ACTA ARITHMETICA
173.3 (2016)

On the generalized Fermat equation over totally real fields

by

Heline Deconinck (Coventry)

1. Introduction. The idea that the Fermat equation over totally real fields can be studied using modularity and level lowering (thereby extending the approach of Wiles [13] for the Fermat equation over $\mathbb{Q}$) appears first in the papers of Jarvis [7] and Jarvis and Meekin [8]. In particular, Jarvis and Meekin show that the Fermat equation $x^n + y^n = z^n$ has no non-trivial solutions with $x, y, z \in \mathbb{Q}(\sqrt{2})$ and $n \geq 4$. This work is extended to other totally real fields in more recent papers of Freitas and Siksek [2], [3].

Let K be a totally real number field and let $\mathcal{O}_K$ be its ring of integers. In [2], Freitas and Siksek study the Fermat equation $a^p + b^p + c^p = 0$ with $a, b, c \in \mathcal{O}_K$ and p prime. For now let S be the set of primes of $\mathcal{O}_K$ above 2 and let $\mathcal{O}_S$ be the ring of S-integers and $\mathcal{O}_S^*$ be the group of S-units. Freitas and Siksek give a criterion for the non-existence of solutions $a, b, c \in \mathcal{O}_K$ with $abc \neq 0$ for p sufficiently large in terms of the solutions to the S-unit equation $\lambda + \mu = 1$. The proof uses modularity and level lowering arguments over totally real fields. It is natural to seek an extension of the work of Freitas and Siksek to generalized Fermat equations $Aa^p + Bb^p + Cc^p = 0$, for given non-zero coefficients $A, B, C \in \mathcal{O}_K$. In this paper we show that the results of Freitas and Siksek can indeed be extended to any choice of *odd* coefficients A, B, C, provided the set S is enlarged to contain the primes dividing ABC as well as the primes dividing 2.

We now state our results precisely. As in [2], our results will sometimes be conditional on the following standard conjecture.

Conjecture 1.1 ("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 write $\mathbb{Q}_\mathfrak{f}$ for the*

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11F80, 11F03.
Key words and phrases: Fermat equation, modularity, Galois representation, level lowering.
Received 18 May 2015.
Published online 2 May 2016.

DOI: 10.4064/aa8171-1-2016

field generated by its eigenvalues. Suppose that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. *Then there is an elliptic curve* $E_{\mathfrak{f}}/K$ *with conductor* $\mathcal{N}$ *having the same* L*-function as* $\mathfrak{f}$.

Let A, B, C be non-zero elements of $\mathcal{O}_K$, and let p be a prime. Consider the equation

$$Aa^p + Bb^p + Cc^p = 0, \qquad a, b, c \in \mathcal{O}_K; \tag{1.1}$$

we shall refer to this as the *generalized Fermat equation over K with coefficients A, B, C and exponent p.* A solution (a, b, c) is called *trivial* if $abc = 0$, otherwise *non-trivial.* The following notation shall be fixed throughout the paper:

$$\begin{aligned} R &= \mathrm{Rad}(ABC) = \prod_{\substack{\mathfrak{q} \mid ABC \\ \mathfrak{q} \text{ prime in } K}} \mathfrak{q}, \\ S &= \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } \mathcal{O}_K \text{ such that } \mathfrak{P} \mid 2R\}, \\ T &= \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } \mathcal{O}_K \text{ above } 2\}, \\ U &= \{\mathfrak{P} \in T : f(\mathfrak{P}/2) = 1\}, \qquad V = \{\mathfrak{P} \in T : 3 \nmid \upsilon_{\mathfrak{P}}(2)\}. \end{aligned} \tag{1.2}$$

Here $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. As in [2], we need an assumption which we refer to throughout the paper as (ES):

$$\text{(ES)} \qquad \begin{cases} \text{either } [K : \mathbb{Q}] \text{ is odd;} \\ \text{or } U \neq \emptyset; \\ \text{or Conjecture 1.1 holds for } K. \end{cases}$$

THEOREM 1.2. *Let K be a totally real field satisfying* (ES). *Let $A, B, C \in \mathcal{O}_K$, and suppose that A, B, C are odd, in the sense that if $\mathfrak{P} \mid 2$ is a prime of $\mathcal{O}_K$ then $\mathfrak{P} \nmid ABC$. Write $\mathcal{O}_S^*$ for the set of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda, \mu \in \mathcal{O}_S^*, \tag{1.3}$$

there is either

(A) *some* $\mathfrak{P} \in U$ *that satisfies* $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\,\upsilon_{\mathfrak{P}}(2)$, *or*
(B) *some* $\mathfrak{P} \in V$ *that satisfies both* $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\,\upsilon_{\mathfrak{P}}(2)$ *and* $\upsilon_{\mathfrak{P}}(\lambda\mu) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$.

