Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2020) 44: 1197 – 1211
© TÜBİTAK
doi:10.3906/mat-1911-88

On ternary Diophantine equations of signature $(p, p, 2)$ over number fields

Erman IŞIK, Yasemin KARA, Ekin OZMAN*
Department of Mathematics, Faculty of Arts and Sciences, Boğaziçi University, İstanbul, Turkey

Received: 25.11.2019 • **Accepted/Published Online:** 04.06.2020 • **Final Version:** 08.07.2020

Abstract: Let K be a totally real number field with narrow class number one and $\mathcal{O}_K$ be its ring of integers. We prove that there is a constant B_K depending only on K such that for any prime exponent $p > B_K$ the Fermat type equation $x^p + y^p = z^2$ with $x, y, z \in \mathcal{O}_K$ does not have certain type of solutions. Our main tools in the proof are modularity, level lowering, and image of inertia comparisons.

Key words: Fermat equation, generalized Fermat equation, S-units, modularity

1. Introduction

Solving Diophantine equations, in particular Fermat type equations, is of great interest in the area of number theory especially since the proof of Fermat's Last Theorem. Recently, there has been much progress in several different generalizations of this famous result. For instance, in [33], Freitas and Siksek proved the asymptotic Fermat's Last Theorem (FLT) for certain totally real fields K. That is, they showed that there is a constant B_K such that for any prime $p > B_K$, the only solutions to the Fermat equation $a^p + b^p + c^p = 0$ where $a, b, c \in \mathcal{O}_K$ are the trivial ones satisfying $abc = 0$. Then, Deconinck [26] extended the results of Freitas and Siksek [33] to the generalized Fermat equation of the form $Aa^p + Bb^p + Cc^p = 0$ where A, B, C are odd integers belonging to a totally real field. Later in [43], Şengün and Siksek proved the asymptotic FLT for any number field K by assuming modularity. This result has been generalized by Kara and Ozman in [36] to the case of generalized Fermat equation. Also, recently in [51] and [52] Turcas studied Fermat equation over imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with class number one.

However, such generalizations are quite rare for other Fermat type equations such as $x^p + y^p = z^2$. The solutions of this equation have been studied over rationals by many mathematicians including Darmon, Merel, Bennett, and Poonen. Several mathematicians have worked on similar Fermat type equations of different exponent over rational numbers. We summarize these results in the following sections. However, not many results exist for generalizations of these to higher degree number fields. We study such generalizations and get an asymptotic result about certain type of solutions of $x^p + y^p = z^2$ over number fields similar to those obtained for $Ax^p + By^p + Cz^p = 0$. Our results can be summarized as follows.

*Correspondence: ekin.ozman@boun.edu.tr
2010 *AMS Mathematics Subject Classification:* 11D41, 11G05, 11D45

1.1. Our results

Let K be a totally real number field and $\mathcal{O}_K$ be its ring of integers. For a prime number p, we refer the equation

$$a^p + b^p = c^2, \quad a, b, c \in \mathcal{O}_K \tag{1.1}$$

as "the Fermat equation over K with signature $(p, p, 2)$". A solution (a, b, c) is called trivial if $abc = 0$, otherwise nontrivial. We say that "the asymptotic Fermat Theorem holds for K" if there is a constant B_K such that for any prime $p > B_K$, the Fermat equation with signature $(p, p, 2)$ (given in equation (1.1)) does not have nontrivial solutions. This is equivalent to the statement that the set $\underset{p \text{ prime}}{\cup} C_p(K)$ is finite where C_p is the curve given by $x^p + y^p = z^2$. Note that for a fixed prime $p > 3$ the set $C_p(K)$ is finite by Faltings' theorem. However, having a constant B_K as mentioned above means that $C_p(K)$ is empty for big enough prime p; hence, $\underset{p \text{ prime}}{\cup} C_p(K)$ is finite.

Throughout the paper, we assume that $h_K^+ = 1$ where h_K^+ denotes the narrow class number of K. A solution (a, b, c) of equation (1.1) is called primitive if a, b, and c are pairwise coprime. Note that if $a, b, c \in \mathcal{O}_K$ satisfy $a^p + b^p = c$, where p is an odd prime, then $(ac, bc, c^{\frac{p+1}{2}})$ is a nonprimitive solution to the equation (1.1). Therefore, we will consider only primitive solutions to (1.1). Let us define

$$S_K = \{\mathfrak{P} : \mathfrak{P} \text{ is prime of } \mathcal{O}_K \text{ such that } \mathfrak{P}|2\} \text{ and } T_K = \{\mathfrak{P} \in S_K : f(\mathfrak{P}/2) = 1\}$$

where $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. Write $\mathcal{O}_{S_K}$ for the ring of S_K-integers in K and $\mathcal{O}_{S_K}^*$ for the set of S_K-units of K. We define the n-Selmer group of K and S_K to be $K(S_K, n) = \{x \in K^*/K^{*n} : v_\mathfrak{p}(x) \equiv 0 \mod n, \forall \mathfrak{p} \notin S_K\}$. It is known that $K(S_K, n)$ is a finite abelian group ([20], sections 5.2.2 and 7.4). Now, let $L = K(\sqrt{a})$ for $a \in K(S_K, 2)$ and define $S_L = \{\mathfrak{P}' : \mathfrak{P}' \text{ is prime of } \mathcal{O}_L \text{ such that } \mathfrak{P}'|2\}$ and $T_L = \{\mathfrak{P}' \in S_L : \mathfrak{P}'|\mathfrak{P} \text{ for some } \mathfrak{P} \in T_K\}$.

Similarly, write $\mathcal{O}_{S_L}$ for the ring of S_L-integers in L and $\mathcal{O}_{S_L}^*$ for the set of S_L-units of L. Finally, let W_K be the set of $(a, b, c) \in \mathcal{O}_K^3$ such that $a^p + b^p = c^2$ with $\mathfrak{P}|b$ for every $\mathfrak{P} \in T_K$.

Theorem 1.1 (Main Theorem.) *Let K be a totally real number field with narrow class number $h_K^+ = 1$. For each $a \in K(S_K, 2)$, let $L = K(\sqrt{a})$. Suppose that for every solution (λ, μ) to the S_K-unit equation*

$$\lambda + \mu = 1, \qquad \lambda, \mu \in \mathcal{O}_{S_K}^*, \tag{1.2}$$

there is some $\mathfrak{P} \in T_K$ that satisfies $\max\{|v_\mathfrak{P}(\lambda)|, |v_\mathfrak{P}(\mu)|\} \leq 4v_\mathfrak{P}(2)$.

