 7.7. It is clear, however, that the ideas in these alternative proofs cannot be adapted to prove Lemma 7.6.

We are indebted to Alex Bartel, Frank Calegari, John Cremona, Lassina Dembélé, Fred Diamond, Tim Dokchitser, David Loeffler, Michael Stoll and Panagiotis Tsaknias for useful discussions. We are grateful to the referees for many helpful comments and suggestions.

References

AS14 S. Anni and S. Siksek, *On Serre's uniformity conjecture for semistable elliptic curves over totally real fields*, Preprint (2014), arXiv:1408.1279.

Apo76 T. M. Apostol, *Introduction to analytic number theory* (Springer, New York, 1976).

BS04 M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.

BVY04 M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Math. **140** (2004), 1399–1416.

BHV01 Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122.

[1] http://mathoverflow.net/questions/149511/squarefree-parts-of-mersenne-numbers.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Bla04 D. Blasius, *Elliptic curves, Hilbert modular forms, and the Hodge conjecture*, in *Contributions to automorphic forms, geometry, and number theory* (Johns Hopkins University Press, Baltimore, MD, 2004), 83–103.

BCP97 W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

CF67 J. W. S. Cassels and A. Frölich, *Algebraic number theory* (Academic Press, London, 1967).

Coh07 H. Cohen, *Number theory. Volume II: Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240 (Springer, New York, 2007).

Dar04 H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101 (American Mathematical Society, Providence, RI, 2004).

DM97 H. Darmon and L. Merel, *Winding quotients and some variants of fermats last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

Dav11 A. David, *Caractère d'isogénie et critères d'irréductibilité*, Preprint (2011), arXiv:1103.3892.

DK94 O. Debarre and M. J. Klassen, *Points of low degree on smooth plane curves*, J. Reine Angew. Math. **446** (1994), 81–87.

DV13 L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, in *Elliptic curves, Hilbert modular forms and Galois deformations*, ed. L. Berger (Springer, Basel, 2013), 135–198.

Dic71 L. E. Dickson, *History of the theory of numbers, vol. II* (Chelsea, New York, 1971).

Fad61 D. K. Faddeev, *The group of divisor classes on some algebraic curves*, Dokl. Akad. Nauk SSSR **136** (1961), 296–298 (in Russian); Engl. transl. Sov. Math. Dokl. **2** (1961), 67–69.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

FLHS N. Freitas, B. V. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math., to appear.

FS N. Freitas and S. Siksek, *Criteria for irreducibility of mod p representations of Frey curves*, J. Théor. Nombres Bordeaux, to appear.

Fuj06 K. Fujiwara, *Level optimisation in the totally real case*, Preprint (2006), arXiv:math/0602586.

GR78 B. H. Gross and D. E. Rohrlich, *Some results on the Mordell–Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–224.

HK02 E. Halberstadt and A. Kraus, *Courbes de Fermat: resultats et problemes*, J. Reine Angew. Math. **548** (2002), 167–234.

HP84 F. H. Hao and C. J. Parry, *The Fermat equation over quadratic fields*, J. Number Theory **19** (1984), 115–130.

Hid81 H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. Math. **103** (1981), 726–776.

Jar99 F. Jarvis, *Level lowering for modular mod ℓ representations over totally real fields*, Math. Ann. **313** (1999), 141–160.

Jar04 F. Jarvis, *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math. **213** (2004), 267–280.

JM04 F. Jarvis and P. Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$*, J. Number Theory **109** (2004), 182–196.

Kol01 V. A. Kolyvagin, *On the first case of the Fermat theorem for cyclotomic fields*, J. Math. Sci. (New York) **106** (2001), 3302–3311.

Kra90 A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), 353–385.

Kra97 A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press

Kra98 A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Exp. Math. **7** (1998), 1–13.

Lan09 E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen II* (B. G. Teubner, Leipzig, 1909).

Maz78 B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

Mer96 L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

Mom95 F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), 329–348.

Raj01 A. Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65.

Rib90 K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

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

Ser87 J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

Sie29 C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen der Preussischen Akademie der Wissenschaften (Walter de Gruyter, Berlin, 1929), 1–41.

Sil86 J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106 (Springer, Dordrecht, 1986).

Sil94 J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151 (Springer, New York, 1994).

Sma97 N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. Lond. Math. Soc. (3) **75** (1997), 271–307.

Sma98 N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41 (Cambridge University Press, Cambridge, 1998).

Sma99 N. P. Smart, *Determining the small solutions to S-unit equations*, Math. Comp. **68** (1999), 1687–1699.

TW95 R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), 553–572.

Tze03 P. Tzermias, *Parametrization of low-degree points on a Fermat curve*, Acta Arith. **108** (2003), 25–35.

Wil95 A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), 443–551.

Zha01 S.-W. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), 27–147.

Nuno Freitas nunobfreitas@gmail.com
Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany

Samir Siksek samir.siksek@gmail.com
Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

https://doi.org/10.1112/S0010437X14007957 Published online by Cambridge University Press