Then there is some constant $\mathcal{B} = \mathcal{B}(K, A, B, C)$ such that the generalized Fermat equation (1.1) *with exponent p and coefficients A, B, C does not have non-trivial solutions with $p > \mathcal{B}$.*

Theorem 1.2 gives a bound on the exponent of non-trivial solutions to the generalized Fermat equation (1.1) provided certain hypotheses are satisfied. There are practical algorithms for determining the solutions to S-unit equations (e.g. [12]), so these hypotheses can always be checked for specific

K, A, B, C. The following theorem is an example where the S-unit equation can still be solved, even though the coefficients are not completely fixed.

THEOREM 1.3. *Let $d \geq 13$ be squarefree, satisfying $d \equiv 5 \pmod 8$, and let $q \geq 29$ be a prime such that $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Let $K = \mathbb{Q}(\sqrt{d})$ and assume Conjecture 1.1 holds for K. Then there is an effectively computable constant $\mathcal{B}_{K,q}$ such that for all primes $p > \mathcal{B}_{K,q}$, the Fermat equation*

$$x^p + y^p + q^r z^p = 0$$

has no non-trivial solutions with exponent p.

2. Preliminaries. We shall need the theoretical machinary of modularity, irreducibility of Galois representations and level lowering. These tools and the way we use them is practically identical to [2] which we refer the reader to for more details.

2.1. The Frey curve and its modularity. We shall need the following recently proved theorem [1].

THEOREM 2.1 (Freitas, Le Hung and Siksek). *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.*

We shall associate to a solution (a, b, c) of (1.1) the following *Frey elliptic curve*:

$$E : Y^2 = X(X - Aa^p)(X + Bb^p). \tag{2.1}$$

Before applying Theorem 2.1 to the Frey curve associated to our generalized Fermat equation (1.1) we shall need the following lemma.

LEMMA 2.2. *Let $A, B, C \in \mathcal{O}_K$ be odd, and suppose that every solution (λ, μ) to the S-unit equation (1.3) satisfies either condition (A) or (B) of Theorem 1.2. Then $(\pm 1, \pm 1, \pm 1)$ is not a solution to equation (1.1).*

Proof. Suppose $(\pm 1, \pm 1, \pm 1)$ is a solution to (1.1). By changing signs of A, B, C, we may suppose that $(1, 1, 1)$ is a solution, and therefore that $A + B + C = 0$. Let $\lambda = A/C$ and $\mu = B/C$. Clearly (λ, μ) is a solution to the S-unit equation (1.3).

Suppose first that (A) is satisfied. Then $U \neq \emptyset$, so there is some $\mathfrak{P} \mid 2$ with residue field $\mathbb{F}_2$. As A, B, C are odd, we have $\mathfrak{P} \nmid ABC$. Reducing the relation $A+B+C = 0$ modulo $\mathfrak{P}$ we obtain $1+1+1 = 0$ in $\mathbb{F}_2$, giving a contradiction.

Suppose now that (B) holds. By (B) there is some $\mathfrak{P} \in V$ such that $\upsilon_{\mathfrak{P}}(\lambda\mu) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$. However, as A, B, C are odd, $\upsilon_{\mathfrak{P}}(\lambda\mu) = 0$. Moreover, $3 \nmid \upsilon_{\mathfrak{P}}(2)$ by definition of V. This gives a contradiction. ∎

Corollary 2.3. *Let $A, B, C \in \mathcal{O}_K$ be odd, and suppose that every solution (λ, μ) to the S-unit equation* (1.3) *satisfies either condition* (A) *or* (B) *of Theorem* 1.2. *There is some* (*ineffective*) *constant $\mathcal{A} = \mathcal{A}(K, A, B, C)$ such that for any non-trivial solution (a, b, c) of* (1.1) *with prime exponent $p > \mathcal{A}$, the Frey curve E given by* (2.1) *is modular.*

Proof. By Theorem 2.1, there are at most finitely many possible $\overline{K}$-isomorphism classes of elliptic curves over K that are non-modular. Let $j_1, \dots, j_n \in K$ be the j-invariants of these classes. Write $\lambda = -Bb^p/Aa^p$. 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 $\lambda_1, \dots, \lambda_m \in K$ such that if $\lambda \neq \lambda_k$ for all k then E is modular. If $\lambda = \lambda_k$ then

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

This pair of equations results in a bound for p unless $-b/a$ and c/a are both roots of unity. But as K is real, the only roots of unity are ± 1. If $-b/a = \pm 1$ and $c/a = \pm 1$ then (1.1) has a solution of the form $(\pm 1, \pm 1, \pm 1)$, contradicting Lemma 2.2. This completes the proof. ∎

2.2. Irreducibility of mod p representations of elliptic curves. To use a generalized version of level lowering, we need the mod p Galois representation associated to the Frey elliptic curve to be irreducible. The following theorem of Freitas and Siksek [4, Theorem 2], building on earlier work of David, Momose and Merel, is sufficient for our purpose.