Suppose also that for each L, for every solution (λ, μ) to the S_L-unit equation $\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_{S_L}^*$, there is some $\mathfrak{P}' \in T_L$ that satisfies $\max\{|v_{\mathfrak{P}'}(\lambda)|, |v_{\mathfrak{P}'}(\mu)|\} \leq 4v_{\mathfrak{P}'}(2)$.

Then there is a constant B_K—depending only on K—such that for $p > B_K$, equation (1.1) has no solution $(a, b, c) \in W_K$. In other words, $\underset{p \text{ prime}}{\cup} (C(K) \cap W_K)$ is finite. In this case we say that asymptotic Fermat's Last Theorem holds for W_K.

Our strategy to solve the Main Theorem is similar to the method used in [33] and more general explanation of this strategy can be found in [33]. We summarize it here for the convenience of the reader. A nontrivial primitive solution to the equation (1.1) over a totally real number field K with $h_K^+ = 1$ and $T_K \neq \emptyset$ yields a Hilbert modular form $\mathfrak{f}$ of parallel weight 2 and level divisible only by primes in T_K. In general, there are newforms at these levels [35]. This is where our attempt differs from the proof of Fermat's Last Theorem over $\mathbb{Q}$. After enlarging the prime exponent p enough, the Hilbert modular form $\mathfrak{f}$ gives rise to, via Eichler–Shimura construction, an elliptic curve E' defined over K having a nontrivial K-rational point of order 2 and good reduction outside S_K (There are such elliptic curves over every K, for instance $Y^2 = X^3 - X$, so we do not have a contradiction yet). However, such an E' has full 2-torsion over either K or a certain type quadratic extension of K, and we can parametrize all such E' in terms of solutions (λ, μ) to S_K(or S_L)-unit equation $\lambda + \mu = 1$. This type of equation has solutions $(2, -1), (-1, 2), (1/2, 1/2)$ and possibly others and hence cannot end up with a contradiction yet. However, the action of inertia on $E[p]$ for $\mathfrak{P} \in T_K$ gives information on the valuations $\upsilon_{\mathfrak{P}}(\lambda)$, $\upsilon_{\mathfrak{P}}(\mu)$, allowing us to prove the Main Theorem.

1.2. Previous results

Even before Wiles announced his proof, various generalizations of Fermat's Last Theorem had already been considered, which is of the shape

$$Ax^p + By^q = Cz^r, \tag{1.3}$$

for fixed integers A, B, and C. We call (p, q, r) the *signature* of the equation (1.3). The behaviour of primitive solutions depends fundamentally upon the size of the quantity $\sigma(p, q, r) = \dfrac{1}{p} + \dfrac{1}{q} + \dfrac{1}{r}$, in particular, whether $\sigma(p, q, r) < 1$, $\sigma(p, q, r) = 1$ or $\sigma(p, q, r) > 1$. We will focus on the case $\sigma(p, q, r) < 1$, for other cases we refer to [7]. In this case, we know that, for a fixed signature (p, q, r) the number of integer solutions to equation (1.3) is finitely many by a theorem of Darmon and Granville [24]. It is worth to mention that the argument used in the proof is ineffective, meaning that it does not give us an algorithm to find all possible solutions since it depends on the Falting's theorem [30]. In the following tables, we list all known cases where equation (1.3) has been solved in integers. Table 1 contains all unconditional results for infinitely many primes. In Table 2, we give all conditional results, which we denote by $*$ and/or for finitely many signature (p, q, r). For example, in [17], the equation $x^2 + y^{2p} = z^5$ has no solutions if $p \equiv 1 \pmod 4$.

In some signatures the equation also has coefficients. For instance, in [9] the equation $x^5 + y^5 = 3z^p$ is solved. However, in the tables we did not mention the coefficients.

Due to works by Derickx by [27] and Freitas et al. [31], we know the modularity of elliptic curves over quadratic and real cubic number fields. Under certain assumptions of modularity, irreducibility, and level-lowering, we get some results on the equation $Ax^p + By^p = Cz^p$ asymptotically, which we refer the reader to [33, 34] for the case $A = B = C = 1$, and to [26, 36] for a more general result.

2. Preliminaries

In this section, we provide the theoretical results we need concerning modularity, irreducibility of mod p Galois representations, level lowering and Conjecture 2.5 to prove our theorem. We follow [33] and the references therein.

Let G_K be the absolute Galois group of a number field K, E/K be an elliptic curve and $\overline{\rho}_{E,p}$ denote the mod p Galois representation of E. We use $\mathfrak{q}$ for an arbitrary prime of K, and $G_{\mathfrak{q}}$ and $I_{\mathfrak{q}}$ respectively for the decomposition and inertia subgroups of G_K at $\mathfrak{q}$. Let $\mathfrak{f}$ be a Hilbert eigenform over K. We denote the

Table 1. The infinite family of the equations with signature (p, q, r) without additional conditions.

(p, q, r)	reference(s)
(n, n, n), $n \geq 3$	Wiles [53], Taylor and Wiles [50]
(n, n, k), $n \geq 4$, $k \in \{2, 3\}$	Darmon and Merel [25], Poonen [41]
$(2n, 2n, 5)$, $n \geq 2$	Bennett [3]
$(2, 4, n)$, $n \geq 4$	Ellenberg [29], Bennett et al. [6],Bruin [14]
$(2, 6, n)$, $n \geq 3$	Bennett and Chen [4], Bruin [14]
$(2, n, 4)$, $n \geq 4$	Bennett and Skinner [8], Bruin [14]
$(2, n, 6)$, $n \geq 3$	Bennett et al. [5]
$(3j, 3k, n)$,$j, k \geq 2$, $n \geq 3$	immediate from Kraus [39]
$(3, 3, 2n)$, $n \geq 2$	Bennett et al. [5]
$(3, 6, n)$, $n \geq 2$	Bennett et al. [5]
$(2, 2n, k)$, $k \in \{9, 10, 15\}$, $n \geq 2$	Bennett et al. [5]
$(4, 2n, 3)$,	Bennett et al. [5]
$(2j, 2k, n)$, $j, k \geq 5$ prime, $n \in \{3, 5, 7, 11, 13\}$	Anni and Siksek [2]
$(13, 13, n)$, $n \geq 17$ or $n = 11$	Dieulefait and Freitas [28], Freitas and Samir [32]
$(5, 5, n)$, $n \geq 13$	Billerey et al. [9], and Billerey and Dieulefait [11]

Table 2. The equations with signature (p, q, r) of finite family or with additional conditions.