Theorem 2.4. *Let K be a totally real field. There is an effective constant $\mathcal{C}_K$, depending only on K, such that the following holds. If $p > \mathcal{C}_K$ is a rational prime, and E is an elliptic curve over K which is semistable at some $\mathfrak{q} \mid p$, then $\overline{\rho}_{E,p}$ is irreducible.*

In [4] the theorem is stated for Galois totally real fields K, but the version stated here follows immediately on replacing K by its Galois closure.

2.3. Level lowering. As before, K is a totally real field. Let E/K be an elliptic curve of conductor $\mathcal{N}$, and p 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

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \| \mathcal{N} \\ p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \quad \mathcal{N}_p := \mathcal{N}/\mathcal{M}_p. \tag{2.2}$$

The ideal $\mathcal{M}_p$ is precisely the product of the primes where we want to lower the level. For a Hilbert eigenform $\mathfrak{f}$ over K, denote the field generated by its eigenvalues by $\mathbb{Q}_{\mathfrak{f}}$. The following level-lowering recipe is derived by Freitas and Siksek [2] from the works of Fujiwara [5], Jarvis [6] and Rajaei [9].

THEOREM 2.5. *With the above notation, suppose that:*

(i) $p \geq 5$ *and* p *is unramified in* K,
(ii) E *is modular,*
(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 is 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* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$.

3. Conductor of the Frey curve. Let (a,b,c) be a non-trivial solution to the Fermat equation (1.1). Write

$$\mathcal{G}_{a,b,c} = a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K, \tag{3.1}$$

which we naturally think of as the greatest common divisor of a, b, c. Over $\mathbb{Q}$, or over a number field of class number 1, it is natural to scale the solution (a,b,c) so that $\mathcal{G}_{a,b,c} = 1 \cdot \mathcal{O}_K$, but this is not possible in general. The primes that divide all of a, b, c can be additive primes for the Frey curve, and additive primes are not removed by the level lowering recipe given above. To control the final level we need to control $\mathcal{G}_{a,b,c}$. Following [2], we fix a set

$$\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}$$

of prime ideals $\mathfrak{m}_i \nmid 2R$, which is a set of representatives for the ideal classes of $\mathcal{O}_K$. 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. We denote $[\mathcal{G}_{a,b,c}]$ by $[a,b,c]$. The following is Lemma 3.2 of [2], and states that we can always scale our solution (a,b,c) so that the gcd belongs to $\mathcal{H}$.

LEMMA 3.1. *Let* (a,b,c) *be a non-trivial solution to* (1.1). *There is a non-trivial integral solution* (a',b',c') *to* (1.1) *such that the following hold.*

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

LEMMA 3.2. *Let* (a,b,c) *be a non-trivial solution to the Fermat equation* (1.1) *with odd prime exponent* p, *and scaled as in Lemma* 3.1 *so that* $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. *Write* $E = E_{a,b,c}$ *for the Frey curve in* (2.1), *and let* Δ *be its discriminant. For a prime* $\mathfrak{q}$ *we write* $\Delta_{\mathfrak{q}}$ *for the minimal discriminant at* $\mathfrak{q}$. *Then at all* $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$, *the model* E *is minimal, semistable, and satisfies*

$p \mid \upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. *Let $\mathcal{N}$ be the conductor of E, and let $\mathcal{N}_p$ be as defined in* (2.2). *Then*

$$\mathcal{N} = \mathfrak{m}^{s_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r_{\mathfrak{P}}} \cdot \prod_{\substack{\mathfrak{q} \mid abc \\ \mathfrak{q} \notin S \cup \{\mathfrak{m}\}}} \mathfrak{q}, \qquad \mathcal{N}_p = \mathfrak{m}^{s'_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}, \tag{3.2}$$

where $0 \le r'_{\mathfrak{P}} \le r_{\mathfrak{P}} \le 2 + 6\,\upsilon_{\mathfrak{P}}(2)$ *for* $\mathfrak{P} \mid 2$, *and* $0 \le r'_{\mathfrak{P}} \le r_{\mathfrak{P}} \le 2$ *for* $\mathfrak{P} \mid R$, *and* $0 \le s'_{\mathfrak{m}} \le s_{\mathfrak{m}} \le 2$.