(p, q, r)	reference(s)
$(3, 3, n)^*$	Chen and Siksek [19], Kraus [40], Bruin [15, 16], Dahmen [21]
$(2, 2n, 3)^*$	Chen [18], Dahmen [22], Siksek [44]
$(2n, 2n, 5)^*$ $n \geq 2$	Bennett [3]
$(2, 2n, 5)^*$	Chen [17]
$(2m, 2n, 3)^*$	Bennett et al. [5]
$(2, 4n, 3)^*$	Bennett et al. [5]
$(3, 3n, 2)^*$	Bennett et al. [5]
$(2, 3, n)$,$n \in \{6, 7, 8, 9, 10, 15\}$	Poonen et al. [42], Bruin[14], Zureick and Brown [13], Siksek [45], Siksek and Stoll [47]
$(3, 4, 5)$	Siksek and Stoll [46]
$(5, 5, 7)$, $(7, 7, 5)$	Dahmen and Siksek [23]
$(n, n, r)^*$, $r \geq 5$ regular prime	Billerey et al. [10]

field generated by its eigenvalues by $\mathbb{Q}_\mathfrak{f}$ and a prime of $\mathbb{Q}_\mathfrak{f}$ above p by $\overline{\omega}$. For $(a, b, c) \in W_K$ with a prime exponent p, we associate the Frey elliptic curve

$$E = E_{a,b,c} : Y^2 = X^3 + 4cX^2 + 4a^pX. \tag{2.1}$$

2.1. Modularity of the Frey curve

In order to run the modular approach to solve Diophantine equations one needs modularity theorems. Freitas et al. proved the following theorem in [31].

Theorem 2.1 *Let K be a totally real field. Up to isomorphism over $\overline{K}$, there are at most finitely many nonmodular elliptic curves E over K. Moreover, if K is real quadratic, all elliptic curves over K are modular.*

Furthermore, Derickx, Najman and Siksek have recently proved the below theorem in [27].

Theorem 2.2 *Let K be a totally real cubic number field and E be an elliptic curve over K. Then E is modular.*

Hence, we have the modularity result for the Frey elliptic curve $E_{a,b,c}$ given in (2.1) if it is over a real quadratic or totally real cubic field. Otherwise, we will assume the modularity as a conjecture.

2.2. Irreducibility of mod p representations of elliptic curves

In this section, we state the result giving us the irreducibility of the mod p Galois representations associated to the Frey elliptic curve. We need this result in the level lowering step. The below theorem can be found in [34] as Theorem 2 deduced from the work of David, Momose, and Merel's uniform boundedness theorem.

Theorem 2.3 *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 a prime and E/K is an elliptic curve which is semistable at all $\mathfrak{q}|p$, then $\overline{\rho}_{E,p}$ is irreducible.*

One can see that the above theorem is also true for any totally real field by replacing K by its Galois closure.

2.3. Level lowering

We present a level lowering result by Freitas and Siksek [33] derived from the work by Fujira, Jarvis, and Rajaei. Let K be a totally real field, and E/K be an elliptic curve of conductor $\mathcal{N}_E$. Let p be a rational prime. Define the following quantities

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q}\|\mathcal{N}_E,\\ p|\upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q}, \text{ and } \mathcal{N}_p := \frac{\mathcal{N}_E}{\mathcal{M}_p},$$

where $\Delta_{\mathfrak{q}}$ is the minimal discriminant of a local minimal model for E at $\mathfrak{q}$. For a Hilbert eigenform $\mathfrak{f}$ over K, we write $\mathbb{Q}_{\mathfrak{f}}$ for the field generated by its eigenvalues.

Theorem 2.4 *With the notation above, suppose the following statements hold:*

(i) $p \geq 5$, *the ramification index* $e(\mathfrak{q}/p) < p-1$ *for all* $\mathfrak{q}|p$, *and* $\mathbb{Q}(\zeta_p)^+ \nsubseteq K$,

(ii) E *is modular,*

(iii) $\overline{\rho}_{E,p}$ *is irreducible,*

(iv) E *is semistable at all* $\mathfrak{q}|p$,

(v) $p|\upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ *for all* $\mathfrak{q}|p$.

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 $\varpi|p$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$.

2.4. Eichler–Shimura

The Eichler–Shimura Conjecture, which is stated below, has not been proven yet in general. However, there are some partial results towards it. Here, we state a result that is needed in order to prove Theorem 4.1.

Conjecture 2.5 ('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 $\mathfrak{f}$.*

The following theorem proven in [12] gives a partial answer to Conjecture 2.5.

Theorem 2.6 *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 either:*

(i) $[K:\mathbb{Q}]$ is odd; or

(ii) 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 $\mathfrak{f}$.

Freitas and Siksek obtain the following corollary from the above theorem in [33].

Corollary 2.7 *Let E be an elliptic curve over a totally real field K, and p be an odd prime. Suppose that $\overline{\rho}_{E,p}$ is irreducible, and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},p}$ 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 ideal of $\mathcal{O}_K$ such that:*

(a) E has potentially multiplicative reduction at $\mathfrak{q}$,

(b) $p | \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$,

(c) $p \nmid (Norm_{K/\mathbb{Q}}(\mathfrak{q}) \pm 1)$

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

3. Frey curve and related facts

3.1. Behaviour at odd primes

Let u, v, and w be elements of $\mathcal{O}_K$ such that $u + v = w^2$ and $uvw \neq 0$. Consider the elliptic curve

$$E : Y^2 = X^3 + 4wX^2 + 4uX \tag{3.1}$$

whose arithmetic invariants are given by $\Delta_E = 2^{12}u^2v$, $j_E = 2^6\dfrac{(u+4v)^3}{u^2v}$, and $c_4 = 2^6(4w^2 - 3u) = 2^6(4v+u)$.

We can prove the following lemma by using the properties of elliptic curves over local fields (see, e.g., [[48],§VII.1 and VII.5])

Lemma 3.1 *With the notation above, let $\mathfrak{q} \nmid 2$ be a prime ideal of $\mathcal{O}_K$ and*

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

Write E_{min} for a local minimal model at $\mathfrak{q}$. Then we have the following:

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

$$\upsilon_{\mathfrak{q}}(u) = \upsilon_{\mathfrak{q}}(v) = 2\upsilon_{\mathfrak{q}}(w). \tag{3.2}$$

(ii) E_{min} *has multiplicative reduction at* $\mathfrak{q}$ *if and only if* s *is even and the equality (3.2) does not hold. In this case, the minimal discriminant* $\Delta_{\mathfrak{q}}$ *at* $\mathfrak{q}$ *satisfies*

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

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

Proof Let π be the uniformizer of $K_{\mathfrak{q}}$. Suppose that the Weierstrass equation of E is not in the minimal form. Then we have $\upsilon_{\mathfrak{q}}(\Delta_E) \geq 12$ and $\upsilon_{\mathfrak{q}}(c_4) \geq 4$. Combining these with $\pi \nmid 2$, we get that π divides all of u, v, and w.

Now we may use the change of coordinates

$$\begin{array}{rcl} X & \mapsto & t^2X' \\ Y & \mapsto & t^3Y', \end{array}$$

to get the elliptic curve $E' : Y'^2 = X'^3 + 4wt^{-2}X'^2 + 4ut^{-4}X'$.

If the equation was in the minimal form at the beginning, we could take $t = 1$, if not take $t = \pi^s$, where s is the number of times we have to do change of variables to get the minimal form.

For (i), E' has good reduction at $\mathfrak{q}$ if and only if $\upsilon_{\mathfrak{q}}(\Delta_{E'}) = 0$, which holds if and only if $\upsilon_{\mathfrak{q}}(u') = \upsilon_{\mathfrak{q}}(v') = 0$. Note that $\upsilon_{\mathfrak{q}}(u') = \upsilon_{\mathfrak{q}}(u) - 4\upsilon_{\mathfrak{q}}(t)$ and $\upsilon_{\mathfrak{q}}(v') = \upsilon_{\mathfrak{q}}(v) - 2\upsilon_{\mathfrak{q}}(t)$. Hence, E' has good reduction at $\mathfrak{q}$ if and only if $\upsilon_{\mathfrak{q}}(u) = \upsilon_{\mathfrak{q}}(v) = 4\upsilon_{\mathfrak{q}}(t) = 2\upsilon_{\mathfrak{q}}(w)$. We can apply a similar argument to prove (ii) and (iii). □

3.2. Conductor of the Frey curve

Let (a, b, c) be a nontrivial solution to the equation $x^p + y^p = z^2$ with the prime exponent p. Since the narrow class number of K is 1, we can assume that (a, b, c) is a primitive solution. In other words, any prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ can divide at most one of a, b, and c. On the other hand, if $\mathfrak{P} \in T_K$ and $\mathfrak{P} \nmid abc$ we get $0 = a^p + b^p - c^2 \equiv 1 + 1 + 1 \pmod{\mathfrak{P}}$. This gives a contradiction since $\mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_2$. Therefore, we see that $\mathfrak{P}$ divides exactly one of a, b and c.

Recall that for a solution $(a, b, c) \in W_K$ with a prime exponent p, we associate the following Frey elliptic curve defined over K as

$$E = E_{a,b,c} : Y^2 = X^3 + 4cX^2 + 4a^pX$$

with the arithmetic invariants $\Delta_E = 2^{12}(a^2b)^p$, $j_E = 2^6\dfrac{(4b^p + a^p)^3}{(a^2b)^p}$, and the conductor $\mathcal{N}_E$. Recall also the quantities

$$\mathcal{M}_p = \prod_{\substack{\mathfrak{q} \| \mathcal{N}_E, \\ p | \upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q}, \text{ and } \mathcal{N}_p = \mathcal{N}_E/\mathcal{M}_p,$$

where $\Delta_{\mathfrak{q}}$ is the minimal discriminant of a local minimal model for E at $\mathfrak{q}$.

Lemma 3.2 *Let (a,b,c) be the nontrivial primitive solution to the equation (1.1). Let E be the associated Frey curve with conductor $\mathcal{N}_E$. Then, for all primes $\mathfrak{q} \notin S_K$, the model E is minimal, semistable and satisfies $p|\upsilon_{\mathfrak{q}}(\Delta_E)$. Moreover,*

$$\mathcal{N}_E = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r_{\mathfrak{P}}} \prod_{\substack{\mathfrak{q}|ab,\\ \mathfrak{q} odd\ prime}} \mathfrak{q}, \quad \mathcal{N}_p = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r'_{\mathfrak{P}}},$$

where $0 \le r'_{\mathfrak{P}} \le r_{\mathfrak{P}} \le 2 + 6\upsilon_{\mathfrak{P}}(2)$.

Proof Let $\mathfrak{q}$ be an odd prime of K. The invariants of the model E are $\Delta_E = 2^{12}(a^2b)^p$ and $c_4 = 2^6(4b^p + a^p)$. Suppose that $\mathfrak{q}$ divides Δ_E, so $\mathfrak{q}|ab$. Since a and b are relatively prime, $\mathfrak{q}$ divides exactly one of a and b. Therefore, $\mathfrak{q}$ does not divide c_4. By Lemma 3.1, E has multiplicative reduction at $\mathfrak{q}$ and is minimal. Hence, $p|\upsilon_{\mathfrak{q}}(\Delta_E) = \upsilon_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. By the definition of $\mathcal{N}_p$, $\mathfrak{q} \nmid \mathcal{N}_p$. By [[49], Theorem IV.10.4], $r = \upsilon_{\mathfrak{q}}(\mathcal{N}_E) \le 2 + 6\upsilon_{\mathfrak{P}}(2)$.
□

3.3. Images of Inertia

Now, we collect some necessary information about images of inertia $\overline{\rho}_{E,p}(I_{\mathfrak{q}})$. The following is Lemma 3.4 in [33].

Lemma 3.3 *Let E be an elliptic curve over K with j-invariant j_E. Let $p \ge 5$ and $\mathfrak{q} \nmid p$ be a prime of K. Then $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $\upsilon_{\mathfrak{q}}(j_E) < 0$) and $p \nmid \upsilon_{\mathfrak{q}}(j_E)$.*

By using the previous result we obtain:

Lemma 3.4 *Let $\mathfrak{q} \nmid 2$ and let (a,b,c) be a nontrivial primitive solution to the equation (1.1) with the prime exponent $p \ge 5$ such that $\mathfrak{q} \nmid p$. Let E be the Frey curve in (2.1) . Then $p \nmid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$.*

Proof Using Lemma 3.3, it is enough to show that at all $\mathfrak{q} \nmid 2$ with $\mathfrak{q} \nmid p$ either $\upsilon_{\mathfrak{q}}(j_E) \ge 0$ or $p|\upsilon_{\mathfrak{q}}(j_E)$. If $\mathfrak{q} \nmid \Delta_E$, then E has good reduction at $\mathfrak{q}$, so $\upsilon_{\mathfrak{q}}(j_E) \ge 0$. If $\mathfrak{q}|\Delta_E$, then $\mathfrak{q}|ab$. Thus, $\mathfrak{q}$ divides exactly one of a and b. This implies that $\mathfrak{q} \nmid c_4$, i.e. $\upsilon_{\mathfrak{q}}(c_4) = 0$. Thus, $\upsilon_{\mathfrak{q}}(j_E) = -p\upsilon_{\mathfrak{q}}(a^2b)$, i.e. $p|\upsilon_{\mathfrak{q}}(j_E)$. □