Proof. The discriminant of the model given by E is $16(ABC)^2(abc)^{2p}$, thus the primes appearing in $\mathcal{N}$ will be either primes dividing $2R$ or dividing abc. For $\mathfrak{P} \mid 2$ we have $r_{\mathfrak{P}} = \upsilon_{\mathfrak{P}}(\mathcal{N}) \le 2 + 6\,\upsilon_{\mathfrak{P}}(2)$ by [11, Theorem IV.10.4]; this proves the correctness of the bounds for the exponents in $\mathcal{N}$ and $\mathcal{N}_p$ at even primes, and we will restrict our attention to odd primes. As E has full 2-torsion over K, the wild part of the conductor of E/K vanishes [11, p. 380] at all odd $\mathfrak{q}$, and so $\upsilon_{\mathfrak{q}}(\mathcal{N}_p) \le \upsilon_{\mathfrak{q}}(\mathcal{N}) \le 2$. This proves the correctness of the bounds for the exponents in $\mathcal{N}$ and $\mathcal{N}_p$ at $\mathfrak{q}$ that divide R and for $\mathfrak{q} = \mathfrak{m}$.

It remains to consider $\mathfrak{q} \mid abc$ satisfying $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. It is easily checked that the model (2.1) is minimal and has multiplicative reduction at such $\mathfrak{q}$, and it is therefore clear that $p \mid \upsilon_{\mathfrak{q}}(\Delta) = \upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. It follows that $\upsilon_{\mathfrak{q}}(\mathcal{N}) = 1$, and from the recipe for $\mathcal{N}_p$ in (2.2) that $\upsilon_{\mathfrak{q}}(\mathcal{N}_p) = 0$. ∎

4. Level lowering for the Frey curve

THEOREM 4.1. *Let K be a totally real field satisfying* (ES). *Let $A, B, C \in \mathcal{O}_K$ be odd, and suppose that every solution (λ, μ) to the S-unit equation* (1.3) *satisfies either condition* (A) *or* (B) *of Theorem* 1.2. *There is a constant $\mathcal{B} = \mathcal{B}(K, A, B, C)$ depending only on K and A, B, C such that the following hold. Let (a, b, c) be a non-trivial solution to the generalized Fermat equation* (1.1) *with prime exponent $p > \mathcal{B}$, and rescale (a, b, c) as in Lemma* 3.1 *so that it remains integral and satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Write $E = E_{a,b,c}$ for the Frey curve given in* (2.1). *Then there is an elliptic curve E' over K such that*

(i) *the conductor of E' is divisible only by primes in $S \cup \{\mathfrak{m}\}$;*
(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 $\mathfrak{P} \in U$, we have $\upsilon_{\mathfrak{P}}(j') < 0$;*
(b) *for $\mathfrak{P} \in V$, we have either $\upsilon_{\mathfrak{P}}(j') < 0$ or $3 \nmid \upsilon_{\mathfrak{P}}(j')$;*
(c) *for $\mathfrak{q} \notin S$, we have $\upsilon_{\mathfrak{q}}(j') \ge 0$.*

In particular, E' has potentially good reduction away from S.

Proof. We first observe, by Lemma 3.2, that E is semistable outside $S \cup \{\mathfrak{m}\}$. By taking $\mathcal{B}$ to be sufficiently large, we see from Corollary 2.3 that E is modular, and from Theorem 2.4 that $\overline{\rho}_{E,p}$ is irreducible. Applying Theorem 2.5 and Lemma 3.2, 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 $\mathfrak{f}$. The remainder of the proof is identical to the proof of [2, Theorem 9], and so we omit the details, except that we point out that it is here that we make use of assumption (ES). ∎

The constant $\mathcal{B}$ is ineffective as it depends on the ineffective constant $\mathcal{A}$ in Corollary 2.3. However, if K is a real quadratic field then we do not need that corollary as we get modularity from Theorem 2.1. In this case the arguments of [2] produce an effective constant $\mathcal{B}$.

5. Elliptic curves with full 2-torsion and solutions to the S-unit equation. Theorem 4.1 relates non-trivial solutions of the Fermat equation to elliptic curves with full 2-torsion having potentially good reduction outside S. There is a well-known correspondence between such elliptic curves and solutions of the S-unit equation (1.3) that we now sketch.

Consider an elliptic curve over K with full 2-torsion,

$$y^2 = (x - a_1)(x - a_2)(x - a_3), \tag{5.1}$$

where a_1, a_2, a_3 are distinct. The *cross ratio*

$$\lambda = \frac{a_3 - a_1}{a_2 - a_1}$$

belongs to $\mathbb{P}^1(K) - \{0, 1, \infty\}$. Moreover, any $\lambda \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ can be written as a cross ratio of three distinct a_1, a_2, a_3 in K and hence comes from an elliptic curve with full 2-torsion. Write $\mathfrak{S}_3$ for the symmetric group on three letters. The action of $\mathfrak{S}_3$ on the triple (e_1, e_2, e_3) extends via the cross ratio in a well-defined manner to an action on $\mathbb{P}^1(K) - \{0, 1, \infty\}$. The orbit of $\lambda \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ under the action of $\mathfrak{S}_3$ is

$$\left\{\lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}\right\}. \tag{5.2}$$