Lemma 3.5 *Let $\mathfrak{P} \in T_K$ and let $(a,b,c) \in W_K$ with prime exponent $p > 6\upsilon_{\mathfrak{P}}(2)$. Let E be the Frey curve in (2.1) and write j_E for its j-invariant. Then E has potentially multiplicative reduction at $\mathfrak{P}$ and $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.*

Proof Assume that $\mathfrak{P} \in T_K$ with $\upsilon_{\mathfrak{P}}(b) = k$. Then $\upsilon_{\mathfrak{P}}(j_E) = 6\upsilon_{\mathfrak{P}}(2) - pk$. Since $p > 6\upsilon_{\mathfrak{P}}(2)$, $\upsilon_{\mathfrak{P}}(j_E) < 0$ and clearly $p \nmid \upsilon_{\mathfrak{P}}(j_E)$. This implies that E has potentially multiplicative reduction at $\mathfrak{P}$ and $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.
□

4. Level lowering

Theorem 4.1 *Let K be a totally real number field with $h_K^+ = 1$ and assume $T_K \neq \emptyset$. There is a constant B_K depending only on K such that the following hold. Let $(a,b,c) \in W_K$ with prime exponent $p > B_K$. Write E for the Frey curve in (2.1). Then there is an elliptic curve E' over K such that:*

(i) the elliptic curve E' has good reduction away from S_K;

(ii) E' has a K-rational point of order 2;

(iii) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$;

(iv) for $\mathfrak{P} \in T_K$, $\upsilon_{\mathfrak{P}}(j_{E'}) < 0$ where $j_{E'}$ is the j-invariant of E'.

Proof First we note that E is semistable outside S_K by Lemma 3.2. We know that E is modular by either Theorem 2.1 or Theorem 2.2 or conjecturally. Moreover, $\overline{\rho}_{E,p}$ is irreducible by Theorem 2.3 by taking B_K sufficiently large. We then apply Theorem 2.4, Lemma 3.2 and obtain $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for some Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\varpi|p$ of $\mathbb{Q}_{\mathfrak{f}}$ where $\mathbb{Q}_{\mathfrak{f}}$ denotes the field generated by the Hecke eigenvalues of $\mathfrak{f}$.

Now we reduce to the case where $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, after possibly enlarging B_K by an effective amount. The details of this argument can be found in [33]. Next we want to show that there is some elliptic curve E'/K of conductor $\mathcal{N}_p$ having the same L-function as $\mathfrak{f}$. Now, let $\mathfrak{P} \in T_K$. We know that E has potentially multiplicative reduction at $\mathfrak{P}$ and $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ by Lemma 3.5. We can conclude that there is an elliptic curve E' satisfying $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ if we implement Corollary 2.7 after possibly enlarging B_K to ensure that $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{P}) \pm 1)$.

Now we want $\overline{\rho}_{E,p}$ to be isomorphic a mod p Galois representation of an elliptic curve which has a nontrivial K-rational point of order 2. If E' has a such point we are done. If not, we know $E[p] \simeq E'[p]$ as Galois modules for all $p > B_K$. Since 2 divides $\#E[p]$ for all $p > B_K$, 2 divides $E'[p]$ as well. By Theorem 4.2 below, E' is K-isogenous to an elliptic curve E'' such that $\#(\mathrm{Tors}\, E''(K)) \equiv 0 \pmod 2$. Thus, E'' has a nontrivial K-rational point of order 2.

If E' is 2-isogenous to an elliptic curve E'' then (as $p \neq 2$) the isogeny induces an isomorphism $E'[p] \simeq E''[p]$ of Galois modules. Thus, we have $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p} \sim \overline{\rho}_{E'',p}$. Hence, we may, after possibly replacing E' by E'', assume that E' has a nontrivial K-rational 2-torsion point.

Now let $j_{E'}$ denote the j-invariant of E'. Lemma 3.5 implies that $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$, so $p|\#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$. Thus, by Lemma 3.3, we have $\upsilon_{\mathfrak{P}}(j_{E'}) < 0$. □

Theorem 4.2 ([37],Theorem 2) *Let E be an elliptic curve over a number field K, and $m \geq 2$ an integer. For each prime $\mathfrak{p}$ of K at which E has good reduction let $N(\mathfrak{p})$ denote the number of $\mathbb{F}_{\mathfrak{p}}$-rational points on E* mod $\mathfrak{p}$. *If we have*

$$N(\mathfrak{p}) \equiv 0 \pmod m$$

for a set of primes $\mathfrak{p}$ of density one in K, then there exists a K-isogenous elliptic curve E' defined over K such that

$$\#(\mathrm{Tors}\, E'(K)) \equiv 0 \pmod m.$$

5. Proof of the Main Theorem

So far, we have proved that a putative nontrivial solution to the equation (1.1) in W_K yields an elliptic curve E' with a K-rational point of order 2 having good reduction away from the set S_K. In order to prove our Main Theorem, we need to recall that elliptic curves E' with full 2-torsion are related to the solutions of the

S-unit equation (1.2) via λ-invariants of elliptic curves (see, e.g., [48], pp. 53-55). For more details, we refer the reader to the Section 5 of [26].

Let E' be an elliptic curve over K with full 2-torsion: $E' : Y^2 = (X-e_1)(X-e_2)(X-e_3)$, where e_1, e_2, e_3 are all distinct. Every elliptic curve of this form is isomorphic (over $\overline{K}$) to an elliptic curve in the *Legendre form* $E_\lambda : Y^2 = X(X-1)(X-\lambda)$ for $\lambda \in \mathbb{P}^1(K) - \{0,1,\infty\}$ whose j-invariant is

$$j(\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2}. \tag{5.1}$$

Let $\mathfrak{S}_3$ denote the symmetric group on three letters. The action of $\mathfrak{S}_3$ on the set $\{e_1, e_2, e_3\}$ can be extented to an action on $\mathbb{P}^1(K) - \{0,1,\infty\}$ via the cross ratio $\lambda = \frac{e_3-e_1}{e_2-e_1}$. Under the action of $\mathfrak{S}_3$, the orbit of λ in $\mathbb{P}^1(K) - \{0,1,\infty\}$, called λ*-invariants*, is the set:

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

Moreover, there is a one-to-one correspondence between the $\overline{K}$-isomorphism classes of the Legendre elliptic curves and the $\mathfrak{S}_3$-orbits of elements of $\lambda \in \mathbb{P}^1(K) - \{0,1,\infty\}$.

Proof Let K be a number field as in the Main Theorem and B_K be as in Theorem 4.1. Let $(a,b,c) \in W_K$ with a prime exponent $p > B_K$. By applying Theorem 4.1, we obtain an elliptic curve E'/K with a nontrivial K-rational 2-torsion point, having good reduction outside S_K and $\upsilon_{\mathfrak{P}}(j_{E'}) < 0$. Write E' of the form

$$E' : y^2 = x^3 + ax^2 + bx.$$

Thus, $p(x) = x^3 + ax^2 + bx$ is the 2-division polynomial of E'. Let e_1, e_2 be the non-zero roots of $p(x)$. Then the 2-divison field of E', denoted by $L = K(e_1, e_2)$, is an extension of K of degree either 1 or 2. Hence, we have 2 cases:

(1) E' has full 2-torsion on K

(2) E' has full 2-torsion on $L = K(e_1, e_2)$

Case (1): Let λ be any of the λ-invariants of E'. As E' has good reduction away from S_K, the j-invariant $j_{E'}$ belongs to $\mathcal{O}_{S_K}$. From the equation (5.1), we can deduce that $\lambda \in K$ satisfies a monic polynomial with coefficients in $\mathcal{O}_{S_K}$ implying $\lambda \in \mathcal{O}_{S_K}$. On the other hand, notice that $1/\lambda, \mu := 1-\lambda$ and $1/\mu$ are solutions of (5.1) and hence elements of $\mathcal{O}_{S_K}$. Therefore, we conclude that (λ, μ) is a solution of the S_K-unit equation (1.2).

Now, by the assumption of the Main Theorem, for every solution (λ, μ) of the S_K-unit equation (1.2) there is some $\mathfrak{P} \in T_K$ satisfying $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\upsilon_{\mathfrak{P}}(2)$. Let $t := \max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\}$ and further let us express $j_{E'}$ in terms of λ and μ as:

$$j_{E'} = 2^8 \frac{(1-\lambda\mu)^3}{(\lambda\mu)^2}. \tag{5.3}$$

Now, if $t = 0$, then $v_{\mathfrak{P}}(j_{E'}) \geq 8v_{\mathfrak{P}}(2) \geq 0$ by (5.3). This contradicts with the assumption that $v_{\mathfrak{P}}(j_{E'}) < 0$. Hence, we may suppose $t > 0$. The relation $\lambda + \mu = 1$ leads to $v_{\mathfrak{P}}(\lambda + \mu) \geq \min\{v_{\mathfrak{P}}(\lambda), v_{\mathfrak{P}}(\mu)\}$ with equality if $v_{\mathfrak{P}}(\lambda) \neq v_{\mathfrak{P}}(\mu)$. This shows either $v_{\mathfrak{P}}(\lambda) = v_{\mathfrak{P}}(\mu) = -t$, or $v_{\mathfrak{P}}(\lambda) = t$ and $v_{\mathfrak{P}}(\mu) = 0$, or $v_{\mathfrak{P}}(\lambda) = 0$ and $v_{\mathfrak{P}}(\mu) = t$. Therefore, $v_{\mathfrak{P}}(\lambda\mu) = -2t < 0$ or $v_{\mathfrak{P}}(\lambda\mu) = t > 0$. In any of the cases, we have $v_{\mathfrak{P}}(j_{E'}) \geq 8v_{\mathfrak{P}}(2) - 2t \geq 0$, which again yields a contradiction.

Case (2): Suppose that E' has full 2-torsion on L which is a quadratic extension of K. Note that in this case $\lambda \in L$, where λ is the λ-invariant of E'.

By Proposition 3.1. in [38], we know that there are only finitely many quadratic extensions of K with the above properties and there is an algorithm for computing them. In particular, $L = K(\sqrt{a})$ for $a \in K(S_K, 2)$ where $K(S_K, 2)$ is the 2-Selmer group of K.

Now, consider the Frey curve E and the associated elliptic curve E' over L. Then, they have the following properties:

(i) E' has full 2-torsion on L,

(ii) E' has good reduction outside S_L,

(iii) $E[p] \simeq E'[p]$ as Galois modules for $p > B_K$,

(iv) $v_{\mathfrak{P}'}(j_{E'}) < 0$ for $\mathfrak{P}' \in T_L$.

As L is an extension of K, the properties in (i)–(iii) are clear. However, the last statement needs to be proven. In order to prove it, we need the following lemma. □

Lemma 5.1 *Let $\mathfrak{P}' \in T_L$ and $(a, b, c) \in W_K$ with exponent $p > 6v_{\mathfrak{P}'}(2)$. Let E be the Frey curve in (2.1), which we think of it over L. Then E has potentially multiplicative reduction at $\mathfrak{P}'$ and $p \nmid v_{\mathfrak{P}'}(j_E)$.*

Proof Since $\mathfrak{P}' \in T_L$, we have $\mathfrak{P}'|b$. Then $v_{\mathfrak{P}'}(j_E) = 6v_{\mathfrak{P}'}(2) - pv_{\mathfrak{P}'}(b)$. Since $p > 6v_{\mathfrak{P}'}(2)$, we have $v_{\mathfrak{P}'}(j_E) < 0$ which means that E has potentially multiplicative reduction at $\mathfrak{P}'$, and obviously $p \nmid v_{\mathfrak{P}'}(j_E)$. □

By applying Lemma 5.1 and Lemma 3.3 we see that $p | \#\overline{\rho}_{E,p}(I_{\mathfrak{P}'})$, so $p | \#\overline{\rho}_{E',p}(I_{\mathfrak{P}'})$. Hence, Lemma 3.3 implies that $v_{\mathfrak{P}'}(j_{E'}) < 0$ for $\mathfrak{P}' \in T_L$. This finishes the proof of (iv).

Now, we will prove the Main Theorem in Case (2). Let λ be any of the λ-invariants of E'. As E' has good reduction away from S_L, the j-invariant $j_{E'}$ belongs to $\mathcal{O}_{S_L}$. From the equation (5.1), we can deduce that $\lambda \in L$ satisfies a monic polynomial with coefficients in $\mathcal{O}_{S_L}$ implying $\lambda \in \mathcal{O}_{S_L}$. On the other hand, notice that $1/\lambda, \mu := 1 - \lambda$ and $1/\mu$ are solutions of (5.1) and hence elements of $\mathcal{O}_{S_L}$. Therefore, we conclude that (λ, μ) is a solution of the S_L-unit equation (1.2).