It follows from the theory of Legendre elliptic curves [10, pp. 53–55] that the cross ratio in fact defines a bijection between elliptic curves over K having full 2-torsion (up to isomorphism over $\overline{K}$), and λ-invariants up to the action of $\mathfrak{S}_3$. Under this bijection, the $\mathfrak{S}_3$-orbit of a given $\lambda \in \mathbb{P}^1(K) \setminus \{0, 1, \infty\}$ is associated to the $\overline{K}$-isomorphism class of the *Legendre elliptic curve* $y^2 = x(x-1)(x-\lambda)$. We would like to understand the λ-invariants that correspond to elliptic curves over K with full 2-torsion and potentially good reduction outside S. The j-invariant of the Legendre elliptic curve is given by

$$j(\lambda) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1-\lambda)^2}. \tag{5.3}$$

The Legendre elliptic curve (and therefore its $\overline{K}$-isomorphism class) has potentially good reduction outside S if and only if $j(\lambda)$ belongs to $\mathcal{O}_S$. It easily follows from (5.3) that this happens precisely when both λ and $1-\lambda$ are S-units (recall that S includes all the primes above 2); in other words, this is equivalent to (λ, μ) being a solution to the S-unit equation (1.3), where $\mu = 1-\lambda$. Let Λ_S be the set of solutions to the S-unit equation (1.3):

$$\Lambda_S = \{(\lambda, \mu) : \lambda + \mu = 1,\ \lambda, \mu \in \mathcal{O}_S^*\}. \tag{5.4}$$

It is easy to see that the action of $\mathfrak{S}_3$ on $\mathbb{P}^1(K) - \{0, 1, \infty\}$ induces a well-defined action on Λ_S given by

$$(\lambda, \mu)^\sigma = (\lambda^\sigma, 1 - \lambda^\sigma).$$

We denote by $\mathfrak{S}_3 \setminus \Lambda_S$ the set of $\mathfrak{S}_3$-orbits in Λ_S. We deduce the following.

Lemma 5.1. *Let $\mathcal{E}_S$ be the set of all elliptic curves over K with full 2-torsion and potentially good reduction outside S. Define the equivalence relation $E_1 \sim E_2$ on $\mathcal{E}_S$ to mean that E_1 and E_2 are isomorphic over $\overline{K}$. There is a well-defined bijection*

$$\Phi : \mathcal{E}_S/\sim \ \to \mathfrak{S}_3 \setminus \Lambda_S$$

which sends the class of an elliptic curve given by (5.1) to the orbit of

$$\left(\frac{a_3 - a_1}{a_2 - a_1}, \frac{a_2 - a_3}{a_2 - a_1}\right)$$

in $\mathfrak{S}_3 \setminus \Lambda_S$; the map Φ^{-1} sends the orbit of (λ, μ) to the class of the Legendre elliptic curve $y^2 = x(x-1)(x-\lambda)$.

We shall need the following for the proof of Theorem 1.2.

Lemma 5.2. *Let $E' \in \mathcal{E}_S$ and suppose that its $\sim$-equivalence class corresponds via Φ to the orbit of $(\lambda, \mu) \in \Lambda_S$. Let j' be the j-invariant of E' and $\mathfrak{P} \in T$. Then:*

(i) *$\upsilon_{\mathfrak{P}}(j') \geq 0$ if and only if* $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\, \upsilon_{\mathfrak{P}}(2)$;
(ii) *$3 \mid \upsilon_{\mathfrak{P}}(j')$ if and only $\upsilon_{\mathfrak{P}}(\lambda\mu) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$.*

Proof. Observe that

$$j' = j(\lambda) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = 2^8 \cdot \frac{(1 - \lambda\mu)^3}{(\lambda\mu)^2}. \tag{5.5}$$

From this we immediately deduce (ii). Let

$$m = \upsilon_{\mathfrak{P}}(\lambda), \qquad n = \upsilon_{\mathfrak{P}}(\mu), \qquad t = \max(|m|, |n|).$$

If $t = 0$ then $\upsilon_{\mathfrak{P}}(j') \geq 8\upsilon_{\mathfrak{P}}(2) > 0$, and so (i) holds. We may therefore suppose that $t > 0$. Now the relation $\lambda + \mu = 1$ forces either $m = n = -t$, or $m = 0$ and $n = t$, or $m = t$ and $n = 0$. Thus $\upsilon_{\mathfrak{P}}(\lambda\mu) = -2t < 0$ or $\upsilon_{\mathfrak{P}}(\lambda\mu) = t > 0$. In either case, from (5.3),

$$\upsilon_{\mathfrak{P}}(j') = 8\upsilon_{\mathfrak{P}}(2) - 2t.$$

This proves (i). ∎

6. Proof of Theorem 1.2. Let K be a totally real field satisfying assumption (ES). Let S, T, U, V be as in (1.2). Let $\mathcal{B}$ be as in Theorem 4.1, and let (a, b, c) be a non-trivial solution to the Fermat equation (1.1) with exponent $p > \mathcal{B}$, scaled so that $\mathcal{G}_{a,b,c} = \mathfrak{m}$ with $\mathfrak{m} \in \mathcal{H}$. Applying Theorem 4.1 gives an elliptic curve E'/K with full 2-torsion and potentially good reduction outside S whose j-invariant j' satisfies:

(a) for all $\mathfrak{P} \in U$, we have $\upsilon_{\mathfrak{P}}(j') < 0$;
(b) for all $\mathfrak{P} \in V$, we have $\upsilon_{\mathfrak{P}}(j') < 0$ or $3 \nmid \upsilon_{\mathfrak{P}}(j')$.

Let (λ, μ) be a solution to the S-unit equation (1.3), whose $\mathfrak{S}_3$-orbit corresponds to the $\overline{K}$-isomorphism class of E' as in Lemma 5.1. By Lemma 5.2 and (a), (b) we know that

(a′) for all $\mathfrak{P} \in U$, we have $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} > 4\,\upsilon_{\mathfrak{P}}(2)$;
(b′) for all $\mathfrak{P} \in V$, we have $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} > 4\,\upsilon_{\mathfrak{P}}(2)$ or $\upsilon_{\mathfrak{P}}(\lambda\mu) \not\equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$.

These contradict assumptions (A) and (B) of Theorem 1.2, completing the proof.

7. The S-unit equation over real quadratic fields. To prove Theorem 1.3 we need to understand the solutions to the S-unit equation (1.3) for real quadratic fields K. This is easier when S is small in size.

LEMMA 7.1. *Suppose $|S| = 2$. Let $(\lambda, \mu) \in \Lambda_S$. Then there is $\sigma \in \mathfrak{S}_3$ such that $(\lambda', \mu') = (\lambda, \mu)^\sigma$ satisfies $\lambda', \mu' \in \mathcal{O}_K$.*

Proof. As $\mu' = 1 - \lambda'$ we need only find $\sigma \in \mathfrak{S}_3$ such that $\lambda' = \lambda^\sigma \in \mathcal{O}_K$. Write $S = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. If $\upsilon_{\mathfrak{P}_i}(\lambda) \neq 0$ for $i = 1, 2$, then let $\lambda' = \lambda/(\lambda - 1)$, which will have non-negative valuation at $\mathfrak{P}_i$ and so belongs to $\mathcal{O}_K$. Thus without loss of generality we may suppose that $\upsilon_{\mathfrak{P}_1}(\lambda) = 0$. Now if $\upsilon_{\mathfrak{P}_2}(\lambda) \geq 0$ then $\lambda' = \lambda \in \mathcal{O}_K$, and if $\upsilon_{\mathfrak{P}_2}(\lambda) < 0$ then $\lambda' = 1/\lambda \in \mathcal{O}_K$. ∎

For the remainder of this section, d denotes a squarefree integer ≥ 13 that satisfies $d \equiv 5 \pmod 8$, and $q \geq 29$ a prime satisfying $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Let K denote the real quadratic field $\mathbb{Q}(\sqrt{d})$. It follows that both q and 2 are inert in K. We let $S = \{2, q\}$.

LEMMA 7.2. *Let K and S be as above, and let $(\lambda,\mu)\in\Lambda_S$. Then $\lambda,\mu\in\mathbb{Q}$ if and only if (λ,μ) belongs to the $\mathfrak{S}_3$-orbit $\{(1/2,1/2),(2,-1),(-1,2)\}\subseteq\Lambda_S$.*

Proof. Suppose $\lambda,\mu\in\mathbb{Q}$. By Lemma 7.1 we may suppose that λ and μ belong to $\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$, and hence $\lambda=\pm 2^{r_1}q^{s_1}$ and $\mu=\pm 2^{r_2}q^{s_2}$ where $r_i\geq 0$ and $s_i\geq 0$. As $\lambda+\mu=1$ we see that one of r_1, r_2 is 0, and likewise one of s_1,s_2 is 0. Without loss of generality $r_2=0$. If $s_2=0$ too then we have $\lambda\pm 1=1$, which forces $(\lambda,\mu)=(2,-1)$ as required. We may therefore suppose that $s_1=0$. Hence $\pm 2^{r_1}\pm q^{s_2}=1$. If $s_2=0$ then again we obtain $(\lambda,\mu)=(2,-1)$, so suppose $s_2>0$.