Now, by the assumption of the Main Theorem, for every solution (λ, μ) of the S_L-unit equation (1.2) there is some $\mathfrak{P}' \in T_L$ satisfying $\max\{|v_{\mathfrak{P}'}(\lambda)|, |v_{\mathfrak{P}'}(\mu)|\} \leq 4v_{\mathfrak{P}'}(2)$. By exactly the same argument in Case (i), let $t := \max\{|v_{\mathfrak{P}'}(\lambda)|, |v_{\mathfrak{P}'}(\mu)|\}$. Now, if $t = 0$, then $v_{\mathfrak{P}'}(j_{E'}) \geq 8v_{\mathfrak{P}'}(2) \geq 0$ by (5.3). This contradicts with the $v_{\mathfrak{P}'}(j_{E'}) < 0$. Hence, we may suppose $t > 0$. The relation $\lambda+\mu = 1$ leads to $v_{\mathfrak{P}'}(\lambda+\mu) \geq \min\{v_{\mathfrak{P}'}(\lambda), v_{\mathfrak{P}'}(\mu)\}$ with equality if $v_{\mathfrak{P}'}(\lambda) \neq v_{\mathfrak{P}'}(\mu)$. This shows either $v_{\mathfrak{P}'}(\lambda) = v_{\mathfrak{P}'}(\mu) = -t$, or $v_{\mathfrak{P}'}(\lambda) = t$ and $v_{\mathfrak{P}'}(\mu) = 0$, or $v_{\mathfrak{P}'}(\lambda) = 0$ and $v_{\mathfrak{P}'}(\mu) = t$. Therefore, $v_{\mathfrak{P}'}(\lambda\mu) = -2t < 0$ or $v_{\mathfrak{P}'}(\lambda\mu) = t > 0$. In any of the cases, we have $v_{\mathfrak{P}'}(j_{E'}) \geq 8v_{\mathfrak{P}'}(2) - 2t \geq 0$, which again yields a contradiction. This completes the proof of the theorem.

6. An example

In this section we give an example of the main theorem and get the following result:

Corollary 6.1 *Let $K=\mathbb{Q}(\sqrt{2})$ and $\beta=(\sqrt{2})\mathcal{O}_K$. The equation $x^p+y^p=z^2$ does not have any nontrivial solution (a,b,c) in K such that $\beta|b$ whenever $p>B_K$ where B_K is a constant that depends only on K.*

Remark 6.2 *For instance for $K=\mathbb{Q}(\sqrt{2})$ we found the bound $B_K=282430599364$ by using [34]. We want to emphasize that this bound need not to be optimal.*

Proof The proof relies on finding all solutions of the S-unit equation $\lambda+\mu=1$ over K and over L where $L=K(\sqrt{a})$ for $a\in K(S_K,2)$. The list of such L is as below:

- $L_1=\mathbb{Q}(a_1)$ where a_1 is root of x^4+1
- $L_2=\mathbb{Q}(a_2)$ where a_2 is root of x^4-2x^2+9
- $L_3=\mathbb{Q}(a_3)$ where a_3 is root of x^4-2
- $L_4=\mathbb{Q}(a_4)$ where a_4 is root of x^4-2x^2-1
- $L_5=\mathbb{Q}(a_5)$ where a_5 is root of x^4+2x^2-1
- $L_6=\mathbb{Q}(a_6)$ where a_6 is root of x^4+4x^2+2
- $L_7=\mathbb{Q}(a_7)$ where a_7 is root of x^4-4x^2+2

Among these L_i's L_1,L_2,L_6, and L_7 are subfields of $M=\mathbb{Q}(\zeta_{16})$ but L_3,L_4,L_5 are not subfields of M. To find the solutions of the S-unit equation and to check that valutive criterion are satisfied we have used the example in [33]. There, they compute this for the S-unit solutions in M which implies the result for any subfield of M too. For the remaning three subfields and $K=\mathbb{Q}(\sqrt{2})$ we use the algorithm implemented in the computer algebra package Sage in [1]. The list of all solutions is avaliable online*. □

Remark 6.3 *For real quadratic number fields K, $T_K\neq\emptyset$ if either 2 ramifies or 2 splits in K. In the first case, we had to restrict the example to the field $K=\mathbb{Q}(\sqrt{2})$ since the only real quadratic number field with narrow class number one in which 2 is ramified is $\mathbb{Q}(\sqrt{2})$. There are real quadratic number fields with narrow class number one in which 2 splits. However, for those fields, computing the solutions of the S-unit equation over the quadratic extensions L of K coming from the Selmer group were not possible for all possible L. Similarly, we had the same computational difficulty for totally real fields of degree greater than 2 with narrow class number one and $T_K\neq\emptyset$.*

Acknowledgment

All authors are supported by TÜBİTAK (The Scientific and Technological Research Council of Turkey) Research Grant 117F045.

*https://sites.google.com/view/erman-isik/research?authuser=0

References

[1] Alvarado A, Koutsianas A, Malmskog B, Rasmussen C, Vincent C et al. A robust implementation for solving the S-unit equation and several applications. arXiv:1903.00977

[2] Anni S, Siksek S. Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^2+y^{2m}=z^p$. Algebra & Number Theory 2016; 6 (10): 1147-1172.

[3] Bennett MA. The equation $x^{2n}+y^{2n}=z^5$. Journal de théorie des nombres de Bordeaux 2006; 2 (18) : 315-321.

[4] Bennett MA, Chen I. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2+b^6=c^n$. Algebra & Number Theory 2012; 4 (6): 707-730.

[5] Bennett MA, Chen I, Dahmen SR, Yazdani S. Generalized Fermat equations: a miscellany. International Journal of Number Theory 2015; 1 (11): 1-28.

[6] Bennett MA, Ellenberg JS, Ng NC. The diophantine equation $A^4+2\delta B^2=C^n$. International Journal of Number Theory 2010; 2 (6): 311-338.

[7] Bennet M, Mihăilescu P, Siksek S. The generalized Fermat equation, in Open problems in mathematics 2016; Springer, pp. 173-205.

[8] Bennett MA, Skinner CM. Ternary Diophantine equations via Galois representations and modular forms. Canadian Journal of Mathematics 2004; 1 (56): 23-54.

[9] Billerey N, Chen I, Dieulefait L, Freitas N. A multi-Frey approach to Fermat equations of signature(r,r,p).Transactions of American Mathematical Society 2019; 12 (371): 8651-8677.

[10] Billerey N, Chen I, Dieulefait L, Freitas N. A result on the equation $x^p+y^p=z^r$ using Frey abelian varieties. Proceedings of the American Mathematical Society 2017; 10 (145), pp.4111-4117.