We now easily check that $r_1=1$ and $r_1=2$ are both incompatible with our hypotheses on q. Thus $r_1\geq 3$ and so $\mu=\pm q^{s_2}\equiv 1 \pmod 8$. As $q\equiv 5 \pmod 8$, we have $\mu=q^{2t}$ for some integer $t\geq 1$. Hence $(q^t+1)(q^t-1)=\mu-1=-\lambda=\mp 2^{r_1}$. This implies that $q^t+1=2^a$ and $q^t-1=2^b$ where $a\geq b\geq 1$. Subtracting we have $2^a-2^b=2$, and so $b=1$ and $q=3$, giving a contradiction. ∎

Following [2] we call the elements of the orbit $\{(1/2,1/2),(2,-1),(-1,2)\}$ *irrelevant*, and other elements of Λ_S *relevant.* Next we give a parametrization of all relevant elements of Λ_S. This the analogue of [2, Lemma 6.4], and shows that such a parametrization is possible even though our set S is larger, containing the odd prime q.

LEMMA 7.3. *Up to the action of $\mathfrak{S}_3$, every relevant $(\lambda,\mu)\in\Lambda_S$ has the form*

$$(7.1)\qquad \lambda=\frac{\eta_1\cdot 2^{2r_1}\cdot q^{2s_1}-\eta_2\cdot q^{2s_2}+1+v\sqrt{d}}{2},\qquad \mu=\frac{\eta_2\cdot q^{2s_2}-\eta_1\cdot 2^{2r_1}\cdot q^{2s_1}+1-v\sqrt{d}}{2}$$

where

$$(7.2)\qquad \eta_1=\pm 1,\quad \eta_2=\pm 1,\quad r_1\geq 0,\quad s_1,s_2\geq 0,\quad s_1\cdot s_2=0,\quad v\in\mathbb{Z},\quad v\neq 0,$$

are related by

$$(7.3)\qquad (\eta_1\cdot 2^{2r_1}\cdot q^{2s_1}-\eta_2\cdot q^{2s_2}+1)^2-dv^2=\eta_1\cdot 2^{2r_1+2}\cdot q^{2s_1},$$

$$(7.4)\qquad (\eta_2\cdot q^{2s_2}-\eta_1\cdot 2^{2r_1}\cdot q^{2s_1}+1)^2-dv^2=\eta_2\cdot 2^2\cdot q^{2s_2}.$$

Proof. If η_1, η_2, r_1, s_1, s_2 and v satisfy (7.2)–(7.4) and λ, μ are given by (7.1), it is clear that (λ,μ) is a relevant element of Λ_S.

Conversely, suppose (λ,μ) is a relevant element of Λ_S. By Lemma 7.2, we may suppose that $\lambda,\mu\in\mathcal{O}_K$ and $\lambda,\mu\notin\mathbb{Q}$. As $S=\{2,q\}$ we can write $\lambda=2^{r_1}q^{s_1}\lambda'$ and $\mu=2^{r_2}q^{s_2}\mu'$ where λ' and μ' are units. As $\lambda+\mu=1$ we have $r_1 r_2 = 0$ and $s_1 s_2 = 0$. Swapping λ and μ if necessary, we can suppose that $r_2 = 0$. Let $x \mapsto \overline{x}$ denote conjugation in K. Then

$$\lambda\overline{\lambda} = \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1}, \qquad \mu\overline{\mu} = \eta_2 \cdot q^{2s_2}, \qquad \eta_1 = \pm 1, \qquad \eta_2 = \pm 1.$$

Now,

$$\begin{aligned} \lambda + \overline{\lambda} &= \lambda\overline{\lambda} - (1-\lambda)(1-\overline{\lambda}) + 1 = \lambda\overline{\lambda} - \mu\overline{\mu} + 1 \\ &= \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} - \eta_2 \cdot q^{2s_2} + 1. \end{aligned}$$

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 (7.1), and we deduce the expression for μ from $\mu = 1 - \lambda$. Finally, (7.3) follows from the identity

$$(\lambda + \overline{\lambda})^2 - (\lambda - \overline{\lambda})^2 = 4\lambda\overline{\lambda},$$

and (7.4) from the corresponding identity for μ. ■

Lemma 7.4. *Let $d \equiv 5 \pmod 8$ be squarefree ≥ 13, and $q \geq 29$ a prime such that $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Then there are no relevant elements of Λ_S.*

Proof. We apply Lemma 7.3. In particular, $s_1 s_2 = 0$. Suppose first that $s_1 > 0$. Thus $s_2 = 0$. As $\left(\frac{d}{q}\right) = -1$, we deduce from (7.3) that $q^{s_1} \mid v$ and $q^{s_1} \mid (\eta_2 - 1)$. Hence $\eta_2 = 1$. Now (7.3) can be rewritten as

$$2^{4r_1} q^{2s_1} - d(v/q^{s_1})^2 = \eta_1 2^{2r_1+2}.$$

Thus $\left(\frac{d}{q}\right) = \left(\frac{-\eta_1}{q}\right) = 1$ as $q \equiv 5 \pmod 8$. This is a contradiction.

Thus, henceforth, $s_1 = 0$. Next suppose that $s_2 = 0$. We will consider the subcases $\eta_2 = -1$ and $\eta_2 = 1$ separately and obtain contradictions in both subcases showing that $s_2 > 0$.

Suppose $\eta_2 = -1$. From (7.4) we have $2^{4r_1} - dv^2 = -4$. If $r_1 = 0$ or 1 then $d = 5$, and if $r_1 \geq 2$ then $d \equiv 1 \pmod 8$, giving a contradiction.

Hence suppose $\eta_2 = 1$. From (7.3), we have $2^{4r_1} - dv^2 = \eta_1 2^{2r_1+2}$. If $r_1 = 0, 1, 2$ then $dv^2 = 1 \pm 4$, $dv^2 = 16 \pm 16$, $dv^2 = 256 \pm 64$, all of which contradict the assumptions on d or the fact that $v \neq 0$ (by (7.2)). If $r_1 \geq 3$ then $2^{2r_1-2} - \eta_1 = d(v/2^{r_1+1})^2$, which forces $d \equiv \pm 1 \pmod 8$, a contradiction.

We are reduced to $s_1 = 0$ and $s_2 > 0$. From (7.4), as $\left(\frac{d}{q}\right) = -1$, we have $q^{s_2} \mid v$ and

$$q^{s_2} \mid (\eta_1 2^{2r_1} - 1). \tag{7.5}$$

The conditions $q \geq 29$ and $q \equiv 5 \pmod 8$ force $r_1 \geq 5$. Write $v = 2^t w$ where $2 \nmid w$. Suppose $t \leq r_1 - 1$. From (7.3) we have $\eta_1 2^{2r_1} - \eta_2 q^{2s_2} + 1 = 2^t w'$ where $2 \nmid w'$. Thus ${w'}^2 - dw^2 \equiv 0 \pmod 8$, contradicting $d \equiv 5 \pmod 8$. We may therefore suppose $t \geq r_1$. Hence $2^{r_1} \mid (\eta_2 q^{2s_2} - 1)$. Thus $\eta_2 = 1$.

Therefore $2^{r_1} \mid (q^{s_2} - 1)(q^{s_2} + 1)$. Since $q \equiv 5 \pmod 8$, we have $2 \parallel (q^{s_2} + 1)$ and so

$$2^{r_1 - 1} \mid (q^{s_2} - 1).$$

As $q \equiv 5 \pmod 8$ and $r_1 \geq 5$, we see that s_2 must be even, and that $2^{r_1-2} \mid (q^{s_2/2} - 1)$. We can write $q^{s_2/2} = k \cdot 2^{r_1-2} + 1$. From (7.5),

$$k^2 2^{2r_1-4} + k2^{r_1-1} + 1 = q^{s_2} \leq 2^{2r_1} + 1.$$

Hence $k = 1$, 2 or 3. Moreover, as $q^{s_2/2} \equiv 1 \pmod 8$, we have $4 \mid s_2$. Hence

$$(q^{s_2/4} - 1)(q^{s_2/4} + 1) = k2^{r_1-2}.$$

Again as $q \equiv 5 \pmod 8$ we have $2 \parallel (q^{s_2/4} + 1)$ and so $q^{s_2/4} + 1 = 2$ or 6, both of which are impossible. This completes the proof. ∎

8. Proof of Theorem 1.3. We apply Theorem 1.2. By Lemma 7.4 all solutions to (1.3) are irrelevant, and the irrelevant solutions satisfy condition (A) of Theorem 1.2. This completes the proof of Theorem 1.3.

Acknowledgements. The author's research is funded by an EPSRC studentship.

References

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

[2] N. Freitas and S. Siksek, *An asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields*, Compos. Math. 151 (2015), 1395–1415.

[3] N. Freitas and S. Siksek, *Fermat's Last Theorem for some small real quadratic fields*, Algebra Number Theory 9 (2015), 875–895.

[4] N. Freitas and S. Siksek, *Criteria for irreducibility of mod p representations of Frey curves*, J. Théor. Nombres Bordeaux 27 (2015), 67–76.

[5] K. Fujiwara, *Level optimisation in the totally real case*, arXiv:0602586v1 (2006).

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

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

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

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

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[11] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

[12] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Texts 41, Cambridge Univ. Press, 1998.

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

Heline Deconinck
Mathematics Institute
University of Warwick
Coventry, CV4 7AL, United Kingdom
E-mail: heline.deconinck@gmail.com