[11] Billerey N, Dieulefait L. Solving Fermat-type equations $x^5+x^5=dz^p$. Mathematics of Computation 2010; 269 (79), pp.535-544.

[12] Blasius D. Elliptic curves. Hilbert modular forms and the Hodge conjecture, In: Hida H, Ramakrishnan D, Shahidi F (editors). Contributions to Automorphic Forms, Geometry, and Number Theory. Baltimore, MD, USA: Johns Hopkins University Press, pp. 83-103.

[13] Brown D. Primitive Integral Solutions to $x^2+y^3=z^{10}$, International Mathematics Research Notices IMRN 2012 : 423-436.

[14] Bruin N. The Diophantine Equations $x^2\pm y^4=z^6$ and $x^2+y^8=z^3$. Compositio Mathematica 1999; 3 (118): 305-321.

[15] Bruin N. On powers as sums of two cubes. In: International Algorithmic Number Theory Symposium 2000; July, Springer, Berlin, Heidelberg, pp. 169-184.

[16] Bruin N. The primitive solutions to $x^3+y^9=z^2$. J. Number Theory 2005; 1 (111) : 179-189.

[17] Chen I. On the equation $a^2+b^{2p}=c^5$, Acta Arithmetica 2010; 4 (143): 345-375.

[18] Chen I. On the equation $s^2+y^{2p}=\alpha^3$. Mathematical Componrnts 2008; 77 : 1223-1227.

[19] Chen I, Siksek S. Perfect powers expressible as sums of two cubes. Journal of Algebra 2009; 3 (322) : 638-656.

[20] Cohen H. Advanced Topics in Computational Number Theory. New York, NY, USA: Springer, 1999.

[21] Dahmen S. Classical and modular methods applied to Diophantine equations. Utrecht University, 2008.

[22] Dahmen S. A refined modular approach to the Diophantine equation $x^2+y^{2n}=z^3$. International Journal Number Theory 7 2011; 5 : 1303-1316.

[23] Dahmen SR, Siksek S. Perfect powers expressible as sums of two fifth or seventh powers. arXiv preprint 2013; arXiv:1309.4030.

[24] Darmon H, Granville A. On the equations $z^m = F(x,y)$ and $Ax^p+By^q = Cz^r$. Bulletin of the London Mathematical Society 1995; 6 (27): 513-543.

[25] Darmon H, Merel L. Winding quotients and some variants of Fermat's Last Theorem. Journal Reine Angew Mathematik 1997; 490: 81-100.

[26] Deconinck H. On the generalized Fermat equation over totally real fields. Acta Arithmetica 2016; 3 (173): 225-237.

[27] Derickx M, Najman F, Siksek S. Elliptic curves over totally real cubic fields are modular. arXiv:1901.03436v1

[28] Dieulefait L, Freitas N. Fermat-type equations of signature $(13,13,p)$ via Hilbert cuspforms. Mathematische Annalen 2013; 3 (357): 987-1004.

[29] Ellenberg JS. Galois Representations Attached to $\mathbb{Q}$-Curves and the Generalized Fermat Equation $A^4 + B^2 = C^p$. American journal of mathematics 2004; 763-787.

[30] Faltings G. Erratum: Finiteness theorems for abelian varieties over number fields. Inventiones Mathematicae 1984; 2 (75): 381.

[31] Freitas N, Le Hung BV, Siksek S. Elliptic curves over real quadratic field are modular. Inventiones Mathematicae 2015; 1 (201): 159-206.

[32] Freitas N, Siksek S. Criteria for Irreducibility of mod p Representations of Frey Curves. Journal de théorie des nombres de Bordeaux 2015; 1 (27): 67-76.

[33] Freitas N, Siksek S. The asymptotic Fermat's last theorem for five-sixths of real quadratic fields. Compositio Mathematica 2015; 8 (18): 1395-1415.

[34] Freitas N, Siksek S. Criteria for irreducibility of mod p representations of Frey curves. Journal de Theorie des Nombres de Bordeaux 2015; 1 (27): 67-76.

[35] Jarvis F, Meekin P. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. Journal of Number Theory 2004; (109) : 182-196.

[36] Kara Y, Ozman E. Asymptotic Generalized Fermat's Last Theorem over Number Fields. To appear in International Journal of Number Theory. doi: 10.1142/S1793042120500463

[37] Katz NM. Galois properties of torsion points on abelian varieties. Inventiones Mathematicae 1981; 3 (62): 481-502.

[38] Koutsianas A. Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction. Experimental Mathematics 2019; 1 (28): 1-15.

[39] Kraus A. Majorations effectives pour l'équation de Fermat Généralisée. Canadian Journal of Mathematics 1997; 49 : 1139-1161 (in French).

[40] Kraus A. Sur l'équation $a^3 + b^3 = c^p$. Experimental Mathematics 1998; 7 (1) : 1-13.

[41] Poonen B. Some Diophantine equations of the form $x^n + y^n = z^m$. Acta Arithmetica 1998; 86 : 193-205.

[42] Poonen B, Schaefer EF, Stoll M. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. Duke Mathematical Journal 2007; 1 (137): 103-158.

[43] Şengün MH, Siksek S. On the asymptotic Fermat's last theorem over number fields. Commentarii Mathematici Helvetici 2018; 2 (93): 359-375.

[44] Siksek S. On the Diophantine equation $x^2 = y^p + 2^k z^p$. Journal de Théorie des Nombres de Bordeaux 2003; 15 : 839-846.

[45] Siksek S. Explicit Chabauty over number fields. Algebra & Number Theory, 7 (4): 765-793.

[46] Siksek S, Stoll M. Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$. Bulletin of the LMS 2012; 44 : 151-166

[47] Siksek S, Stoll M. The generalised Fermat equation $x^2 + y^3 = z^{15}$. Archiv Mathematik (Basel) 2014; 5 (102): 411-421.

[48] Silverman JH. The arithmetic of elliptic curves. Graduate Texts in Mathematics 1986; vol. 106, Springer, Dordrecht.

[49] Silverman JH. Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 1994; vol. 151. Springer, New York.

[50] Taylor R, Wiles A. Ring-theoretic properties of certain Hecke algebras. Annals of Mathematics 1995; 141: 553-572.

[51] Turcas G. On Fermat's equation over some quadratic imaginary number fields. Research in Number Theory 2018; 4:24.

[52] Turcas G. On Serre's modularity conjecture and Fermat's equation over quadratic imaginary fields of class number one. arXiv:1908.11690v1

[53] Wiles A. Modular elliptic curves and Fermat's last theorem. Annals of Mathematics 1995; 2 (141): 443-551.